User Guide

AWS Entity Resolution

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Entity Resolution: User Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Entity Resolution? 1
Sind Sie ein Erstbenutzer? AWS Entity Resolution 1
Funktionen von AWS Entity Resolution 2
Zugehörige Services 5
Zugreifen AWS Entity Resolution 6
Preisgestaltung für AWS Entity Resolution 6
Einrichtung 7
Melden Sie sich an für ein AWS-Konto 7
Erstellen einer IAM-Rolle für einen Konsolenbenutzer 7
Eine Workflow-Jobrolle erstellen 8
Eingabedatentabellen vorbereiten 17
Vorbereiten von Eingabedaten von Erstanbietern 17
Schritt 1: Bereiten Sie Datentabellen von Erstanbietern vor 17
Schritt 2: Speichern Sie Ihre Eingabedatentabelle in einem unterstützten Datenformat 20
Schritt 3: Laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch 21
Schritt 4: Erstellen Sie ein AWS Glue Tabelle 21
Schritt 4: Erstellen Sie eine partitionierte AWS Glue Tabelle 23
Vorbereiten von Eingabedaten von Drittanbietern 25
Schritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange 26
Schritt 2: Bereite Datentabellen von Drittanbietern vor 27
Schritt 3: Speichern Sie Ihre Eingabedatentabelle in einem unterstützten Datenformat 32
Schritt 4: Laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch 33
Schritt 5: Erstellen Sie ein AWS Glue Tabelle 33
Schemazuordnung 36
Eine Schemazuordnung erstellen 37
Klonen einer Schemazuordnung 51
Eine Schemazuordnung bearbeiten 52
Löschen einer Schemazuordnung 53
ID-Namespace 54
ID-Namespace-Quelle 55
Eine ID-Namespace-Quelle erstellen (regelbasiert) 55
Eine ID-Namespace-Quelle erstellen (Providerdienste) 60
ID-Namespace-Ziel 62
Erstellen eines ID-Namespace-Ziels (regelbasierte Methode) 63

Erstellen eines ID-Namespace-Ziels (Provider-Services-Methode) ... 66
Einen ID-Namespace bearbeiten ... 67
Löschen eines ID-Namespaces ... 67
Hinzufügen oder Aktualisieren einer Ressourcenrichtlinie für einen ID-Namespace ... 68
Passender Arbeitsablauf ... 69
Passende Workflowtypen ... 70
Optionen für die Datenausgabe ... 70
Passende Workflow-Ergebnisse ... 71
Einen regelbasierten Matching-Workflow erstellen ... 72
Erweiterter Regeltyp ... 74
Einfacher Regeltyp ... 94
Erstellung eines Matching-Workflows, der auf maschinellem Lernen basiert ... 105
Erstellen eines auf dem Provider-Service basierenden Matching-Workflows ... 111
Erstellen Sie einen passenden Workflow mit LiveRamp ... 111
Erstellen Sie einen passenden Workflow mit TransUnion ... 120
Einen passenden Workflow mit UID 2.0 erstellen ... 128
Bearbeitung eines passenden Workflows ... 134
Einen passenden Workflow löschen ... 135
Ändern oder Generieren einer Match-ID ... 135
Eine Match-ID nachschlagen ... 140
Löschen von Datensätzen aus einem regelbasierten oder passenden Workflow ML-based ... 144
Fehlerbehebung ... 144
Ich habe nach der Ausführung eines passenden Workflows eine Fehlerdatei erhalten ... 145
Arbeitsablauf für die ID-Zuordnung ... 147
Workflow für die ID-Zuordnung für einen AWS-Konto ... 148
Voraussetzungen ... 149
Erstellen eines Workflows zur ID-Zuordnung (regelbasiert) ... 150
Erstellen eines Workflows für die ID-Zuordnung (Provider-Services) ... 157
Workflow zur ID-Zuordnung über zwei AWS-Konten ... 163
Voraussetzungen ... 164
Erstellen eines Workflows zur ID-Zuordnung (regelbasiert) ... 165
Erstellen eines Workflows für die ID-Zuordnung (Provider-Services) ... 171
Ausführen eines Workflows zur ID-Zuordnung ... 177
Ausführen eines benutzerdefinierten ID-Zuordnungs-Workflows ... 179
Bearbeitung eines Workflows zur ID-Zuordnung ... 182
Löschen eines Workflows zur ID-Zuordnung ... 183

Hinzufügen oder Aktualisieren einer Ressourcenrichtlinie für einen ID-Zuordnungs-Workflow ... 184
Anbieterintegration ... 185
Voraussetzungen ... 185
Einen Anbieterdienst auflisten unter AWS Data Exchange ... 185
Identifizieren Sie Ihre Eigenschaften ... 187
Fordern Sie die AWS Entity Resolution OpenAPI-Spezifikation an ... 187
Verwendung der OpenAPI-Spezifikation ... 187
Integration der Stapelverarbeitung ... 188
Integration der synchronen Verarbeitung ... 191
Testen einer Anbieterintegration ... 192
Sicherheit ... 201
Datenschutz ... 202
Datenverschlüsselung im Ruhezustand für AWS Entity Resolution ... 203
Schlüsselverwaltung ... 204
AWS PrivateLink ... 215
Identity and Access Management ... 217
Zielgruppe ... 217
Authentifizierung mit Identitäten ... 218
Verwalten des Zugriffs mit Richtlinien ... 219
Wie AWS Entity Resolution funktioniert mit IAM ... 221
Beispiele für identitätsbasierte Richtlinien ... 227
AWS verwaltete Richtlinien ... 230
Fehlerbehebung ... 233
Compliance-Validierung ... 235
AWS Entity Resolution Bewährte Verfahren zur Einhaltung ... 236
Ausfallsicherheit ... 237
Überwachen ... 238
CloudTrail protokolliert ... 238
AWS Entity Resolution Informationen in CloudTrail ... 239
AWS Entity Resolution Logdateieinträge verstehen ... 240
CloudWatch Logs ... 240
Einrichten der Protokollbereitstellung ... 241
Protokollierung deaktivieren (Konsole) ... 249
Die Protokolle lesen ... 249
AWS CloudFormation Ressourcen ... 252
AWS-Entitätsauflösung und CloudFormation Vorlagen ... 252

Erfahren Sie mehr über CloudFormation ... 254
Kontingente ... 255
API-Drosselungskontingente ... 259
Dokumentverlauf ... 265
Glossar ... 273
Amazon-Ressourcenname (ARN) ... 273
Attribut Typ ... 273
Automatische Verarbeitung ... 273
AWS KMS key ARN ... 273
Batch-Arbeitsablauf ... 274
Klartext ... 274
Konfidenzniveau () ConfidenceLevel ... 274
Konfidenzniveau aufzeichnen (RecordConfidenceLevel) ... 274
Entschlüsselung ... 274
Verschlüsselung ... 274
Gruppenname ... 275
Hash ... 275
Hash-Protokoll (HashingProtocol) ... 275
Methode der ID-Zuordnung ... 275
Arbeitsablauf für die ID-Zuordnung ... 276
ID-Namespace ... 276
Inkrementeller Arbeitsablauf ... 276
Eingabefeld ... 277
Eingabequelle ARN (InputSourceARN) ... 277
Abgleich auf Grundlage von Machine Learning ... 277
Manuelle Verarbeitung ... 277
Many-to-Many übereinstimmend ... 277
Spiel-ID (MatchID) ... 278
Schlüssel abgleichen (MatchKey) ... 278
Name des Abgleichsschlüssels ... 279
Regel abgleichen (MatchRule) ... 279
Übereinstimmung ... 279
Passender Arbeitsablauf ... 279
Passende Workflow-Beschreibung ... 279
Passender Workflow-Name ... 279
Passende Workflow-Metadaten ... 280

Normalisierung () ApplyNormalization 280
Name 281
Email 281
Phone 282
Adresse 282
Gehasht 285
Source_ID 285
Normalisierung () — nur ApplyNormalization ML-based 286
Name 286
Email 286
Phone 286
One-to-One übereinstimmend 287
Ausgabe 287
Gibt S3Path aus 288
OutputSourceConfig 288
Abgleich auf Basis des Provider-Dienstes 288
Rule-based übereinstimmend 288
Transitiver Abgleich 289
Schema 289
Beschreibung des Schemas 289
Name des Schemas 290
Schema-Zuordnung 290
ARN für Schemazuordnung 290
Eindeutige ID 290
..... ccxcii

Was ist AWS Entity Resolution?

AWS Entity Resolution ist ein Service, mit dem Sie zusammengehörende Datensätze, die in mehreren Anwendungen, Kanälen und Datenspeichern gespeichert sind, abgleichen, verknüpfen und verbessern können. Sie können mit Workflows zur Entitätsauflösung beginnen, die flexibel und skalierbar sind und eine Verbindung zu Ihren bestehenden Anwendungen und Datendienstanbietern herstellen können.

AWS Entity Resolution bietet fortschrittliche Matching-Techniken, wie z. B. regelbasierten Abgleich, auf maschinellem Lernen basierenden Abgleich (ML-Matching) und von Datendienstanbietern gesteuertes Matching. Diese Techniken können Ihnen dabei helfen, zugehörige Datensätze mit Kundeninformationen, Produktcodes oder Geschäftsdatencodes genauer zu verknüpfen und zu verbessern.

Sie können AWS Entity Resolution damit eine einheitliche Ansicht der Kundeninteraktionen erstellen, indem Sie aktuelle Ereignisse (wie Anzeigenklicks, abgebrochene Warenkörbe und Käufe) mit pseudonymisierten Signalen Ihrer Datendienstleister zu einer eindeutigen Entitäts-ID verknüpfen. Sie können auch Produkte, die unterschiedliche Codes (z. B. SKU, UPC) verwenden, in Ihren Geschäften besser nachverfolgen. Sie können AWS Entity Resolution damit die Genauigkeit der Abgleiche kontrollieren, die Datensicherheit besser schützen und gleichzeitig Datenbewegungen minimieren.

Themen

- Sind Sie ein Erstbenutzer? AWS Entity Resolution
- Funktionen von AWS Entity Resolution
- Zugehörige Services
- Zugreifen AWS Entity Resolution
- Preisgestaltung für AWS Entity Resolution

Sind Sie ein Erstbenutzer? AWS Entity Resolution

Wenn Sie zum ersten Mal Benutzer von sind AWS Entity Resolution, empfehlen wir Ihnen, zunächst die folgenden Abschnitte zu lesen:

- Funktionen von AWS Entity Resolution
- Zugreifen AWS Entity Resolution

- Einrichten AWS Entity Resolution

Funktionen von AWS Entity Resolution

AWS Entity Resolution beinhaltet die folgenden Funktionen:

- Flexible und anpassbare Datenaufbereitung

  AWS Entity Resolution liest Ihre Daten aus AWS Glue , um sie als Eingabe für die Spielverarbeitung zu verwenden. Sie können maximal 20 Dateneingaben angeben. AWS Entity Resolution verarbeitet jede Zeile der Dateneingabetabelle als Datensatz, wobei eine eindeutige Entität als Primärschlüssel dient. AWS Entity Resolution kann mit verschlüsselten Datensätzen arbeiten. Definieren Sie zunächst das Schema-Mapping AWS Entity Resolution , um zu verstehen, welche Eingabefelder Sie in Ihrem Matching-Workflow verwenden möchten. Sie können Ihr eigenes Datenschema oder Ihren eigenen Blueprint aus einer vorhandenen AWS Glue Dateneingabe übernehmen. Oder Sie können Ihr benutzerdefiniertes Schema mithilfe einer interaktiven Benutzeroberfläche oder eines JSON-Editors erstellen. Normalisiert standardmäßig AWS Entity Resolution auch Dateneingaben vor dem Abgleich, um die Match-Verarbeitung zu verbessern, z. B. das Entfernen von Sonderzeichen und zusätzlichen Leerzeichen und das Formatieren von Text in Kleinbuchstaben. Wenn Ihre Dateneingabe bereits normalisiert ist, können Sie die Normalisierung deaktivieren. Wir bieten auch eine GitHub Bibliothek, mit der Sie den Datennormalisierungsprozess weiter an Ihre Bedürfnisse anpassen können.
- Konfigurierbare Workflows zum Abgleich von Entitäten

  Ein Workflow für den Entitätsabgleich besteht aus einer Abfolge von Schritten, die Sie einrichten, um festzulegen, AWS Entity Resolution wie Ihre Dateneingabe abgeglichen werden soll und wo die konsolidierte Datenausgabe geschrieben werden soll. Sie können einen oder mehrere Abgleichs-Workflows einrichten, um verschiedene Dateneingaben zu vergleichen und unterschiedliche Abgleichstechniken wie regelbasierten Abgleich, maschinellen Lernabgleich oder von Datendienstanbietern gesteuerter Abgleich ohne Erfahrung mit Entitätsauflösung oder maschinellem Lernen zu verwenden. Sie können auch den Auftragsstatus vorhandener Abgleichs-Workflows und Metriken anzeigen, z. B. die Ressourcennummer, die Anzahl der verarbeiteten Datensätze und die Anzahl der gefundenen Treffer.

  - Ready-to-use regelbasierter Abgleich

    Diese Vergleichstechnik beinhaltet eine Reihe von ready-to-use Regeln im AWS-Managementkonsole oder AWS Command Line Interface ()AWS CLI. Sie können diese Regeln

verwenden, um anhand Ihrer Eingabefelder nach verwandten Datensätzen zu suchen. Sie können die Regeln auch anpassen, indem Sie Eingabefelder für jede Regel hinzufügen oder entfernen, Regeln löschen, die Regelpriorität neu anordnen und neue Regeln erstellen. Sie können die Regeln auch auf ihre ursprüngliche Konfiguration zurücksetzen. Die in Ihrem Amazon Simple Storage Service (Amazon S3) -Bucket ausgegebenen Daten enthalten Übereinstimmungsgruppen, die mithilfe der regelbasierten Vergleichstechnik AWS Entity Resolution generiert werden. Jeder Match-Gruppe ist die Regelnummer zugeordnet, die zur Generierung des Matches verwendet wurde, um Ihnen das Verständnis des Matches zu erleichtern. Die Regelnummer kann beispielsweise die Genauigkeit jeder Spielgruppe belegen, sodass Regel eins genauer ist als Regel zwei.

- Vorkonfigurierter Abgleich auf Basis von maschinellem Lernen (ML-Matching)

  Diese Abgleichstechnik umfasst ein vorkonfiguriertes ML-Modell, mit dem Sie Übereinstimmungen für all Ihre Dateneingaben, insbesondere für verbraucherbasierte Datensätze, finden können. Das Modell verwendet alle Eingabefelder, die den Datentypen Name, E-Mail-Adresse, Telefonnummer, Adresse und Geburtsdatum zugeordnet sind. Das Modell generiert Zuordnungsgruppen verwandter Datensätze mit einem Konfidenzwert für jede Gruppe, der die Qualität der Übereinstimmung im Vergleich zu anderen Übereinstimmungsgruppen erklärt. Das Modell berücksichtigt fehlende Eingabefelder und analysiert den gesamten Datensatz zusammen, sodass er eine Einheit darstellt. Die Datenausgabe in Ihrem Amazon S3 S3-Bucket enthält Übereinstimmungsgruppen, die mithilfe des ML-Matchings AWS Entity Resolution generiert werden. Hier ist jeder Spielgruppe ein Konfidenzwert von 0,0-1,0 zugeordnet, der die Genauigkeit des Spiels angibt.

- Datensätze mit Datendienstanbietern abgleichen

  Damit können AWS Entity Resolution Sie Ihre Datensätze mit führenden Datendienstanbietern und lizenzierten Datensätzen abgleichen, verknüpfen und verbessern, um Ihre Kunden besser zu verstehen, zu erreichen und zu betreuen. Sie können beispielsweise Attribute an Ihre Daten anhängen, um Ihre Datensätze zu verbessern, oder Sie können die Interoperabilität von Systemen und Plattformen verbessern, mit denen Sie arbeiten, um Ihre Geschäftsziele zu erreichen. Sie können diesen Matching-Workflow mit wenigen Klicks verwenden, sodass Sie keine komplexen proprietären Integrationen erstellen und verwalten müssen. Sie benötigen eine Lizenzvereinbarung mit diesen Datendienstanbietern, um diese Matching-Technik nutzen zu können.

- Manuelle Massenverarbeitung und automatische inkrementelle Verarbeitung

Mithilfe der Datenverarbeitung können Sie Ihre Dateneingabe oder -eingaben in eine konsolidierte Datenausgabetabelle mit ähnlichen Datensätzen konvertieren, die über eine gemeinsame Match-ID verfügen, die mithilfe von Workflow-Konfigurationen für den Entitätsabgleich generiert wurde. Mithilfe der API AWS-Managementkonsole und/oder der AWS CLI können Sie bei Bedarf eine manuelle Massenverarbeitung auf der Grundlage Ihrer vorhandenen ETL-Datenpipeline (Extrahieren, Transformieren und Laden) ausführen, die alle Daten für neue Treffer und Aktualisierungen vorhandener Treffer erneut verarbeitet. Für regelbasierte Vergleichsszenarien können Sie außerdem eine automatische inkrementelle Verarbeitung einleiten, sodass der Service diese neuen Datensätze liest und mit vorhandenen Datensätzen vergleicht, sobald neue Daten in Ihrem Amazon S3 S3-Bucket verfügbar sind. Dadurch bleiben Ihre Matches bei allen Änderungen der Amazon S3 S3-Daten auf dem neuesten Stand.

- Suche nahezu in Echtzeit

  Wenn Sie über den AWS Entity Resolution GetMatchId API-Vorgang nach beliebigen Entitätsfeldern suchen, können Sie eine vorhandene Match-ID synchron abrufen. Sie können AWS Entity Resolution mit Attributen personenbezogener Daten (PII) anrufen, die über verschiedene Quellen und Kanäle erfasst wurden. AWS Entity Resolution Hasht diese Attribute aus Datenschutzgründen und ruft die entsprechende Match-ID ab, um den Kunden zu verknüpfen und zuzuordnen. Sie können beispielsweise eine Webanmeldung mit einem zugehörigen Namen, einer E-Mail-Adresse und einer Postanschrift erhalten. Verwenden Sie den AWS Entity Resolution GetMatchId API-Vorgang, um herauszufinden, ob dieser Kunde oder diese Entität bereits in Ihren übereinstimmenden Ergebnissen, die in Ihrem S3-Bucket gespeichert sind, vorhanden ist, zusammen mit der entsprechenden Entitäts-Match-ID, die ihm zugeordnet ist. Nachdem Sie die Entitäts-Match-ID erhalten haben, können Sie die damit verknüpften Transaktionsinformationen in Ihren Quellanwendungen finden, z. B. in Ihren Systemen für Kundenbeziehungsmanagement (CRM) oder Kundendatenplattform (CDP).

- Datenschutz und Regionalisierung von Haus aus

  AWS Entity Resolution bietet eine Standardverschlüsselungsfunktion, mit der Sie Ihre Daten schützen können, und stattet Sie mit einem Verschlüsselungsschlüssel für jede Dateneingabe in den Dienst aus. Bietet Ihnen beispielsweise die AWS Entity Resolution Flexibilität, serverseitig verschlüsselte und gehashte Daten zur Ausführung regelbasierter Abgleichs-Workflows zu verwenden. AWS Entity Resolution unterstützt Regionalisierung, was bedeutet, dass Ihre Abgleichs-Workflows zur Verarbeitung Ihrer Daten an derselben Stelle ausgeführt werden, von der AWS-Region aus Sie den Service verwenden. Sie können die Datenausgabe in Amazon S3 auch verschlüsseln und hashen, bevor Sie Ihre aufgelösten Daten in anderen Anwendungen verwenden.

- Transcodierung für mehrere Parteien

  AWS Entity Resolution hilft Ihnen bei der Definition Ihrer Datenquellen und der passenden Konfigurationen zwischen mehreren Parteien, die eine Datenzusammenarbeit nutzen möchten, z. B. in. AWS Clean Rooms

Zugehörige Services

Folgendes bezieht AWS-Services sich auf AWS Entity Resolution:

- Amazon S3

  Speichern Sie Daten, die Sie AWS Entity Resolution in Amazon S3 importieren.

  Weitere Informationen finden Sie unter Was ist Amazon S3? im Amazon Simple Storage Service-Benutzerhandbuch.

- AWS Glue

  Erstellen Sie AWS Glue Tabellen aus Ihren Daten in Amazon S3 zur Verwendung in AWS Entity Resolution.

  Weitere Informationen finden Sie unter Was ist AWS Glue? im AWS Glue Entwicklerhandbuch.

- AWS CloudTrail

  Verwenden Sie es AWS Entity Resolution zusammen mit CloudTrail Protokollen, um Ihre AWS-Service Aktivitätsanalyse zu verbessern.

  Weitere Informationen finden Sie unter Protokollieren von AWS Entity Resolution API-Aufrufen mit AWS CloudTrail.

- CloudFormation

  Erstellen Sie die folgenden Ressourcen in CloudFormation: AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace und AWS::EntityResolution::PolicyStatement

  Weitere Informationen finden Sie unter Erstellen Sie AWS Entity Resolution-Ressourcen mit AWS CloudFormation.

Zugreifen AWS Entity Resolution

Sie können AWS Entity Resolution über die folgenden Optionen darauf zugreifen:

- Direkt über die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
- Programmgesteuert über die AWS Entity Resolution API. Weitere Informationen finden Sie in der AWS Entity Resolution -API-Referenz.
  - Wenn Sie die AWS Entity Resolution API in AWS Lambda Runtime aufrufen möchten, erstellen Sie Ihr eigenes Bereitstellungspaket und fügen Sie die gewünschte Version der AWS SDK-Bibliothek hinzu. Weitere Informationen finden Sie in den folgenden Beispielen im AWS Lambda Entwicklerhandbuch:
    - Stellen Sie Java-Lambda-Funktionen mit ZIP- oder JAR-Dateiarchiven bereit
    - Arbeiten mit ZIP-Dateiarchiven für Python-Lambda-Funktionen

Preisgestaltung für AWS Entity Resolution

Preisinformationen finden Sie unter AWS Entity Resolution – Preise.

Einrichten AWS Entity Resolution

Melden Sie sich vor der ersten Nutzung AWS Entity Resolution an AWS und erstellen Sie einen Administratorbenutzer, um Rollen zu erstellen.

Melden Sie sich an für ein AWS-Konto

Um loszulegen AWS, benötigen Sie eine AWS-Konto. Informationen zum Erstellen eines AWS-Konto finden Sie unter Erste Schritte mit einem AWS-Konto im AWS -Kontenverwaltung Referenzhandbuch.

Erstellen einer IAM-Rolle für einen Konsolenbenutzer

Gehen Sie wie folgt vor, wenn Sie die AWS Entity Resolution Konsole verwenden.

So erstellen Sie eine IAM-Rolle

1. Melden Sie sich mit Ihrem Administratorkonto bei der IAM-Konsole (https://console.aws.amazon.com/iam/) an.
2. Wählen Sie unter Access management (Zugriffsverwaltung) Roles (Rollen) aus.

   Sie können Rollen verwenden, um kurzfristige Anmeldeinformationen zu erstellen. Dies wird aus Sicherheitsgründen empfohlen. Sie können auch Benutzer auswählen, um langfristige Anmeldeinformationen zu erstellen.
3. Wählen Sie Rolle erstellen aus.
4. Wählen Sie im Assistenten zum Erstellen von Rollen unter Vertrauenswürdiger Entitätstyp die Option AWS-Konto.
5. Behalten Sie die Option Dieses Konto ausgewählt bei und klicken Sie dann auf Weiter.
6. Wählen Sie für Berechtigungen hinzufügen die Option Richtlinie erstellen aus.

   Eine neue Registerkarte wird geöffnet.

   a. Wählen Sie die Registerkarte JSON aus und fügen Sie dann je nach den Fähigkeiten, die dem Konsolenbenutzer gewährt wurden, Richtlinien hinzu. AWS Entity Resolution bietet die folgenden verwalteten Richtlinien auf der Grundlage gängiger Anwendungsfälle:

      - AWS verwaltete Richtlinie: AWSEntityResolutionConsoleFullAccess

- AWS verwaltete Richtlinie: AWSEntityResolutionConsoleReadOnlyAccess

b. Wählen Sie Weiter: Schlagworte, fügen Sie Schlagworte hinzu (optional) und wählen Sie dann Weiter: Überprüfen aus.

c. Geben Sie unter Richtlinie überprüfen einen Namen und eine Beschreibung ein und überprüfen Sie die Zusammenfassung.

d. Wählen Sie Richtlinie erstellen aus.

Sie haben eine Richtlinie für ein Kollaborationsmitglied erstellt.

e. Kehren Sie zu Ihrer ursprünglichen Registerkarte zurück und geben Sie unter Berechtigungen hinzufügen den Namen der Richtlinie ein, die Sie gerade erstellt haben. (Möglicherweise müssen Sie die Seite neu laden.)

f. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die Sie erstellt haben, und klicken Sie dann auf Weiter.

7. Geben Sie unter Name, review and create den Rollennamen und die Beschreibung ein.

a. Überprüfen Sie Vertrauenswürdige Entitäten auswählen und geben Sie die AWS-Konto für die Person oder Personen ein, die die Rolle übernehmen werden (falls erforderlich).

b. Überprüfen Sie die Berechtigungen unter Berechtigungen hinzufügen und bearbeiten Sie sie gegebenenfalls.

c. Überprüfen Sie die Tags und fügen Sie bei Bedarf Stichwörter hinzu.

d. Wählen Sie Rolle erstellen aus.

Erstellen einer Workflow-Jobrolle für AWS Entity Resolution

AWS Entity Resolution verwendet eine Workflow-Jobrolle, um einen Workflow auszuführen. Sie können diese Rolle mithilfe der Konsole erstellen, wenn Sie über die erforderlichen IAM-Berechtigungen verfügen. Wenn Sie keine `CreateRole` Berechtigungen haben, bitten Sie Ihren Administrator, die Rolle zu erstellen.

Um eine Workflow-Jobrolle zu erstellen für AWS Entity Resolution

1. Melden Sie sich https://console.aws.amazon.com/iam/mit Ihrem Administratorkonto bei der IAM-Konsole unter an.
2. Wählen Sie unter Access management (Zugriffsverwaltung) Roles (Rollen) aus.

Sie können Rollen verwenden, um kurzfristige Anmeldeinformationen zu erstellen. Dies wird aus Sicherheitsgründen empfohlen. Sie können auch Benutzer auswählen, um langfristige Anmeldeinformationen zu erstellen.

3. Wählen Sie Rolle erstellen aus.
4. Wählen Sie im Assistenten zum Erstellen von Rollen unter Vertrauenswürdiger Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus.
5. Kopieren Sie die folgende benutzerdefinierte Vertrauensrichtlinie und fügen Sie sie in den JSON-Editor ein.

   JSON

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

6. Wählen Sie Weiter aus.
7. Wählen Sie für Berechtigungen hinzufügen die Option Richtlinie erstellen aus.

   Eine neue Registerkarte wird angezeigt.

   a. Kopieren Sie die folgende Richtlinie und fügen Sie sie in den JSON-Editor ein.

> **Note**
>
> Die folgende Beispielrichtlinie unterstützt die Berechtigungen, die zum Lesen entsprechender Datenressourcen wie Amazon S3 und erforderlich sind AWS Glue.

Je nachdem, wie Sie Ihre Datenquellen eingerichtet haben, müssen Sie diese Richtlinie jedoch möglicherweise ändern.
Sie können AWS Glue Ressourcen und die zugrunde liegenden Amazon S3 S3-Ressourcen aus jeder Region in der AWS kommerziellen Partition verwenden, in der sie unterstützt AWS Glue wird — sie müssen sich nicht in derselben Region befinden wie AWS Entity Resolution.
Sie müssen keine AWS KMS Berechtigungen erteilen, wenn Ihre Datenquellen nicht ver- oder entschlüsselt sind.

JSON

```
{
    "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": [
                        "444455556666"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::{{output-bucket}}",
                "arn:aws:s3:::{{output-bucket}}/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:ResourceAccount": [
                        "444455556666"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:GetSchema",
                "glue:GetSchemaVersion",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:us-east-1:444455556666:database/{{input-
databases}}",
                "arn:aws:glue:us-east-1:444455556666:table/{{input-
database}}/{{input-tables}}",
                "arn:aws:glue:us-east-1:444455556666:catalog"
            ]
        }
    ]
}
```

Ersetzen Sie jeden *{{user input placeholder}}* durch Ihre Informationen.

aws-region	AWS-Region Ihrer Ressourcen. Sie können Amazon S3 und AWS KMS Ressourcen von allen kommerziellen Anbietern verwenden AWS Glue, in AWS-Region denen diese Dienste unterstützt werden.
&ExampleAWSAccountNo1;	Ihre AWS-Konto ID.
input-buckets	Amazon S3 S3-Buckets, die die zugrunde liegenden Datenobjekte enthalten AWS Glue , aus denen gelesen `AWS Entity Resolution` werden soll.
output-buckets	Amazon S3 S3-Buckets, in denen die Ausgabedaten generiert `AWS Entity Resolution` werden.
input-databases	AWS Glue Datenbanken, aus denen gelesen `AWS Entity Resolution` wird.

b. (Optional) Wenn der eingegebene Amazon S3 S3-Bucket mit dem KMS-Schlüssel des Kunden verschlüsselt ist, fügen Sie Folgendes hinzu:

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{aws-
region}}:{{&ExampleAWSAccountNo1;}}:key/{{inputKeys}}"
            ]
        }
```

Ersetzen Sie jeden *{{user input placeholder}}* durch Ihre Informationen.

aws-region	AWS-Region Ihrer Ressourcen. Sie können Amazon S3 und AWS KMS Ressourcen von allen kommerziellen Anbietern verwenden AWS Glue, in AWS-Region denen diese Dienste unterstützt werden.
&ExampleAWSAccountNo1;	Ihre AWS-Konto ID.
inputKeys	Verwaltete Schlüssel rein AWS Key Management Service. Wenn Ihre Eingabequellen verschlüsselt sind, AWS `Entity Resolution` müssen Sie Ihre Daten mit Ihrem Schlüssel entschlüsseln.

c. (Optional) Wenn die Daten, die in den Amazon S3 S3-Ausgabe-Bucket geschrieben werden, verschlüsselt werden müssen, fügen Sie Folgendes hinzu:

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Encrypt"
            ],
            "Resource": [
                "arn:aws:kms:{{aws-
region}}:{{&ExampleAWSAccountNo1;}}:key/{{outputKeys}}"
            ]
        }
```

Ersetzen Sie jeden *{{user input placeholder}}* durch Ihre Informationen.

aws-region	AWS-Region Ihrer Ressourcen. Sie können Amazon S3 und AWS KMS Ressourcen von allen kommerziellen Anbietern verwenden AWS Glue, in AWS-Region denen diese Dienste unterstützt werden.
&ExampleAWSAccountNo1;	Ihre AWS-Konto ID.
outputKeys	Verwaltete Schlüssel rein AWS Key Management Service. Wenn Sie möchten, dass Ihre Ausgabequellen verschlüsselt werden, `AWS Entity Resolution` müssen Sie die Ausgabedaten mit Ihrem Schlüssel verschlüsseln.

d. (Optional) Wenn Sie über AWS Data Exchange ein Abonnement bei einem Provider-Service verfügen und eine vorhandene Rolle für einen auf einem Provider-Service basierenden Workflow verwenden möchten, fügen Sie Folgendes hinzu:

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

Ersetzen Sie jeden *{{user input placeholder}}* durch Ihre Informationen.

aws-region	Der AWS-Region Ort, an dem die Anbieterr essource gewährt wird. Sie finden diesen Wert im Asset-ARN auf der AWS Data Exchange Konsole. Beispiel: `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
datasetId	Die ID des Datensatzes, die sich auf der AWS Data Exchange Konsole befindet.
revisionId	Die Revision des Datensatzes, gefunden auf der AWS Data Exchange Konsole.
assetId	Die ID des Assets, gefunden auf der AWS Data Exchange Konsole.

8. Kehren Sie zu Ihrer ursprünglichen Registerkarte zurück und geben Sie unter Berechtigungen hinzufügen den Namen der Richtlinie ein, die Sie gerade erstellt haben. (Möglicherweise müssen Sie die Seite neu laden.)
9. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die Sie erstellt haben, und klicken Sie dann auf Weiter.
10. Geben Sie unter Name, review and create den Rollennamen und die Beschreibung ein.

> **Note**
>
> Der Rollenname muss mit dem Muster in den `passRole` Berechtigungen übereinstimmen, die dem Mitglied erteilt wurden, das den `workflow job role` zum Erstellen eines passenden Workflows weiterreichen kann.
> Wenn Sie beispielsweise die `AWSEntityResolutionConsoleFullAccess` verwaltete Richtlinie verwenden, denken Sie daran, diesen Namen `entityresolution` in Ihren Rollennamen aufzunehmen.

a. Überprüfen Sie die Option Vertrauenswürdige Entitäten auswählen und bearbeiten Sie sie gegebenenfalls.
b. Überprüfen Sie die Berechtigungen unter Berechtigungen hinzufügen und bearbeiten Sie sie gegebenenfalls.
c. Überprüfen Sie die Tags und fügen Sie bei Bedarf Stichwörter hinzu.
d. Wählen Sie Rolle erstellen aus.

Die Workflow-Jobrolle für AWS Entity Resolution wurde erstellt.

Eingabedatentabellen vorbereiten

In AWS Entity Resolution enthält jede Ihrer Eingabedatentabellen Quelldatensätze. Diese Datensätze enthalten Verbraucher-Identifikatoren wie Vorname, Nachname, E-Mail-Adresse oder Telefonnummer. Diese Quelldatensätze können mit anderen Quelldatensätzen abgeglichen werden, die Sie in derselben oder anderen Eingabedatentabellen angeben. Jeder Datensatz muss eine eindeutige Datensatz-ID (Eindeutige ID) haben, und Sie müssen ihn als Primärschlüssel definieren, während Sie darin eine Schemazuordnung erstellen AWS Entity Resolution.

Jede Eingabedatentabelle ist als AWS Glue Tabelle verfügbar, die von Amazon S3 unterstützt wird. Sie können Ihre Erstanbieterdaten bereits in Amazon S3 verwenden oder Datentabellen von anderen SaaS-Drittanbietern in Amazon S3 importieren. Nachdem Sie die Daten auf Amazon S3 hochgeladen haben, können Sie einen AWS Glue Crawler verwenden, um eine Datentabelle in der AWS Glue Data Catalog zu erstellen. Anschließend können Sie die Datentabelle als Eingabe für verwenden. AWS Entity Resolution

In den folgenden Abschnitten wird beschrieben, wie Daten von Erstanbietern und Daten von Drittanbietern vorbereitet werden.

Themen

- Vorbereiten von Eingabedaten von Erstanbietern
- Vorbereiten von Eingabedaten von Drittanbietern

Vorbereiten von Eingabedaten von Erstanbietern

In den folgenden Schritten wird beschrieben, wie Sie Daten von Erstanbietern für die Verwendung in einem regelbasierten Abgleichsworkflow, einem auf maschinellem Lernen basierenden Abgleichsworkflowoder einem ID-Mapping-Workflow vorbereiten.

Schritt 1: Bereiten Sie Datentabellen von Erstanbietern vor

Für jeden passenden Workflowtyp gibt es unterschiedliche Empfehlungen und Richtlinien, um den Erfolg sicherzustellen.

Informationen zur Erstellung von Datentabellen von Erstanbietern finden Sie in der folgenden Tabelle:

First-party Richtlinien für Datentabellen

Workflow-Typ	Erforderlich

Rule-based Abgleich des Workflows mit dem Regeltyp „Erweitert“	• Eine eindeutige ID ist erforderlich.
	• Die eindeutige ID umfasst nicht mehr als 38 Zeichen.
	• (Optional) Eine DELETE-Spalte, die angibt, aus welchen Datensätzen entfernt werden sollen, AWS Entity Resolution nachdem der Workflow die Verarbeitung abgeschlossen hat. Der Standardwert ist`false`, wenn die Spalte ohne Werte existiert. Datensätze, bei denen die DELETE-Spalte auf gesetzt ist, `true` werden gelöscht. Datensätze, bei denen die DELETE-Spalte auf `false` oder leer gesetzt ist, werden von verarbeitet AWS Entity Resolution.
	
	Das Schema muss eine DELETE-Spalte mit dem Typ `String` und ohne `matchKey` und enthalten`groupName` .
	
	Note
	Das Nachschlagen der Match-ID (`GetMatchID`) wird nicht unterstützt, da der Regeltyp „Erweitert“ für den manuellen Verarbeitungsrhythmus keine aufgenommenen Daten speichert.
	
	Im folgenden Beispiel `S1` werden sie aufgenommen und `S2` gelöscht.
	
	Example
	
	`sourceID, name, lastName, DELETE`
	`S1, name, lastname, false`
	`S2, name2, lastname2, true`

regelbasierter Abgleichs -Workflow mit einfachem Regeltyp	• Eine eindeutige ID ist erforderlich. • Die eindeutige ID umfasst nicht mehr als 38 Zeichen.

Workflow-Typ	Erforderlich

Auf maschinellem Lernen basierender Matching-Workflow	• Eine eindeutige ID ist erforderlich.
	• Der Datensatz enthält einen der folgenden Typen:
	  • **`Full Name`**
	  • **`Full Address`**
	  • **`Full phone`**
	  • **`Email address`**
	  • **`Date`**— mit dem Match-Schlüsselnamen Geburtsdatum
	• Keiner der Spaltennamen verwendet die folgenden reservierten Namen: "`MatchId`„," `MatchRule` „,`RecordId`, `SourceId` „," und`TargetId`“.
	• (Optional) Eine DELETE-Spalte, die angibt, aus welchen Datensätzen gelöscht werden sollen, AWS Entity Resolution nachdem der Workflow die Verarbeitung abgeschlossen hat. Der Standardwert ist*`false`*, wenn die Spalte ohne Werte existiert. Datensätze, bei denen die DELETE-Spalte auf gesetzt ist, *`true`* werden gelöscht. Datensätze, bei denen die DELETE-Spalte auf *`false`* oder leer gesetzt ist, werden von verarbeitet AWS Entity Resolution.
	
	Das Schema muss eine DELETE-Spalte mit dem Typ `String` und ohne `matchKey` und enthaltengroupName .
	
	Im folgenden Beispiel `S1` wird sie aufgenommen und `S2` gelöscht.
	
	Example
	
	`sourceID, name, lastName, DELETE`
	`S1, name, lastname, false`
	`S2, name2, lastname2, true`

Workflow-Typ	Erforderlich

Arbeitsablauf bei der ID-Zuordnung	• Eine eindeutige ID ist erforderlich.
	• Die eindeutige ID umfasst nicht mehr als 257 Zeichen.
	• (Optional) Eine DELETE-Spalte, die angibt, aus welchen Datensätzen entfernt werden sollen, AWS Entity Resolution nachdem der Workflow die Verarbeitung abgeschlossen hat. Der Standardwert ist`false`, wenn die Spalte ohne Werte existiert. Datensätze, bei denen die DELETE-Spalte auf gesetzt ist, `true` werden gelöscht. Datensätze, bei denen die DELETE-Spalte auf `false` oder leer gesetzt ist, werden von verarbeitet AWS Entity Resolution.
	
	Das Schema muss eine DELETE-Spalte mit dem Typ `String` und ohne `matchKey` und enthalten`groupName` .
	
	Im folgenden Beispiel `S1` wird sie aufgenommen und `S2` gelöscht.
	
	Example
	
	`sourceID, name, lastName, DELETE`
	`S1, name, lastname, false`
	`S2, name2, lastname2, true`

Schritt 2: Speichern Sie Ihre Eingabedatentabelle in einem unterstützten Datenformat

Wenn Sie Ihre Eingabedaten von Erstanbietern bereits in einem unterstützten Datenformat gespeichert haben, können Sie diesen Schritt überspringen.

Um sie verwenden zu können AWS Entity Resolution, müssen die Eingabedaten in einem Format vorliegen, das AWS Entity Resolution unterstützt.

AWS Entity Resolution unterstützt die folgenden Datenformate:

- Kommagetrennter Wert (CSV)
- Parquet

Schritt 3: Laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch

Wenn Sie Ihre First-Party-Datentabelle bereits in Amazon S3 haben, können Sie diesen Schritt überspringen.

> **Note**
>
> Sie können die Eingabedaten in Amazon S3Resources in jeder Region der AWS kommerziellen Partition speichern, in der S3 unterstützt wird. Auf diese Daten kann aus einer anderen Region oder AWS-Konto bei der Ausführung des passenden Workflows zugegriffen werden.

So laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Buckets und dann einen Bucket zum Speichern Ihrer Datentabelle aus.
3. Wählen Sie Hochladen und folgen Sie dann den Anweisungen.
4. Wählen Sie die Registerkarte Objekte, um das Präfix anzuzeigen, in dem Ihre Daten gespeichert sind. Notieren Sie sich den Namen des Ordners.

   Sie können den Ordner auswählen, um die Datentabelle anzuzeigen.

Schritt 4: Erstellen Sie ein AWS Glue Tabelle

> **Note**
>
> Wenn Sie partitionierte AWS Glue Tabellen benötigen, fahren Sie mit Schritt 4: Erstellen Sie eine partitionierte AWS Glue Tabelle fort.

Die Eingabedaten in Amazon S3 müssen katalogisiert AWS Glue und als AWS Glue Tabelle dargestellt werden. Weitere Informationen zum Erstellen einer AWS Glue Tabelle mit Amazon S3 als Eingabe finden Sie unter Arbeiten mit Crawlern auf der AWS Glue Konsole im AWS Glue Entwicklerhandbuch.

In diesem Schritt richten Sie einen Crawler ein, der alle Dateien in AWS Glue Ihrem S3-Bucket crawlt und eine Tabelle erstellt. AWS Glue

> **Note**
>
> AWS Entity Resolution unterstützt derzeit keine Amazon S3 S3-Standorte, bei denen Sie registriert sind AWS Lake Formation.

Um ein zu erstellen AWS Glue Tabelle

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die AWS Glue Konsole unter https://console.aws.amazon.com/glue/.
2. Wählen Sie in der Navigationsleiste Crawlers aus.
3. Wählen Sie Ihren S3-Bucket aus der Liste aus und wählen Sie dann Crawler erstellen aus.
4. Geben Sie auf der Seite „Crawler-Eigenschaften festlegen“ einen Crawler-Namen und eine optionale Beschreibung ein und wählen Sie dann Weiter aus.
5. Fahren Sie mit der Seite Crawler hinzufügen fort und geben Sie die Details an.
6. Wählen Sie auf der Seite „IAM-Rolle auswählen“ die Option Vorhandene IAM-Rolle auswählen aus und klicken Sie dann auf Weiter.

   Sie können bei Bedarf auch eine IAM-Rolle erstellen wählen oder Ihren Administrator die IAM-Rolle erstellen lassen.
7. Behalten Sie unter Einen Zeitplan für diesen Crawler erstellen die Standardeinstellung Frequenz (Bei Bedarf ausführen) bei und wählen Sie dann Weiter aus.
8. Geben Sie für Configure the Crawler's output die AWS Glue Datenbank ein und wählen Sie dann Next aus.
9. Überprüfen Sie alle Details und wählen Sie dann Fertig stellen.
10. Aktivieren Sie auf der Seite Crawler das Kontrollkästchen neben Ihrem S3-Bucket und wählen Sie dann Crawler ausführen aus.
11. Nachdem der Crawler fertig ausgeführt wurde, wählen Sie in der AWS Glue Navigationsleiste Datenbanken und dann Ihren Datenbanknamen aus.
12. Wählen Sie auf der Datenbankseite Tabellen in {Ihr Datenbankname} aus.

    a. Sehen Sie sich die Tabellen in der AWS Glue Datenbank an.

    b. Um das Schema einer Tabelle anzuzeigen, wählen Sie eine bestimmte Tabelle aus.

c. Notieren Sie sich den AWS Glue Datenbanknamen und den AWS Glue Tabellennamen.

Sie sind jetzt bereit, ein Schema-Mapping zu erstellen. Weitere Informationen finden Sie unter Eine Schemazuordnung erstellen.

Schritt 4: Erstellen Sie eine partitionierte AWS Glue Tabelle

> **Note**
>
> Die AWS Glue Partitionierungsfunktion in AWS Entity Resolution wird nur in Workflows zur ID-Zuordnung unterstützt. Mit dieser AWS Glue Partitionierungsfunktion können Sie bestimmte Partitionen für die Verarbeitung auswählen. AWS Entity Resolution
> Wenn Sie keine partitionierten AWS Glue Tabellen benötigen, können Sie diesen Schritt überspringen.

Eine partitionierte AWS Glue Tabelle spiegelt automatisch neue Partitionen in der AWS Glue Tabelle wider, wenn Sie der Datenstruktur neue Ordner hinzufügen (z. B. einen neuen Tagesordner unter einem Monat).

Wenn Sie eine partitionierte AWS Glue Tabelle erstellen, können Sie angeben AWS Entity Resolution, welche Partitionen Sie in einem ID-Zuordnungs-Workflow verarbeiten möchten. Jedes Mal, wenn Sie den ID-Zuordnungs-Workflow ausführen, werden dann nur die Daten in diesen Partitionen verarbeitet, nicht alle Daten in der gesamten AWS Glue Tabelle. Diese Funktion ermöglicht eine genauere, effizientere und kostengünstigere Datenverarbeitung und bietet Ihnen mehr Kontrolle und Flexibilität bei der Verwaltung Ihrer Aufgaben zur Entitätsauflösung. AWS Entity Resolution

Sie können in einem ID-Zuordnungs-Workflow eine partitionierte AWS Glue Tabelle für das Quellkonto erstellen.

Sie müssen zuerst die Eingabedaten in Amazon S3 katalogisieren AWS Glue und als AWS Glue Tabelle darstellen. Weitere Informationen zum Erstellen einer AWS Glue Tabelle mit Amazon S3 als Eingabe finden Sie unter Arbeiten mit Crawlern auf der AWS Glue Konsole im AWS Glue Entwicklerhandbuch.

In diesem Schritt richten Sie einen Crawler ein, der alle Dateien in AWS Glue Ihrem S3-Bucket crawlt und dann eine partitionierte Tabelle erstellt. AWS Glue

> **Note**
>
> AWS Entity Resolution unterstützt derzeit keine Amazon S3 S3-Standorte, bei denen Sie registriert sind AWS Lake Formation.

Um eine partitionierte zu erstellen AWS Glue Tabelle

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Glue Konsole unter https://console.aws.amazon.com/glue/.
2. Wählen Sie in der Navigationsleiste Crawlers aus.
3. Wählen Sie Ihren S3-Bucket aus der Liste aus und wählen Sie dann Crawler erstellen aus.
4. Geben Sie auf der Seite „Crawler-Eigenschaften festlegen“ einen Crawler-Namen und optional eine Beschreibung ein und wählen Sie dann Weiter aus.
5. Fahren Sie mit der Seite Crawler hinzufügen fort und geben Sie die Details an.
6. Wählen Sie auf der Seite „IAM-Rolle auswählen“ die Option Vorhandene IAM-Rolle auswählen aus und klicken Sie dann auf Weiter.

   Sie können bei Bedarf auch eine IAM-Rolle erstellen wählen oder Ihren Administrator die IAM-Rolle erstellen lassen.
7. Behalten Sie unter Einen Zeitplan für diesen Crawler erstellen die Standardeinstellung Frequenz (Bei Bedarf ausführen) bei und wählen Sie dann Weiter aus.
8. Geben Sie für Configure the Crawler's output die AWS Glue Datenbank ein und wählen Sie dann Next aus.
9. Überprüfen Sie alle Details und wählen Sie dann Fertig stellen.
10. Aktivieren Sie auf der Seite Crawler das Kontrollkästchen neben Ihrem S3-Bucket und wählen Sie dann Crawler ausführen aus.
11. Nachdem der Crawler fertig ausgeführt wurde, wählen Sie in der AWS Glue Navigationsleiste Datenbanken und dann Ihren Datenbanknamen aus.
12. Wählen Sie auf der Datenbankseite unter Tabellen die Tabelle aus, die partitioniert werden soll.
13. Wählen Sie in der Tabellenübersicht die Dropdownliste Aktionen aus und wählen Sie dann Tabelle bearbeiten aus.

    a. Wählen Sie unter Tabelleneigenschaften die Option Hinzufügen aus.

b. Geben Sie für den neuen Schlüssel ein**`aerPushDownPredicateString`**.

c. Geben Sie für den neuen Wert ein**`'<PartitionKey>=<PartitionValue'`**.

d. Notieren Sie sich den AWS Glue Datenbanknamen und den AWS Glue Tabellennamen.

Sie sind jetzt bereit für:

- Erstellen Sie ein Schema-Mapping und dann einen ID-Mapping-Workflow für ein solches AWS-Konto.
- Erstellen Sie eine ID-Namespace-Quelle, erstellen Sie ein ID-Namespace-Ziel und erstellen Sie dann einen ID-Zuordnungs-Workflow für zwei. AWS-Konten

Vorbereiten von Eingabedaten von Drittanbietern

Third-party Datendienste stellen Identifikatoren bereit, die Ihren bekannten Kennungen zugeordnet werden können.

AWS Entity Resolution unterstützt derzeit die folgenden Dienste von Drittanbietern von Datenanbietern:

Dienste von Datenanbietern

Name des Unternehmens	Verfügbar AWS-Regionen	Kennung
LiveRamp	USA Ost (Nord-Virginia) (us-east-1), USA Ost (Ohio) (us-east-2) und USA West (Oregon) (US-West-2)	Rampen-ID
TransUnion	USA Ost (Nord-Virginia) (us-east-1), USA Ost (Ohio) (us-east-2) und USA West (Oregon) (US-West-2)	TransUnion Ausweise für Einzelpersonen und Haushalte
Einheitliche ID 2.0	USA Ost (Nord-Virginia) (us-east-1), USA Ost (Ohio) (us-east-2) und USA West (Oregon) (US-West-2)	unformatierte UID 2

In den folgenden Schritten wird beschrieben, wie Drittanbieterdaten für die Verwendung eines auf Provider-Services basierenden Matching-Workflows oder eines ID-Zuordnungs-Workflows auf Anbieterservice-Basis vorbereitet werden.

Themen

- Schritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange
- Schritt 2: Bereite Datentabellen von Drittanbietern vor
- Schritt 3: Speichern Sie Ihre Eingabedatentabelle in einem unterstützten Datenformat
- Schritt 4: Laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch
- Schritt 5: Erstellen Sie ein AWS Glue Tabelle

Schritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange

Wenn Sie ein Abonnement bei einem Anbieterdienst abgeschlossen haben AWS Data Exchange, können Sie einen Abgleichsworkflow mit einem der folgenden Anbieterdienste ausführen, um Ihre bekannten Kennungen mit Ihrem bevorzugten Anbieter abzugleichen. Ihre Daten werden mit einer Reihe von Eingaben abgeglichen, die von Ihrem bevorzugten Anbieter definiert wurden.

Um einen Anbieterdienst zu abonnieren auf AWS Data Exchange

1. Sehen Sie sich die Anbieterliste unter an AWS Data Exchange. Die folgenden Anbieterlisten sind verfügbar:
   - LiveRamp
     - LiveRampAuflösung der Identität
     - LiveRampTranscodierung
   - TransUnion
     - TruAudience Auflösung und Anreicherung von Identitäten
   - Einheitliche ID 2.0
     - Einheitliche ID 2.0-Identitätslösung
2. Führen Sie je nach Angebotstyp einen der folgenden Schritte aus.
   - Privates Angebot — Wenn Sie bereits eine Geschäftsbeziehung mit einem Anbieter haben, folgen Sie dem Verfahren für private Produkte und Angebote im AWS Data Exchange Benutzerhandbuch, um ein privates Angebot anzunehmen AWS Data Exchange.

- Bringen Sie Ihr eigenes Abonnement mit — Wenn Sie bereits ein bestehendes Datenabonnement bei einem Anbieter haben, folgen Sie dem Verfahren für BYOS-Angebote (Bring Your Own Subscription) im AWS Data Exchange Benutzerhandbuch, um ein BYOS-Angebot anzunehmen. AWS Data Exchange

3. Nachdem Sie einen Provider-Service am abonniert haben AWS Data Exchange, können Sie einen passenden Workflow oder einen ID-Mapping-Workflow mit diesem Provider-Service erstellen.

Weitere Informationen zum Zugriff auf ein Anbieterprodukt, das APIs enthält, finden Sie unter Zugreifen auf ein API-Produkt im im AWS Data Exchange Benutzerhandbuch.

Schritt 2: Bereite Datentabellen von Drittanbietern vor

Für jeden Drittanbieter-Service gelten unterschiedliche Empfehlungen und Richtlinien, um einen erfolgreichen Matching-Workflow sicherzustellen.

Informationen zur Erstellung von Datentabellen von Drittanbietern finden Sie in der folgenden Tabelle:

Richtlinien für Dienste von Datenanbietern

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen
LiveRamp	Ja	Stellen Sie Folgendes sicher: • Die eindeutige ID kann entweder Ihre eigene pseudonyme Kennung oder eine Zeilen-ID sein. • Das Format und die Normalisierung Ihrer Dateneingabedatei entsprechen den Richtlinien. LiveRamp Weitere Informationen zu den Richtlinien für die Formatierung von Eingabedateien für den Abgleichs-Workflow finden Sie in der Dokumentation unter Perform Identity Resolution Through ADX. LiveRamp

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen
		Weitere Informationen zu den Richtlinien zur Formatierung von Eingabedateien für den Workflow zur ID-Zuordnung finden Sie in der Dokumentation unter Perform Transcoding Through ADX. LiveRamp

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen

TransUnion	Ja	Stellen Sie sicher, dass es sich bei den folgenden Spalten um eine `string` Typspalte in der Eingabeansicht handelt:
		• Eine eindeutige ID ist erforderlich und kann eine CRM-ID, eine Kontakt-ID, eine Benutzer-ID oder eine beliebige eindeutige ID sein.
		• **`Name`**
		  • **`First Name`**kann in Klein- oder Großbuchstaben geschrieben werden, Spitznamen werden unterstützt, Titel und Suffixe sollten jedoch ausgeschlossen werden.
		  • **`Last Name`**können Klein- oder Großbuchstaben sein, mittlere Initialen sollen ausgeschlossen werden.
		• **`Address`**
		  • **`Street address1`**und **`Street address1`** wird zu einer einzigen **`Full address`** Zeile zusammengefasst, falls vorhanden.
		  • **`City`**ist getrennt von**`Full address`**.
		  • **`Zip`**(oder**`zip plus4`**), ohne Sonderzei chen wie Leerzeichen, Bindestriche oder Leerzeichen. Verwenden Sie Nullen, wenn keine Daten vorhanden sind.
		  • **`State`**wird als 2-Buchstaben-Code in Großbuchstaben angegeben.
		• • **`Phone`**

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen

		• **`Phone number`**sollte aus 10 Ziffern bestehen, ohne Sonderzeichen wie Leerzeichen oder Bindestriche.
		• **`Email addresses`** ist entweder Klartext oder Zeichenketten in SHA256-hashed Kleinbuchstaben.
		• **`Date of Birth`**ist im `yyy-mm-dd` Y-Format.
		• **`Digital identifiers`** (Geräte-IDs) können IDs mit Bindestrichen (unformat iertes Gerät mit 36 Zeichen IDs/MAIDs/ IFAs) und ohne Bindestriche (32 und 40 Zeichen langes Hash-Gerät) enthalten. IDs/ MAIDs/IFAs
		  • **`IPV4`**ist eine 32-Bit-IP-Adresse, ausgedrückt in punktierter Dezimalsc hreibweise. Beispiel: `192.0.2.1`
		  • **`IPV6`**ist eine 128-Bit-IP-Adresse, ausgedrückt in hexadezimaler Schreibwe ise, getrennt durch Doppelpunkte. Beispiel: `2001:db8:0000:0000 :0000:0000:0000:0001`
		  • **`MAID`**(Mobile Advertising ID) ist eine eindeutige, alphanumerische Zeichenfo lge, die einem Mobilgerät zu Werbezwec ken zugewiesen wird. Ein Dienstmädchen besteht normalerweise aus 36 Zeichen. Beispiel: `a1b2c3d4-5678-90ab- cdef-EXAMPLE11111`

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen
Vereinheitlichte ID 2.0	Ja	Stellen Sie Folgendes sicher: • Die eindeutige ID darf kein Hash sein. • Entweder **`Phone number`** oder **`Email addresses`** wird im Schema verwendet, nicht beide. • UID2 unterstützt sowohl E-Mail als auch Telefonnummer für die UID2-Generierung. Wenn jedoch beide Werte in der Schemazuordnung vorhanden sind, dupliziert der Workflow jeden Datensatz in der Ausgabe. Ein Datensatz verwendet die E-Mail für die UID2-Generierung und der zweite Datensatz verwendet die Telefonnummer. Wenn Ihre Daten eine Mischung aus E-Mails und Telefonnummern enthalten und Sie diese doppelte Anzahl von Datensätzen in der Ausgabe vermeiden möchten, ist es am besten, für jeden einen eigenen Workflow mit separaten Schemazuordnungen zu erstellen. Führen Sie in diesem Szenario die Schritte zweimal durch: Erstellen Sie einen Workflow für E-Mails und einen separaten für Telefonnummern. **Note** Eine bestimmte E-Mail oder Telefonnummer zu einem bestimmten Zeitpunkt führt zu demselben UID2-Rohwert, unabhängig davon, wer die Anfrage gestellt hat.

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen
		Roh-UID2-Werte werden durch Zugabe von Salzen aus Salzkübel n erzeugt, die etwa einmal pro Jahr rotiert werden, sodass auch die Roh-UID2 mit rotiert wird. Verschiedene Salzkübel wechseln im Laufe des Jahres zu unterschiedlichen Zeiten. AWS Entity Resolution verfolgt derzeit nicht die rotierenden Salzeimer und Roh-UID2. Es wird daher empfohlen , die rohen UID2 täglich zu regenerie ren. Weitere Informationen finden Sie unter Wie oft sollten UID2s für inkrementelle Updates aktualisi ert werden? in der UID 2.0-Dokum entation.

Schritt 3: Speichern Sie Ihre Eingabedatentabelle in einem unterstützten Datenformat

Wenn Sie Ihre Eingabedaten von Drittanbietern bereits in einem unterstützten Datenformat gespeichert haben, können Sie diesen Schritt überspringen.

Um sie verwenden zu können AWS Entity Resolution, müssen die Eingabedaten in einem Format vorliegen, das AWS Entity Resolution unterstützt.

AWS Entity Resolution unterstützt die folgenden Datenformate:

- Kommagetrennter Wert (CSV)

> **Note**
>
> LiveRamp unterstützt nur CSV-Dateien.

- Parquet

Schritt 4: Laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch

Wenn Sie Ihre Drittanbieter-Datentabelle bereits in Amazon S3 haben, können Sie diesen Schritt überspringen.

> **Note**
>
> Sie können die Eingabedaten in Amazon S3 S3-Ressourcen in jeder Region der AWS kommerziellen Partition speichern, in der S3 unterstützt wird. Auf diese Daten kann aus einer anderen Region oder AWS-Konto bei der Ausführung des passenden Workflows zugegriffen werden.

So laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Buckets und dann einen Bucket zum Speichern Ihrer Datentabelle aus.
3. Wählen Sie Hochladen und folgen Sie dann den Anweisungen.
4. Wählen Sie die Registerkarte Objekte, um das Präfix anzuzeigen, in dem Ihre Daten gespeichert sind. Notieren Sie sich den Namen des Ordners.

   Sie können den Ordner auswählen, um die Datentabelle anzuzeigen.

Schritt 5: Erstellen Sie ein AWS Glue Tabelle

Die Eingabedaten in Amazon S3 müssen katalogisiert AWS Glue und als AWS Glue Tabelle dargestellt werden. Weitere Informationen zum Erstellen einer AWS Glue Tabelle mit Amazon S3 als Eingabe finden Sie unter Arbeiten mit Crawlern auf der AWS Glue Konsole im AWS Glue Entwicklerhandbuch.

> **Note**
>
> AWS Entity Resolution unterstützt keine partitionierten Tabellen.

In diesem Schritt richten Sie einen Crawler ein, der alle Dateien in AWS Glue Ihrem S3-Bucket crawlt und eine Tabelle erstellt. AWS Glue

> **Note**
>
> AWS Entity Resolution unterstützt derzeit keine Amazon S3 S3-Standorte, bei denen Sie registriert sind AWS Lake Formation.

Um ein zu erstellen AWS Glue Tabelle

1. Melden Sie sich bei an AWS-Managementkonsole und öffnen Sie die AWS Glue Konsole unter https://console.aws.amazon.com/glue/.
2. Wählen Sie in der Navigationsleiste Crawlers aus.
3. Wählen Sie Ihren S3-Bucket aus der Liste aus und klicken Sie dann auf Crawler hinzufügen.
4. Geben Sie auf der Seite Crawler hinzufügen einen Crawler-Namen ein und wählen Sie dann Weiter aus.
5. Fahren Sie mit der Seite Crawler hinzufügen fort und geben Sie die Details an.
6. Wählen Sie auf der Seite „IAM-Rolle auswählen“ die Option Vorhandene IAM-Rolle auswählen aus und klicken Sie dann auf Weiter.

   Sie können bei Bedarf auch eine IAM-Rolle erstellen wählen oder Ihren Administrator die IAM-Rolle erstellen lassen.
7. Behalten Sie unter Einen Zeitplan für diesen Crawler erstellen die Standardeinstellung Frequenz (Bei Bedarf ausführen) bei und wählen Sie dann Weiter aus.
8. Geben Sie für Configure the Crawler's output die AWS Glue Datenbank ein und wählen Sie dann Next aus.
9. Überprüfen Sie alle Details und wählen Sie dann Fertig stellen.
10. Aktivieren Sie auf der Seite Crawler das Kontrollkästchen neben Ihrem S3-Bucket und wählen Sie dann Crawler ausführen aus.
11. Nachdem der Crawler fertig ausgeführt wurde, wählen Sie in der AWS Glue Navigationsleiste Datenbanken und dann Ihren Datenbanknamen aus.
12. Wählen Sie auf der Datenbankseite Tabellen in {Ihr Datenbankname} aus.

    a. Sehen Sie sich die Tabellen in der AWS Glue Datenbank an.

    b. Um das Schema einer Tabelle anzuzeigen, wählen Sie eine bestimmte Tabelle aus.

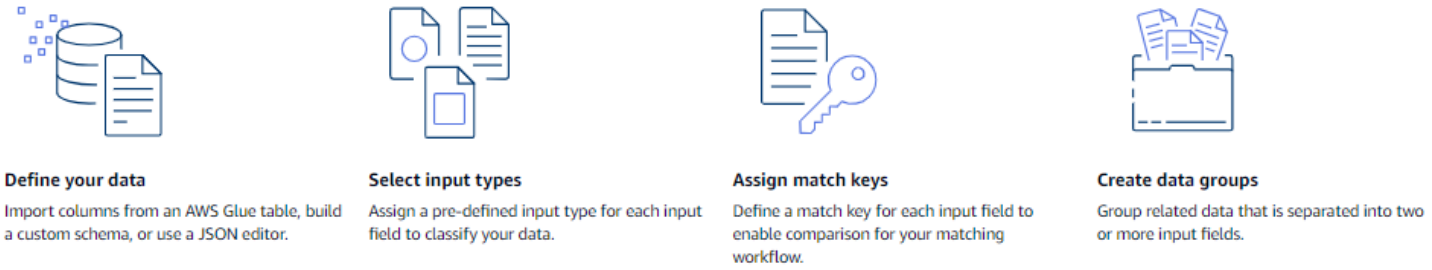
c. Notieren Sie sich den AWS Glue Datenbanknamen und den AWS Glue Tabellennamen.

Sie sind jetzt bereit, ein Schema-Mapping zu erstellen. Weitere Informationen finden Sie unter Eine Schemazuordnung erstellen.

Definieren Sie Eingabedaten mithilfe von Schema-Mapping

Eine Schemazuordnung definiert die Eingabedaten, die Sie auflösen möchten. Es stellt auch Metadaten zu den Eingabedaten bereit, z. B. die Attributtypen der Spalten (Eingabefelder) und welche Spalten zugeordnet werden sollen.

Wenn Sie ein Schema-Mapping erstellen, definieren Sie zuerst Ihre Eingabefelder und Attributtypen und dann Ihre Abgleichsschlüssel und gruppenbezogenen Daten. Das folgende Diagramm fasst zusammen, wie Sie ein Schema-Mapping erstellen.



Bevor Sie ein Schema-Mapping erstellen, müssen Sie zuerst Ihre Datentabellen einrichten AWS Entity Resolution und vorbereiten. Weitere Informationen erhalten Sie unter Einrichten AWS Entity Resolution und Eingabedatentabellen vorbereiten.

Nachdem Sie eine Schemazuordnung erstellt haben, können Sie einen der folgenden Schritte ausführen:

- Erstellen Sie einen passenden Workflow, um Übereinstimmungen zwischen verschiedenen Dateneingaben zu finden.
- Erstellen Sie eine ID-Namespace-Quelle, die Sie in einem ID-Mapping-Workflow verwenden können, um Daten von einer Quelle in ein Ziel zu übersetzen.
- Erstellen Sie innerhalb desselben Workflows einen ID-Mapping-Workflow, AWS-Konto indem Sie Ihre Schemazuordnung als Quelle verwenden.

Themen

- Eine Schemazuordnung erstellen
- Klonen einer Schemazuordnung
- Eine Schemazuordnung bearbeiten
- Löschen einer Schemazuordnung

Eine Schemazuordnung erstellen

Dieses Verfahren beschreibt den Prozess der Erstellung einer Schemazuordnung mithilfe der AWS Entity Resolution Konsole.

Es gibt drei Möglichkeiten, eine Schemazuordnung zu erstellen:

- Importieren vorhandener Eingabedaten mit der AWS Glue Option Import von — Verwenden Sie diese Erstellungsmethode, um Eingabefelder, die mit vorab ausgefüllten Spalten aus einer AWS Glue Tabelle beginnen, mithilfe eines geführten Ablaufs zu definieren.
- Manuelles Definieren von Eingabedaten mithilfe der Option Benutzerdefiniertes Schema erstellen — Verwenden Sie diese Erstellungsmethode, um die Eingabefelder mithilfe eines geführten Ablaufs manuell zu definieren.
- Manuell mit der Option JSON-Editor verwenden erstellen — Verwenden Sie einen JSON-Editor, um manuell Eingabedaten zu erstellen, ein Beispiel zu verwenden oder vorhandene Eingabedaten zu importieren.

> **Note**
>
> Die Felder „Eindeutige ID“ und „Eingabe“ sind bei dieser Option nicht verfügbar.

Import from AWS Glue

Um eine Schemazuordnung zu erstellen, indem Sie vorhandene Eingabedaten importieren von AWS Glue

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie auf der Seite Schemazuordnungen in der oberen rechten Ecke die Option Schema-Mapping erstellen aus.
4. Gehen Sie für Schritt 1: Schemadetails angeben wie folgt vor:

    a. Geben Sie unter Name und Erstellungsmethode einen Namen für die Schemazuordnung und optional eine Beschreibung ein.

b. Wählen Sie als Erstellungsmethode die Option Import von aus AWS Glue.

c. Wählen Sie das Symbol AWS-Region.

d. Wählen Sie die AWS Glue Datenbank aus.

e. Wählen Sie die AWS Glue Tabelle aus.

   Um eine neue Tabelle zu erstellen, gehen Sie zur AWS Glue Konsole https://console.aws.amazon.com/glue/. Weitere Informationen finden Sie in den AWS Glue Tabellen im AWS Glue Benutzerhandbuch.

f. Geben Sie für Unique ID die Spalte an, die eindeutig auf jede Zeile Ihrer Daten verweist.

   Example

   Beispiel: **`Primary_key`**, **`Row_ID`** oder **`Record_ID`**.

   > **Note**
   >
   > Die Spalte „Eindeutige ID“ ist erforderlich. Die eindeutige ID muss ein eindeutiger Bezeichner innerhalb einer einzelnen Tabelle sein. In verschiedenen Tabellen kann die Unique ID jedoch doppelte Werte haben. Wenn die eindeutige ID nicht angegeben ist, innerhalb derselben Quelle nicht eindeutig ist oder sich in Bezug auf die Attributnamen der verschiedenen Quellen überschneidet, wird der Datensatz AWS Entity Resolution zurückgewiesen, wenn der entsprechende Workflow ausgeführt wird. Wenn Sie diese Schemazuordnung in einem regelbasierten Abgleichsworkflow verwenden, darf die eindeutige ID 38 Zeichen nicht überschreiten.

g. Wählen Sie für Eingabefelder die Spalten aus, die Sie für den Abgleich und für die optionale Weiterleitung verwenden möchten.

   Sie können insgesamt maximal 34 Spalten sowohl für den Abgleich als auch für die Weiterleitung auswählen.

   i. Wählen Sie unter Abgleich die Spalten aus, die Sie als Eingabefelder für den Abgleich verwenden möchten.

      Sie können insgesamt maximal 24 Spalten für den Abgleich auswählen.

   ii. Wählen Sie Spalten für Weiterleitung hinzufügen aus, wenn Sie die Spalten angeben möchten, die nicht für den Abgleich verwendet werden.

iii. (Optional) Wählen Sie unter Weiterleiten die Spalten aus, die als Durchgangsspalten aufgenommen werden sollen.

> **Note**
>
> Verwenden Sie keinen der folgenden reservierten Namen als Spaltennamen in Ihren Daten, wenn Sie auf maschinellem Lernen basierende Matching-Workflows ausführen: "`MatchId`„," „,, `MatchRule` „, `SourceId` „`RecordId`," und“. `TargetId` Die Verwendung eines dieser reservierten Namen führt zu Namenskonflikten und fehlgeschlagenen ML-basierten Abgleichs-Workflows.

h. (Optional) Wenn Sie Tags für die Ressource aktivieren möchten, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

i. Wählen Sie Weiter aus.

5. Definieren Sie für Schritt 2: Eingabefelder zuordnen die Eingabefelder, die Sie für den Abgleich und für die optionale Weiterleitung verwenden möchten.

   a. Für Eingabefelder für den Abgleich gilt für jedes Eingabefeld

      - Geben Sie den Attributtyp an, um die Daten zu klassifizieren.
      - Geben Sie den Namen des Match-Schlüssels an, um den Vergleich des Eingabefeldes mit Ihrem Abgleichs-Workflow zu ermöglichen. Bestimmte Namen von Abgleichsschlüsseln werden standardmäßig automatisch bestimmten Attributtypen zugeordnet.
      - Aktivieren Sie das Kontrollkästchen Hashed, wenn der Spaltenwert für dieses Eingabefeld gehasht ist, oder lassen Sie das Kontrollkästchen leer, wenn der Wert Klartext ist.

> **Note**
>
> Wenn Sie ein Schema-Mapping für die Verwendung mit der auf dem LiveRamp Provider-Service basierenden Matching-Technik erstellen, können Sie:
>
> - Geben Sie den Attributtyp für die Provider-ID als LiveRamp ID an.
> - Geben Sie den Attributtyp für das Namensfeld entweder in mehreren Feldern (wie Vorname, Nachname) oder in einem Feld an.

- Geben Sie den Attributtyp für das Adressfeld entweder in mehreren Feldern (z. B. Straße 1, Straße 2) oder in einem Feld (Vollständige Adresse) an.

  Beim Abgleich mit einer Adresse ist eine Postleitzahl (Postleitzahl) erforderlich.
- Wenn Sie E-Mail (E-Mail-Adresse) oder Telefonnummer (Telefonnummer) mit einem Namen angeben, können diese Felder mit der Straßenanschrift übereinstimmen.

Note

Wenn Sie eine Schemazuordnung für die Verwendung mit der auf dem TransUnion Provider-Service basierenden Vergleichstechnik erstellen, können Sie einen der folgenden Attributtypen angeben:

- Vollständiger Name, Vorname, Nachname
- Vollständige Adresse, Straße 1, Stadt, Bundesland, Land, Postleitzahl
- Phone number (Telefonnummer)
- E-Mail-Adresse
- Date (Datum)
- Digitale Identifikatoren: IPV4, IPV6, oder MAID

Note

Wenn Sie ein Schema-Mapping zur Verwendung mit dem auf maschinellem Lernen basierenden Matching-Workflow erstellen, muss Ihr Datensatz mindestens einen der folgenden Attributtypen enthalten:

- Vollständiger Name
- Vollständige Adresse
- Volles Telefon
- E-Mail-Adresse
- Datum mit einem Match-Schlüsselnamen oder Geburtsdatum

Geben Sie den Attributtyp für keines dieser Attribute als benutzerdefinierte Zeichenfolge an.

b. (Optional) Fügen Sie für Eingabefelder für die Weiterleitung die Eingabefelder hinzu, die nicht zugeordnet werden sollen, und den entsprechenden Hashing-Status.

   Der Hashing-Status gibt an, ob der Spaltenwert für dieses Eingabefeld ein Hashwert oder Klartext ist.

c. Wählen Sie Weiter aus.

6. Für Schritt 3: Daten gruppieren können Sie die Eingabefelder Name, Adresse und Telefonnummer gruppieren, wenn sie in mehrere Felder aufgeteilt wurden.

   In diesem Schritt werden die zugehörigen Eingabefelder zu einem Feld verkettet, sodass Sie sie als ein Feld in einem passenden Workflow vergleichen können.

   Wenn den Eingabefeldern Name, Adresse oder Telefonnummer keine Daten zugeordnet sind, ist dieser Abschnitt leer.

   Sie können auch weitere Gruppen hinzufügen, wenn Sie mehr Datentypen haben.

   a. Wenn Sie Eingabedaten nach Namen gruppieren möchten:

      Wählen Sie unter Vollständiger Name zwei oder mehr Eingabefelder aus, die Sie gruppieren möchten.

      Der Gruppenname und der Match-Schlüssel werden automatisch dem Datentyp zugeordnet.

      Sie können den Gruppennamen und den Abgleichsschlüssel mit einem benutzerdefinierten Abgleichsschlüssel aktualisieren, der bis zu 255 Zeichen enthalten kann, darunter Buchstaben, Zahlen, Unterstriche (_) oder Bindestriche (-).

      Wählen Sie Gruppe hinzufügen, um eine weitere Gruppe hinzuzufügen.

      > **Note**
      >
      > Die Normalisierung wird nur für den vollständigen Namen unterstützt.

Wenn Sie die Untertypen Vollständiger Name normalisieren möchten, weisen Sie der Gruppe Vollständiger Name die folgenden Untertypen zu: Vorname, Zweiter Vorname und Nachname.

b. Wenn Sie Eingabedaten für Adressen gruppieren möchten:

Wählen Sie für Vollständige Adresse zwei oder mehr Eingabefelder aus, die Sie gruppieren möchten.

Der Gruppenname und der Match-Schlüssel werden automatisch dem Datentyp zugeordnet.

Sie können den Gruppennamen und den Abgleichsschlüssel mit einem benutzerdefinierten Abgleichsschlüssel aktualisieren, der bis zu 255 Zeichen enthalten kann, darunter Buchstaben, Zahlen, Unterstriche (_) oder Bindestriche (-).

Wählen Sie Gruppe hinzufügen, um eine weitere Gruppe hinzuzufügen.

> **Note**
>
> Die Normalisierung wird nur für die vollständige Adresse unterstützt.
> Wenn Sie die Untertypen Vollständige Adresse normalisieren möchten, weisen Sie der Gruppe Vollständige Adresse die folgenden Untertypen zu: Straße 1, Straße 2: Name der Straße 3, Name der Stadt, Bundesland, Land und Postleitzahl.

c. Wenn Sie Telefoneingabedaten gruppieren möchten:

Wählen Sie für Vollständiges Telefon zwei oder mehr Eingabefelder aus, die Sie gruppieren möchten.

Der Gruppenname und der Match-Schlüssel werden automatisch dem Datentyp zugeordnet.

Sie können den Gruppennamen und den Abgleichsschlüssel mit einem benutzerdefinierten Abgleichsschlüssel aktualisieren, der bis zu 255 Zeichen enthalten kann, darunter Buchstaben, Zahlen, Unterstriche (_) oder Bindestriche (-).

Wählen Sie Gruppe hinzufügen, um eine weitere Gruppe hinzuzufügen.

> **Note**
>
> Die Normalisierung wird nur für das vollständige Telefon unterstützt.
> Wenn Sie die Untertypen „Vollständige Telefonnummer“ normalisieren möchten, weisen Sie der Telefongruppe „Vollständig“ die folgenden Untertypen zu: Telefonnummer und Landesvorwahl des Telefons.

d. Wählen Sie Weiter aus.

7. Gehen Sie für Schritt 4: Überprüfen und erstellen wie folgt vor:

   a. Überprüfen Sie die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Schema-Mapping erstellen aus.

> **Note**
>
> Sie können eine Schemazuordnung nicht ändern, nachdem Sie sie einem Workflow zugeordnet haben. Sie können eine Schemazuordnung klonen, wenn Sie eine bestehende Konfiguration verwenden möchten, um eine neue Schemazuordnung zu erstellen.

Nachdem Sie die Schemazuordnung erstellt haben, können Sie einen passenden Workflow oder einen ID-Namespace erstellen.

Build custom schema

So erstellen Sie eine Schemazuordnung mit der Option Benutzerdefiniertes Schema erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie auf der Seite Schemazuordnungen in der oberen rechten Ecke die Option Schema-Mapping erstellen aus.
4. Gehen Sie für Schritt 1: Schemadetails angeben wie folgt vor:

a. Geben Sie als Name und Erstellungsmethode einen Namen für die Schemazuordnung und optional eine Beschreibung ein.

b. Wählen Sie als Erstellungsmethode die Option Benutzerdefiniertes Schema erstellen aus.

c. Geben Sie unter Eindeutige ID eine eindeutige ID ein, um jede Zeile Ihrer Daten zu identifizieren.

   Example

   Beispiel: **`Primary_key`**, **`Row_ID`** oder **`Record_ID`**.

   > **Note**
   >
   > Die Spalte „Eindeutige ID“ ist erforderlich. Die eindeutige ID muss ein eindeutiger Bezeichner innerhalb einer einzelnen Tabelle sein. In verschiedenen Tabellen kann die Unique ID jedoch doppelte Werte haben. Wenn die eindeutige ID nicht angegeben ist, innerhalb derselben Quelle nicht eindeutig ist oder sich in Bezug auf die Attributnamen der verschiedenen Quellen überschneidet, wird der Datensatz AWS Entity Resolution zurückgewiesen, wenn der entsprechende Workflow ausgeführt wird. Wenn Sie diese Schemazuordnung in einem regelbasierten Abgleichsworkflow verwenden, darf die eindeutige ID 38 Zeichen nicht überschreiten.

d. (Optional) Wenn Sie Tags für die Ressource aktivieren möchten, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.

e. Wählen Sie Weiter aus.

5. Definieren Sie für Schritt 2: Eingabefelder zuordnen die Eingabefelder, die Sie für den Abgleich und für die optionale Weiterleitung verwenden möchten.

   Sie können insgesamt maximal 34 Spalten sowohl für den Abgleich als auch für den Durchlauf definieren.

   a. Geben Sie für Eingabefelder für den Abgleich ein Eingabefeld ein.

> **Note**
>
> Verwenden Sie keinen der folgenden reservierten Namen als Spaltennamen in Ihren Daten, wenn Sie auf maschinellem Lernen basierende Matching-Workflows ausführen: "`MatchId`„," „,, `MatchRule` „, `SourceId` „`RecordId`," und“. `TargetId` Die Verwendung eines dieser reservierten Namen führt zu Namenskonflikten und fehlgeschlagenen ML-basierten Abgleichs-Workflows.

b. Wählen Sie den Attributtyp aus, um die Daten zu klassifizieren.

> **Note**
>
> Wenn Sie eine Schemazuordnung für die Verwendung mit der auf dem LiveRamp Provider-Service basierenden Vergleichstechnik erstellen, können Sie den ProviderID-Attributtyp als ID angeben. LiveRamp Wenn Sie PII-Daten in die Ausgabe einbeziehen möchten, müssen Sie den Attributtyp als Benutzerdefinierte Zeichenfolge angeben.

> **Note**
>
> Wenn Sie eine Schemazuordnung für die Verwendung mit der auf dem TransUnion Provider-Service basierenden Vergleichstechnik erstellen, können Sie einen der folgenden Attributtypen angeben:
>
> - Vollständiger Name, Vorname, Nachname
> - Vollständige Adresse, Straße 1, Stadt, Bundesland, Land, Postleitzahl
> - Phone number (Telefonnummer)
> - E-Mail-Adresse
> - Date (Datum)
> - Digitale Identifikatoren: IPV4, IPV6, oder MAID

> **Note**
>
> Wenn Sie ein Schema-Mapping zur Verwendung mit dem auf maschinellem Lernen basierenden Matching-Workflow erstellen, muss Ihr Datensatz mindestens einen der folgenden Attributtypen enthalten:
>
> - Vollständiger Name
> - Vollständige Adresse
> - Volles Telefon
> - E-Mail-Adresse
> - Datum mit einem Match-Schlüsselnamen oder Geburtsdatum
>
> Geben Sie den Attributtyp für keines dieser Attribute als benutzerdefinierte Zeichenfolge an.

c. Wählen Sie den Namen des Match-Schlüssels aus, um den Vergleich des Eingabefeldes mit Ihrem Abgleichs-Workflow zu ermöglichen.

   Bestimmte Namen von Abgleichsschlüsseln werden standardmäßig automatisch bestimmten Attributtypen zugeordnet.

d. Aktivieren Sie das Kontrollkästchen Hashed, wenn der Spaltenwert für dieses Eingabefeld gehasht ist, oder lassen Sie das Kontrollkästchen leer, wenn der Wert Klartext ist.

e. Wählen Sie Eingabefeld hinzufügen, um weitere Eingabefelder hinzuzufügen.

   Sie können insgesamt maximal 24 Eingabefelder für den Abgleich hinzufügen.

f. (Optional) Fügen Sie für Eingabefelder für die Weiterleitung die Eingabefelder hinzu, die nicht zugeordnet werden sollen, und den entsprechenden Hashing-Status.

g. Wählen Sie Weiter aus.

6. Für Schritt 3: Gruppendaten können Sie die Eingabefelder Name, Adresse und Telefonnummer gruppieren, wenn sie in mehrere Felder aufgeteilt wurden.

   In diesem Schritt werden die zugehörigen Eingabefelder zu einem Feld verkettet, sodass Sie sie als ein Feld in einem passenden Workflow vergleichen können.

Wenn den Eingabefeldern Name, Adresse und Telefonnummer keine Daten zugeordnet sind, ist dieser Abschnitt leer.

Sie können auch weitere Gruppen hinzufügen, wenn Sie mehr Datentypen haben.

a. Wenn Sie Eingabedaten nach Namen gruppieren möchten:

   Wählen Sie unter Vollständiger Name zwei oder mehr Eingabefelder aus, die Sie gruppieren möchten.

   Der Gruppenname und der Match-Schlüssel werden automatisch dem Datentyp zugeordnet.

   Sie können den Gruppennamen und den Abgleichsschlüssel mit einem benutzerdefinierten Abgleichsschlüssel aktualisieren, der bis zu 255 Zeichen enthalten kann, darunter Buchstaben, Zahlen, Unterstriche (_) oder Bindestriche (-).

   Wählen Sie Gruppe hinzufügen, um eine weitere Gruppe hinzuzufügen.

   > **Note**
   >
   > Die Normalisierung wird nur für den vollständigen Namen unterstützt.
   > Wenn Sie die Untertypen Vollständiger Name normalisieren möchten, weisen Sie der Gruppe Vollständiger Name die folgenden Untertypen zu: Vorname, Zweiter Vorname und Nachname.

b. Wenn Sie Eingabedaten für Adressen gruppieren möchten:

   Wählen Sie für Vollständige Adresse zwei oder mehr Eingabefelder aus, die Sie gruppieren möchten.

   Der Gruppenname und der Match-Schlüssel werden automatisch dem Datentyp zugeordnet.

   Sie können den Gruppennamen und den Abgleichsschlüssel mit einem benutzerdefinierten Abgleichsschlüssel aktualisieren, der bis zu 255 Zeichen enthalten kann, darunter Buchstaben, Zahlen, Unterstriche (_) oder Bindestriche (-).

   Wählen Sie Gruppe hinzufügen, um eine weitere Gruppe hinzuzufügen.

> **Note**
>
> Die Normalisierung wird nur für die vollständige Adresse unterstützt.
> Wenn Sie die Untertypen Vollständige Adresse normalisieren möchten, weisen Sie der Gruppe Vollständige Adresse die folgenden Untertypen zu: Straße 1, Straße 2: Name der Straße 3, Name der Stadt, Bundesland, Land und Postleitzahl.

c. Wenn Sie Telefoneingabedaten gruppieren möchten:

   Wählen Sie für Vollständiges Telefon zwei oder mehr Eingabefelder aus, die Sie gruppieren möchten.

   Der Gruppenname und der Match-Schlüssel werden automatisch dem Datentyp zugeordnet.

   Sie können den Gruppennamen und den Abgleichsschlüssel mit einem benutzerdefinierten Abgleichsschlüssel aktualisieren, der bis zu 255 Zeichen enthalten kann, darunter Buchstaben, Zahlen, Unterstriche (_) oder Bindestriche (-).

   Wählen Sie Gruppe hinzufügen, um eine weitere Gruppe hinzuzufügen.

> **Note**
>
> Die Normalisierung wird nur für das vollständige Telefon unterstützt.
> Wenn Sie die Untertypen „Vollständige Telefonnummer“ normalisieren möchten, weisen Sie der Telefongruppe „Vollständig“ die folgenden Untertypen zu: Telefonnummer und Landesvorwahl des Telefons.

d. Wählen Sie Weiter aus.

7. Gehen Sie für Schritt 4: Überprüfen und erstellen wie folgt vor:

   a. Überprüfen Sie die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Schema-Mapping erstellen aus.

> **Note**
>
> Sie können eine Schemazuordnung nicht ändern, nachdem Sie sie einem Workflow zugeordnet haben. Sie können eine Schemazuordnung klonen, wenn Sie eine bestehende Konfiguration verwenden möchten, um eine neue Schemazuordnung zu erstellen.

Nachdem Sie die Schemazuordnung erstellt haben, können Sie einen passenden Workflow oder einen ID-Namespace erstellen.

Use JSON editor

Um eine Schemazuordnung mit dem JSON-Editor zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie auf der Seite Schemazuordnungen in der oberen rechten Ecke die Option Schema-Mapping erstellen aus.
4. Gehen Sie für Schritt 1: Schemadetails angeben wie folgt vor:
    a. Geben Sie als Name und Erstellungsmethode einen Namen für die Schemazuordnung und optional eine Beschreibung ein.
    b. Wählen Sie als Erstellungsmethode die Option JSON-Editor verwenden aus.
    c. (Optional) Wenn Sie Tags für die Ressource aktivieren möchten, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.
    d. Wählen Sie Weiter aus.
5. Für Schritt 2: Zuordnung angeben:
    a. Beginnen Sie mit der Erstellung des Schemas im JSON-Editor oder wählen Sie je nach Ziel eine der folgenden Optionen aus:

Ihr Ziel	Empfohlene Option
Beginnen Sie mit der Erstellung Ihres Schema-Mappings	Fügen Sie ein JSON-Beispiel ein und bearbeiten Sie die Informationen nach Bedarf.
Verwenden Sie eine vorhandene JSON-Datei	Aus einer Datei importieren

> **Note**
>
> Die Normalisierung wird nur für die folgenden Typen unterstützt:`NAME`, `ADDRESSPHONE`, und`EMAIL_ADRESS`.
> Wenn Sie die `NAME` Untertypen normalisieren möchten, weisen Sie dem `NAME` groupName die folgenden Untertypen zu:`NAME_FIRST`,, und `NAME_MIDDLE` `NAME_LAST`
> Wenn Sie die `ADDRESS` Untertypen normalisieren möchten,
> weisen Sie dem `ADDRESS` groupName die folgenden Untertypen zu:`ADDRESS_STREET1`,,,`ADDRESS_STREET2`, `ADDRESS_STREET3` `ADDRESS_CITY`ADDRESS_STATE, `ADDRESS_COUNTRY` und. `ADDRESS_POSTALCODE`
> Wenn Sie die `PHONE` Untertypen normalisieren möchten, weisen Sie dem `PHONE` groupName die folgenden Untertypen zu: und. `PHONE_NUMBER` `PHONE_COUNTRYCODE`

b. Wählen Sie Weiter aus.

6. Für Schritt 3: Überprüfen und erstellen:

   a. Überprüfen Sie die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Schema-Mapping erstellen aus.

> **Note**
>
> Sie können eine Schemazuordnung nicht ändern, nachdem Sie sie einem Workflow zugeordnet haben. Sie können eine Schemazuordnung klonen, wenn Sie eine bestehende Konfiguration verwenden möchten, um eine neue Schemazuordnung zu erstellen.

Nachdem Sie die Schemazuordnung erstellt haben, können Sie einen passenden Workflow oder einen ID-Namespace erstellen.

Klonen einer Schemazuordnung

Sie können ein Schema-Mapping klonen, wenn Sie eine bestehende Konfiguration verwenden möchten, um ein neues Schema-Mapping zu erstellen.

So klonen Sie ein Schema-Mapping:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie die Schemazuordnung aus.
4. Klicken auf Clone.
5. Nehmen Sie auf der Seite Schemadetails angeben die erforderlichen Änderungen vor und wählen Sie dann Weiter.
6. Nehmen Sie auf der Seite Passende Technik auswählen die erforderlichen Änderungen vor und klicken Sie dann auf Weiter.
7. Nehmen Sie auf der Seite Map-Eingabefelder alle erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
8. Nehmen Sie auf der Seite Gruppendaten die erforderlichen Änderungen vor und wählen Sie dann Weiter.
9. Nehmen Sie auf der Seite Überprüfen und speichern die erforderlichen Änderungen vor und wählen Sie dann Schema-Mapping klonen aus.

Eine Schemazuordnung bearbeiten

Sie können eine Schemazuordnung nur bearbeiten, bevor Sie sie einem Workflow zuordnen. Nachdem Sie eine Schemazuordnung einem Workflow zugeordnet haben, können Sie sie nicht mehr bearbeiten. Sie können ein Schema-Mapping klonen, wenn Sie eine bestehende Konfiguration verwenden möchten, um ein neues Schema-Mapping zu erstellen.

Um ein Schema-Mapping zu bearbeiten:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie die Schemazuordnung aus.
4. Wählen Sie Bearbeiten aus.
5. Nehmen Sie auf der Seite Schemadetails angeben die erforderlichen Änderungen vor und wählen Sie dann Weiter.
6. Nehmen Sie auf der Seite Passende Technik auswählen die erforderlichen Änderungen vor und klicken Sie dann auf Weiter.
7. Nehmen Sie auf der Seite Map-Eingabefelder alle erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
8. Nehmen Sie auf der Seite Gruppendaten die erforderlichen Änderungen vor und wählen Sie dann Weiter.

> **Note**
>
> Die Normalisierung wird nur für den vollständigen Namen, die vollständige Adresse, die vollständige Telefonnummer und die E-Mail-Adresse unterstützt.
> Wenn Sie die Untertypen Vollständiger Name normalisieren möchten, weisen Sie der Gruppe Vollständiger Name die folgenden Untertypen zu: Vorname, Zweiter Vorname und Nachname.
> Wenn Sie die Untertypen Vollständige Adresse normalisieren möchten, weisen Sie der Gruppe Vollständige Adresse die folgenden Untertypen zu: Straße 1, Straße 2: Name der Straße 3, Name der Stadt, Bundesland, Land und Postleitzahl.

Wenn Sie die Untertypen Vollständige Telefonnummer normalisieren möchten, weisen Sie der Gruppe Vollständige Telefonnummer die folgenden Untertypen zu: Telefonnummer und Landesvorwahl des Telefons.

9. Nehmen Sie auf der Seite Überprüfen und speichern die erforderlichen Änderungen vor und wählen Sie dann Schemazuordnung bearbeiten aus.

Löschen einer Schemazuordnung

Sie können eine Schemazuordnung nicht löschen, wenn sie einem passenden Workflow zugeordnet ist. Sie müssen zuerst die Schemazuordnung aus allen zugehörigen passenden Workflows entfernen, bevor Sie sie löschen können.

Um eine Schemazuordnung zu löschen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie die Schemazuordnung aus.
4. Wählen Sie Löschen aus.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Definieren Sie Eingabedaten mithilfe eines ID-Namespace

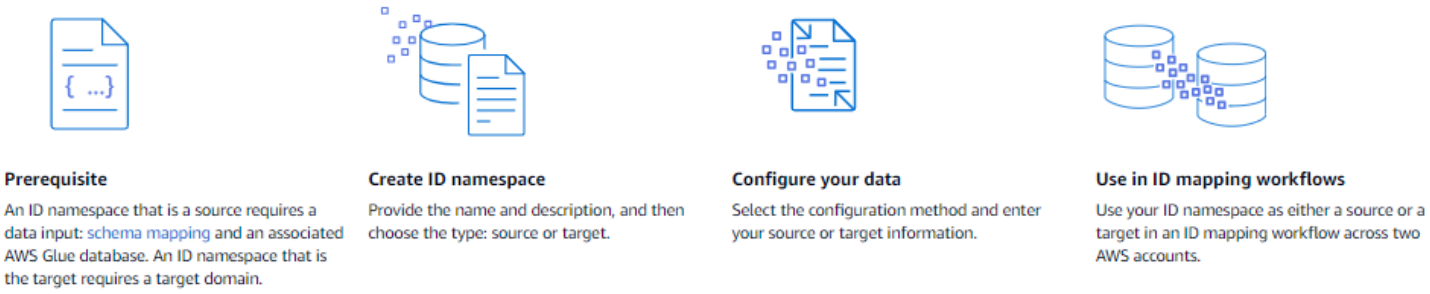
Ein ID-Namespace ist ein Wrapper, der Ihre Eingabedatentabelle umschließt. Sie verwenden einen ID-Namespace, um Metadaten bereitzustellen, in denen Ihre Eingabedaten und Abgleichstechniken sowie deren Verwendung in einem ID-Mapping-Workflow erläutert werden.

Es gibt zwei Arten von ID-Namespaces: Quelle und Ziel.

- Die Quelle enthält Konfigurationen für die Quelldaten, die in einem AWS Entity Resolution ID-Mapping-Workflow verarbeitet werden.
- Das Ziel enthält eine Konfiguration der Zieldaten, in die alle Quellen aufgelöst werden.

Sie können die Eingabedaten, die Sie über zwei Daten hinweg auflösen möchten, AWS-Konten in einem ID-Mapping-Workflow definieren. Ein Teilnehmer erstellt eine ID-Namespace-Quelle und ein anderer Teilnehmer erstellt ein ID-Namespace-Ziel. Nachdem die Teilnehmer die Quelle und das Ziel erstellt haben, können Sie einen ID-Mapping-Workflow ausführen, um die Daten von der Quelle in das Ziel zu übersetzen.

Das folgende Diagramm fasst zusammen, wie ein ID-Namespace zur Verwendung in einem ID-Zuordnungs-Workflow erstellt wird.



In den folgenden Abschnitten wird beschrieben, wie eine ID-Namespace-Quelle und ein ID-Namespace-Ziel erstellt werden.

Topics

- ID-Namespace-Quelle
- ID-Namespace-Ziel
- Einen ID-Namespace bearbeiten
- Löschen eines ID-Namespaces

- Hinzufügen oder Aktualisieren einer Ressourcenrichtlinie für einen ID-Namespace

ID-Namespace-Quelle

Die ID-Namespace-Quelle ist die Quelle der Daten in einem ID-Zuordnungs-Workflow.

Bevor Sie eine ID-Namespace-Quelle erstellen, müssen Sie je nach Anwendungsfall zunächst eine Schemazuordnung oder einen passenden Workflow erstellen. Weitere Informationen erhalten Sie unter Eine Schemazuordnung erstellen und Abgleichen von Eingabedaten mithilfe eines Abgleich-Workflows.

Nachdem Sie eine ID-Namespace-Quelle erstellt haben, können Sie sie zusammen mit einem ID-Namespace-Ziel in einem ID-Zuordnungs-Workflow verwenden. Weitere Informationen finden Sie unter Eingabedaten mithilfe eines ID-Zuordnungs-Workflows zuordnen.

Es gibt zwei Möglichkeiten, eine ID-Namespace-Quelle in der AWS Entity Resolution Konsole zu erstellen: die regelbasierte Methode oder die Provider Services-Methode.

Themen

- Eine ID-Namespace-Quelle erstellen (regelbasiert)
- Eine ID-Namespace-Quelle erstellen (Providerdienste)

Eine ID-Namespace-Quelle erstellen (regelbasiert)

In diesem Thema wird beschrieben, wie eine ID-Namespace-Quelle mithilfe der regelbasierten Methode erstellt wird. Diese Methode verwendet Abgleichsregeln, um Erstanbieterdaten in einem ID-Zuordnungs-Workflow von einer Quelle in ein Ziel zu übersetzen.

> **Note**
>
> Wenn es sich bei den Eingabedaten um die Quelle handelt, müssen sie über eine Schemazuordnung und eine zugehörige AWS Glue Datenbank verfügen.

Um eine ID-Namespace-Quelle zu erstellen (regelbasiert)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter. https://console.aws.amazon.com/entityresolution/

2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option ID-Namespaces aus.
3. Wählen Sie auf der Seite ID-Namespaces in der oberen rechten Ecke die Option ID-Namespace erstellen aus.
4. Gehen Sie wie folgt vor, um Details zu erhalten:

   a. Geben Sie für den ID-Namespace-Namen einen eindeutigen Namen ein.

   b. (Optional) Geben Sie unter Beschreibung eine optionale Beschreibung ein.

   c. Wählen Sie als ID-Namespace-Typ die Option Source aus.
5. Wählen Sie für die ID-Namespace-Methode die Option Regelbasiert aus.
6. Wählen Sie für die Dateneingabe den Eingabetyp aus, den Sie verwenden möchten, und ergreifen Sie dann die empfohlenen Maßnahmen.

Eingabetyp	Empfohlene Aktionen
Eine bestehende Schemazuordnung	1. Wählen Sie Schema-Mapping. 2. Wählen Sie die AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und das Schema-Mapping aus der Drop-down-Liste aus. Sie können bis zu 19 Dateneingaben hinzufügen. **Note** Wenn Ihre Datentabelle eine DELETE-Spalte hat, muss der Typ der Schemazuordnung lauten, `String` und Sie dürfen kein `matchKey` AND haben`groupName` .
Ein vorhandener Abgleichs-Workflow	1. Wählen Sie den Matching-Workflow aus. 2. Wählen Sie das Konto aus, das dem ID-Namespace zugeordnet ist: entweder Ihr

Eingabetyp	Empfohlene Aktionen
	Konto AWS-Konto oder Ein anderes AWS-Konto. 3. Wählen Sie je nach Kontotyp den Namen des Matching-Workflows aus oder geben Sie den Matching-Workflow-ARN ein.

7. Gehen Sie für Regelparameter wie folgt vor.

   a. Geben Sie die Regelsteuerelemente an, indem Sie je nach Ziel eine der folgenden Optionen auswählen.

Ihr Ziel	Empfohlene Option
Lassen Sie Regeln sowohl von der Quelle als auch vom Ziel zu	Keine Präferenz
Wählen Sie aus, ob eine Quelle, ein Ziel oder beide Regeln in einem ID-Mapping-Workflow bereitstellen können	Eingeschränkte Regeln

   Regelsteuerungen müssen zwischen der Quelle und dem Ziel kompatibel sein, damit sie in einem ID-Mapping-Workflow verwendet werden können. Wenn beispielsweise ein Quell-ID-Namespace die Regeln auf das Ziel beschränkt, der Ziel-ID-Namespace die Regeln jedoch auf die Quelle beschränkt, führt dies zu einem Fehler.

   b. Geben Sie die Abgleichsregeln an, indem Sie je nach Dateneingabetyp eine der folgenden Optionen auswählen.

Art der Dateneingabe	Empfohlene Aktion
Schemazuordnung	Wählen Sie Weitere Regel hinzufügen aus, um eine passende Regel hinzuzufügen. Sie können bis zu 25 Zuordnungsregeln anwenden, um Ihre Übereinstimmungskriterien zu definieren.

Art der Dateneingabe	Empfohlene Aktion
Workflow für den Abgleich	Wählen Sie entweder Regeln aus dem Abgleichs-Workflow verwenden oder Neue Regeln bereitstellen, um Ihre Abgleichs regeln zu definieren.

8. Gehen Sie für Vergleichs- und Abgleichsparameter wie folgt vor.

   a. Geben Sie den Vergleichstyp an, indem Sie je nach Ziel eine der folgenden Optionen auswählen.

Ihr Ziel	Empfohlene Option
Erlauben Sie die Verwendung eines beliebigen Vergleichstyps, wenn Sie den ID-Mapping-Workflow erstellen.	Keine Präferenz
Suchen Sie nach einer beliebigen Kombination von Übereinstimmungen in Daten, die in mehreren Eingabefeldern gespeichert sind, unabhängig davon, ob sich die Daten im selben oder in einem anderen Eingabefeld befinden.	Mehrere Eingabefelder
Beschränken Sie den Vergleich innerhalb eines einzelnen Eingabefeldes, wenn ähnliche Daten, die in mehreren Eingabefe ldern gespeichert sind, nicht abgeglichen werden sollen.	Einzelnes Eingabefeld

   b. Geben Sie den Abgleichstyp Datensatz an, indem Sie je nach Ziel eine der folgenden Optionen auswählen.

Ihr Ziel	Empfohlene Option
Erlauben Sie die Verwendung eines beliebigen Vergleichstyps, wenn Sie den ID-Mapping-Workflow erstellen.	Keine Präferenz
Beschränken Sie den Datensatzabgleichstyp so, dass für jeden übereinstimmenden Datensatz im Ziel nur ein übereinstimmender Datensatz in der Quelle gespeichert wird, wenn Sie den ID-Mapping-Workflow erstellen.	Eingeschränkter Datensatzabgleich und Eine Quelle für ein Ziel
Beschränken Sie den Datensatzabgleichstyp auf das Speichern aller übereinstimmenden Datensätze in der Quelle für jeden übereinstimmenden Datensatz im Ziel, wenn Sie den ID-Mapping-Workflow erstellen.	Eingeschränkter Datensatzabgleich und Viele Quellen für ein Ziel

> **Note**
>
> Sie müssen kompatible Einschränkungen für die Quell- und Ziel-ID-Namespaces angeben. Wenn beispielsweise ein Quell-ID-Namespace die Regeln auf das Ziel beschränkt, der Ziel-ID-Namespace die Regeln jedoch auf die Quelle beschränkt, führt dies zu einem Fehler.

9. Geben Sie die Dienstzugriffsberechtigungen an, indem Sie einen vorhandenen Servicerollennamen aus der Dropdownliste auswählen.
10. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.
11. Wählen Sie „ID-Namespace erstellen“.

Die ID-Namespace-Quelle wird erstellt. Sie sind jetzt bereit, ein ID-Namespace-Ziel zu erstellen.

Eine ID-Namespace-Quelle erstellen (Providerdienste)

In diesem Thema wird beschrieben, wie eine ID-Namespace-Quelle mithilfe der Provider Services-Methode erstellt wird. Diese Methode verwendet einen Anbieterdienst namens LiveRamp. LiveRamp übersetzt während eines ID-Mapping-Workflows codierte Daten von Drittanbietern von einer Quelle in ein Ziel.

> **Note**
>
> Wenn es sich bei den Eingabedaten um die Quelle handelt, müssen sie über eine Schemazuordnung und eine zugehörige AWS Glue Datenbank verfügen.

Um eine ID-Namespace-Quelle zu erstellen (Providerdienste)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option ID-Namespaces aus.
3. Wählen Sie auf der Seite ID-Namespaces in der oberen rechten Ecke die Option ID-Namespace erstellen aus.
4. Gehen Sie wie folgt vor, um Details zu erhalten:
   a. Geben Sie für den ID-Namespace-Namen einen eindeutigen Namen ein.
   b. (Optional) Geben Sie unter Beschreibung eine optionale Beschreibung ein.
   c. Wählen Sie als ID-Namespace-Typ die Option Source aus.
5. Wählen Sie für die ID-Namespace-Methode Provider Services aus.

   > **Note**
   >
   > AWS Entity Resolution bietet den LiveRamp Provider-Dienst derzeit als ID-Namespace-Methode an. Wenn Sie ein Abonnement für haben LiveRamp, wird der Status als Abonniert angezeigt. Weitere Informationen zum Abonnieren finden Sie LiveRamp unterSchritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange.

6. Wählen Sie für die Dateneingabe die AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und das Schema-Mapping aus der Dropdownliste aus.

Sie können bis zu 20 Dateneingaben hinzufügen.

7. Um die Zugriffsberechtigungen für den Dienst festzulegen, wählen Sie eine Option und ergreifen Sie die empfohlene Maßnahme.

Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname für die Servicerolle lautet `entityresolution-id-mapping-workflow-<timestamp>` . • Sie müssen über die erforderlichen Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar.

Option	Empfohlene Aktion
	2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenric htlinie zu aktualisieren, um die erforderl ichen Berechtigungen hinzuzufügen.

8. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.
9. Wählen Sie „ID-Namespace erstellen“.

Die ID-Namespace-Quelle wird erstellt. Sie sind jetzt bereit, ein ID-Namespace-Ziel zu erstellen.

ID-Namespace-Ziel

Das ID-Namespace-Ziel ist das Ziel der Daten in einem ID-Zuordnungs-Workflow. Alle Quellen werden in das Ziel aufgelöst.

Bevor Sie ein ID-Namespace-Ziel erstellen, müssen Sie je nach Anwendungsfall zuerst einen passenden Workflow erstellen oder über ein Abonnement für einen Provider-Service (LiveRamp) verfügen. Weitere Informationen erhalten Sie unter Abgleichen von Eingabedaten mithilfe eines Abgleich-Workflows und Schritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange.

Nachdem Sie ein ID-Namespace-Ziel erstellt haben, können Sie es zusammen mit einer ID-Namespace-Quelle in einem ID-Zuordnungs-Workflow verwenden. Weitere Informationen finden Sie unter Eingabedaten mithilfe eines ID-Zuordnungs-Workflows zuordnen.

Es gibt zwei Möglichkeiten, ein ID-Namespace-Ziel in der AWS Entity Resolution Konsole zu erstellen: die regelbasierte Methode oder die Provider Services-Methode.

Themen

- Erstellen eines ID-Namespace-Ziels (regelbasierte Methode)
- Erstellen eines ID-Namespace-Ziels (Provider-Services-Methode)

Erstellen eines ID-Namespace-Ziels (regelbasierte Methode)

In diesem Thema wird beschrieben, wie ein ID-Namespace-Ziel mithilfe der regelbasierten Methode erstellt wird. Diese Methode verwendet Abgleichsregeln, um Erstanbieterdaten während eines ID-Zuordnungs-Workflows von einer Quelle in ein Ziel zu übersetzen.

Um ein ID-Namespace-Ziel zu erstellen (regelbasiert)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter. https://console.aws.amazon.com/entityresolution/
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option ID-Namespaces aus.
3. Wählen Sie auf der Seite ID-Namespaces in der oberen rechten Ecke die Option ID-Namespace erstellen aus.
4. Gehen Sie wie folgt vor, um Details zu erhalten:
   a. Geben Sie für den ID-Namespace-Namen einen eindeutigen Namen ein.
   b. (Optional) Geben Sie unter Beschreibung eine optionale Beschreibung ein.
   c. Wählen Sie als ID-Namespace-Typ die Option Target aus.
5. Wählen Sie für die ID-Namespace-Methode die Option Regelbasiert aus.
6. Gehen Sie für die Dateneingabe unter Abgleichender Workflow wie folgt vor.
   a. Wählen Sie das Konto aus, das dem ID-Namespace zugeordnet ist: entweder Ihr Konto AWS-Konto oder Ein anderes AWS-Konto.
   b. Wählen Sie je nach Kontotyp den Namen des Matching-Workflows aus oder geben Sie den Matching-Workflow-ARN ein.
7. Gehen Sie für Regelparameter wie folgt vor.
   a. Geben Sie die Regelsteuerelemente an, indem Sie je nach Ziel eine der folgenden Optionen auswählen.

Ihr Ziel	Empfohlene Option
Lassen Sie Regeln sowohl von der Quelle als auch vom Ziel zu	Keine Präferenz

Ihr Ziel	Empfohlene Option
Wählen Sie aus, ob eine Quelle, ein Ziel oder beide Regeln in einem ID-Mapping-Workflow bereitstellen können	Eingeschränkte Regeln

Regelsteuerungen müssen zwischen der Quelle und dem Ziel kompatibel sein, damit sie in einem ID-Mapping-Workflow verwendet werden können. Wenn beispielsweise ein Quell-ID-Namespace die Regeln auf das Ziel beschränkt, der Ziel-ID-Namespace die Regeln jedoch auf die Quelle beschränkt, führt dies zu einem Fehler.

b. Fügt für Abgleichsregeln AWS Entity Resolution automatisch die Regeln aus dem Abgleichs-Workflow hinzu.

8. Gehen Sie für Vergleichs- und Abgleichsparameter wie folgt vor.

a. Geben Sie den Vergleichstyp an, indem Sie je nach Ziel eine der folgenden Optionen auswählen.

Ihr Ziel	Empfohlene Option
Erlauben Sie die Verwendung eines beliebigen Vergleichstyps, wenn Sie den ID-Mapping-Workflow erstellen.	Keine Präferenz
Suchen Sie nach einer beliebigen Kombination von Übereinstimmungen in Daten, die in mehreren Eingabefeldern gespeichert sind, unabhängig davon, ob sich die Daten im selben oder in einem anderen Eingabefeld befinden.	Mehrere Eingabefelder
Beschränken Sie den Vergleich innerhalb eines einzelnen Eingabefeldes, wenn ähnliche Daten, die in mehreren Eingabefe ldern gespeichert sind, nicht abgeglichen werden sollen.	Einzelnes Eingabefeld

b. Geben Sie den Abgleichstyp Datensatz an, indem Sie je nach Ziel eine der folgenden Optionen auswählen.

Ihr Ziel	Empfohlene Option
Erlauben Sie die Verwendung eines beliebigen Vergleichstyps, wenn Sie den ID-Mapping-Workflow erstellen.	Keine Präferenz
Beschränken Sie den Datensatzabgleichstyp so, dass für jeden übereinstimmenden Datensatz im Ziel nur ein übereinstimmender Datensatz in der Quelle gespeichert wird, wenn Sie den ID-Mapping-Workflow erstellen.	Eingeschränkter Datensatzabgleich und Eine Quelle für ein Ziel
Beschränken Sie den Datensatzabgleichstyp auf das Speichern aller übereinstimmenden Datensätze in der Quelle für jeden übereinstimmenden Datensatz im Ziel, wenn Sie den ID-Mapping-Workflow erstellen.	Eingeschränkter Datensatzabgleich und Viele Quellen für ein Ziel

> **Note**
>
> Sie müssen kompatible Einschränkungen für die Quell- und Ziel-ID-Namespaces angeben. Wenn beispielsweise ein Quell-ID-Namespace die Regeln auf das Ziel beschränkt, der Ziel-ID-Namespace die Regeln jedoch auf die Quelle beschränkt, führt dies zu einem Fehler.

9. Geben Sie die Dienstzugriffsberechtigungen an, indem Sie einen vorhandenen Servicerollennamen aus der Dropdownliste auswählen.
10. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.
11. Wählen Sie „ID-Namespace erstellen“.

Das ID-Namespace-Ziel wird erstellt. Nachdem Sie die für einen ID-Zuordnungs-Workflow erforderlichen ID-Namespaces (Quelle und Ziel) erstellt haben, können Sie einen ID-Zuordnungs-Workflow erstellen.

Erstellen eines ID-Namespace-Ziels (Provider-Services-Methode)

In diesem Thema wird beschrieben, wie ein ID-Namespace-Ziel mithilfe der Provider Services-Methode erstellt wird. Diese Methode verwendet einen Anbieterdienst namens LiveRamp. LiveRamp übersetzt während eines ID-Mapping-Workflows codierte Daten von Drittanbietern von einer Quelle in ein Ziel.

Um ein ID-Namespace-Ziel zu erstellen (Providerdienste)

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option ID-Namespaces aus.
3. Wählen Sie auf der Seite ID-Namespaces in der oberen rechten Ecke die Option ID-Namespace erstellen aus.
4. Gehen Sie wie folgt vor, um Details zu erhalten:
   a. Geben Sie für den ID-Namespace-Namen einen eindeutigen Namen ein.
   b. (Optional) Geben Sie unter Beschreibung eine optionale Beschreibung ein.
   c. Wählen Sie als ID-Namespace-Typ die Option Target aus.
5. Wählen Sie als ID-Namespace-Methode die Option Provider Services aus.

> **Note**
>
> AWS Entity Resolution bietet den LiveRamp Provider-Dienst derzeit als ID-Namespace-Methode an.
> Wenn Sie ein Abonnement für haben LiveRamp, wird der Status als Abonniert angezeigt.
> Weitere Informationen zum Abonnieren finden Sie LiveRamp unterSchritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange.

6. Geben Sie für Zieldomäne die LiveRamp Client-Domänenkennung ein, die für die Transcodierung vorgesehen ist und die Folgendes LiveRamp bietet:

7. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.
8. Wählen Sie „ID-Namespace erstellen“.

Das ID-Namespace-Ziel wird erstellt. Nachdem Sie die für einen ID-Zuordnungs-Workflow erforderlichen ID-Namespaces (Quelle und Ziel) erstellt haben, können Sie den ID-Zuordnungs-Workflow erstellen.

Einen ID-Namespace bearbeiten

Sie können einen ID-Namespace nur bearbeiten, bevor Sie ihn einem ID-Zuordnungs-Workflow zuordnen. Nachdem Sie einen ID-Namespace einem ID-Zuordnungs-Workflow zugeordnet haben, können Sie ihn nicht mehr bearbeiten.

So bearbeiten Sie einen ID-Namespace:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option ID-Namespaces aus.
3. Wählen Sie den ID-Namespace aus.
4. Wählen Sie Bearbeiten aus.
5. Nehmen Sie auf der Seite ID-Namespace bearbeiten die erforderlichen Änderungen vor und wählen Sie dann Speichern.

Löschen eines ID-Namespaces

Sie können einen ID-Namespace nicht löschen, wenn er einem ID-Zuordnungs-Workflow zugeordnet ist. Sie müssen zuerst die Schemazuordnung aus allen zugehörigen Workflows für die ID-Zuordnung entfernen, bevor Sie sie löschen können.

Um einen ID-Namespace zu löschen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.

2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option ID-Namespaces aus.
3. Wählen Sie den ID-Namespace aus.
4. Wählen Sie Löschen aus.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Hinzufügen oder Aktualisieren einer Ressourcenrichtlinie für einen ID-Namespace

Eine Ressourcenrichtlinie ermöglicht dem Ersteller der ID-Zuordnungsressource den Zugriff auf Ihre ID-Namespace-Ressource.

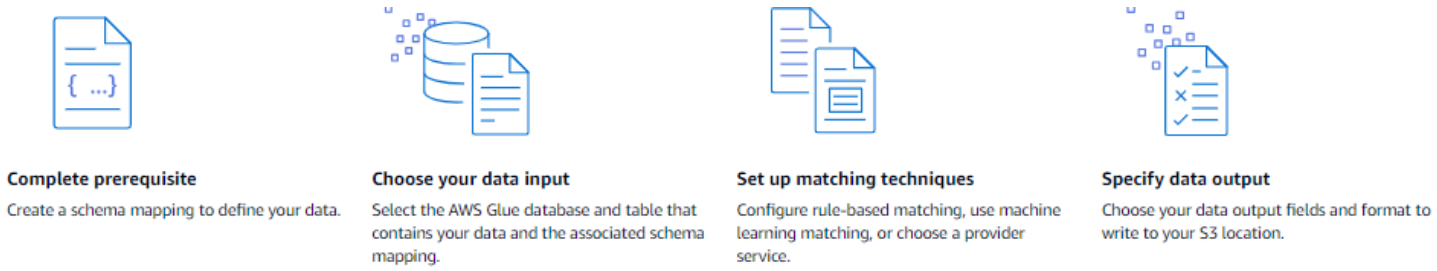
Um eine Ressourcenrichtlinie hinzuzufügen oder zu aktualisieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Namespaces aus.
3. Wählen Sie den ID-Namespace aus.
4. Wählen Sie auf der Seite mit den ID-Namespace-Details die Registerkarte Berechtigungen aus.
5. Wählen Sie im Abschnitt Ressourcenrichtlinie die Option Bearbeiten aus.
6. Fügen Sie die Richtlinie im JSON-Editor hinzu oder aktualisieren Sie sie.
7. Wählen Sie Änderungen speichern aus.

Abgleichen von Eingabedaten mithilfe eines Abgleich-Workflows

Ein Matching-Workflow ist ein Datenverarbeitungsjob, der Daten aus verschiedenen Eingabequellen kombiniert und vergleicht und anhand verschiedener Abgleichstechniken bestimmt, welche Datensätze übereinstimmen. AWS Entity Resolution liest Ihre Daten von den angegebenen Speicherorten, findet Übereinstimmungen zwischen Datensätzen und weist jedem übereinstimmenden Datensatz eine Match-ID zu.

Das folgende Diagramm fasst zusammen, wie Sie einen passenden Workflow erstellen.



Topics

- Passende Workflowtypen
- Optionen für die Datenausgabe
- Passende Workflow-Ergebnisse
- Einen regelbasierten Matching-Workflow erstellen
- Erstellung eines Matching-Workflows, der auf maschinellem Lernen basiert
- Erstellen eines auf dem Provider-Service basierenden Matching-Workflows
- Bearbeitung eines passenden Workflows
- Einen passenden Workflow löschen
- Ändern oder Generieren einer Match-ID für einen regelbasierten Matching-Workflow
- Suche nach einer Match-ID für einen regelbasierten Matching-Workflow
- Löschen von Datensätzen aus einem regelbasierten oder passenden Workflow ML-based
- Fehlerbehebung bei passenden Workflows

Passende Workflowtypen

AWS Entity Resolution unterstützt drei Arten von passenden Workflows:

Rule-based übereinstimmend

: Verwendet konfigurierbare Regeln, um übereinstimmende Datensätze auf der Grundlage einer exakten oder unscharfen Übereinstimmung der angegebenen Felder zu identifizieren. Sie definieren die Übereinstimmungskriterien, z. B. übereinstimmende Namen, die ähnlich geschrieben sind, oder Adressen, die unterschiedlich formatiert sind.

Abgleich auf Grundlage von Machine Learning

: Verwendet Modelle für maschinelles Lernen, um ähnliche Datensätze zu identifizieren, auch wenn die Daten Variationen, Fehler oder fehlende Felder aufweisen. Mit diesem Ansatz können komplexere Übereinstimmungen erkannt werden als bei regelbasierten Übereinstimmungen.

Dienstbasierter Abgleich durch den Anbieter

: Nutzt externe Datenanbieter, um Ihre Daten vor dem Abgleich anzureichern und zu validieren. Diese Art des Abgleichs ist nicht mit der Ausgabe von Connect Customer Customer Profiles kompatibel.

Optionen für die Datenausgabe

AWS Entity Resolution kann Datenausgabedateien schreiben in:

- Ein Amazon S3-Standort, den Sie angeben
- Kundenprofile verbinden (für die Deduplizierung von Kundendaten)

> **Important**
>
> Der Export nach Connect-Kundenprofile ist mit dem anbieterbasierten Abgleich nicht kompatibel. Für den Export in Connect-Kundenprofile müssen Sie den regelbasierten Abgleich oder den auf maschinellem Lernen basierenden Abgleich verwenden.

Falls gewünscht, können Sie AWS Entity Resolution die Ausgabedaten mithilfe eines Hashs versehen — so behalten Sie die Kontrolle über Ihre Daten.

Die folgende Tabelle zeigt die drei Typen von passenden Workflows und ihre unterstützten Ausgabeziele.

Passender Typ	S3-Ausgabe	Ausgabe von Kundenprofilen
regelbasiert	Ja	Ja
basiert auf maschinellem Lernen	Ja	Ja
dienstleistungsorientiert	Ja	Nein

Passende Workflow-Ergebnisse

Nachdem Sie einen passenden Workflow erstellt und ausgeführt haben, können Sie die Ergebnisse an Ihrem angegebenen S3-Standort oder in den Kundenprofilen von Connect einsehen. Abgleichende Workflows generieren IDs, nachdem die Daten indexiert wurden.

Ein passender Workflow kann mehrere Durchläufe haben und die Ergebnisse (Erfolge oder Fehler) werden in einen Ordner mit dem `jobId` als Namen geschrieben.

Für jeden Lauf für S3-Ausgabeziele:

- Die Datenausgabe enthält sowohl eine Datei für erfolgreiche Treffer als auch eine Datei für Fehler
- Erfolgreiche Ergebnisse werden in einen `success` Ordner geschrieben, der mehrere Dateien enthält
- Fehler werden in einen `error` Ordner mit mehreren Feldern geschrieben

Für jeden Lauf für Connect Customer Customer Profiles gelten folgende Ausgabeziele:

- Deduplizierte Kundendatensätze werden direkt an Ihre Connect Customer-Instanz gesendet
- Sie können Ihren letzten Jobverlauf in der Konsole einsehen AWS Entity Resolution
- Bestehende Profile in Connect Customer sind nicht im Deduplizierungsprozess enthalten

Nachdem Sie einen Matching-Workflow erstellt und ausgeführt haben, können Sie die Ergebnisse des regelbasierten Abgleichs oder des maschinellen Lernabgleichs (ML) als Eingabe für den

dienstleistungsbasierten Abgleich verwenden oder umgekehrt, um Ihre Geschäftsanforderungen zu erfüllen.

Um beispielsweise Abonnementkosten für Anbieter zu sparen, können Sie zunächst einen regelbasierten Abgleich ausführen, um Übereinstimmungen in Ihren Daten zu finden. Anschließend können Sie eine Teilmenge der Datensätze, die nicht zugeordnet wurden, an den dienstleistungsbasierten Abgleich des Anbieters senden. Erstellen eines auf dem Provider-Service basierenden Matching-Workflows Beachten Sie, dass Sie beim Exportieren in Kundenprofile nur den regelbasierten oder auf maschinellem Lernen basierenden Abgleich verwenden sollten.

Weitere Informationen zur Behebung von Fehlern finden Sie unter. Fehlerbehebung bei passenden Workflows

Einen regelbasierten Matching-Workflow erstellen

Rule-basedBeim Abgleich handelt es sich um einen hierarchischen Satz von Regeln für den Wasserfallvergleich, der von Ihnen vorgeschlagen wird AWS Entity Resolution, auf der Grundlage der von Ihnen eingegebenen Daten vorgeschlagen wird und von Ihnen vollständig konfiguriert werden kann. Der regelbasierte Abgleichs-Workflow ermöglicht es Ihnen, Klartext- oder Hashdaten zu vergleichen, um anhand von von Ihnen angepasster Kriterien exakte Übereinstimmungen zu finden.

Wenn eine AWS Entity Resolution Übereinstimmung zwischen zwei oder mehr Datensätzen in Ihren Daten gefunden wird, wird Folgendes zugewiesen:

- Eine Match-ID für die Datensätze im übereinstimmenden Datensatz
- Die Match-Regel, die den Treffer generiert hat.

Wenn Sie einen regelbasierten Abgleichs-Workflow in erstellen AWS Entity Resolution, müssen Sie entweder einen einfachen oder einen erweiterten Regeltyp auswählen. Der Regeltyp bestimmt die Komplexität der Regelbedingungen, die Sie erstellen können. Sie können den Regeltyp nach dem Erstellen des Workflows nicht mehr ändern.

Sie können das folgende Diagramm verwenden, um die beiden Regeltypen zu vergleichen und zu ermitteln, welcher für Ihren Anwendungsfall geeignet ist.

Vergleichstabelle für Regeltypen

Anwendungsfall	Erweiterter Regeltyp	Einfacher Regeltyp
Schemazuordnungen, die den Eingabetypen eins zu eins zugeordnet sind	Ja	Nein
Schemazuordnung mit mehreren Datenspalten, die denselben Eingabetypen zugeordnet sind	Nein	Ja
Unterstützt exaktes und Fuzzy-Matching	Ja	Nein (nur exakte Übereinst immung)
Unterstützt AND-, OR- und Klammeroperatoren	Ja	Nein (nur AND-Operator)
Unterstützt Batch-Workflows	Ja	Ja
Unterstützt inkrementelle Workflows	Ja	Ja
Unterstützt Workflows in Echtzeit	Nein	Ja
Unterstützt Workflows zur ID-Mapping	Nein	Ja

Nachdem Sie festgelegt haben, welchen Regeltyp Sie verwenden möchten, verwenden Sie die folgenden Themen, um einen regelbasierten Abgleichsworkflow mit dem Regeltyp „Erweitert“ oder „Einfach“ zu erstellen.

Themen

- Erstellen eines regelbasierten Matching-Workflows mit dem Regeltyp „Erweitert“
- Erstellen eines regelbasierten Matching-Workflows mit dem Regeltyp Einfach

Erstellen eines regelbasierten Matching-Workflows mit dem Regeltyp „Erweitert“

Voraussetzungen

Bevor Sie einen regelbasierten Abgleichs-Workflow erstellen, müssen Sie:

1. Erstellen Sie eine Schemazuordnung. Weitere Informationen finden Sie unter Eine Schemazuordnung erstellen.
2. Wenn Sie Connect Customer Customer Profiles als Ausgabeziel verwenden, stellen Sie sicher, dass Sie die entsprechenden Berechtigungen konfiguriert haben.

Das folgende Verfahren zeigt, wie Sie mithilfe der AWS Entity Resolution Konsole oder der API einen regelbasierten Matching-Workflow mit dem Regeltyp „Erweitert“ erstellen. `CreateMatchingWorkflow`

Console

So erstellen Sie einen regelbasierten Matching-Workflow mit dem Advanced Regeltyp mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Passende Workflows in der oberen rechten Ecke die Option Passenden Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Passende Workflow-Details angeben wie folgt vor:
   a. Geben Sie einen passenden Workflow-Namen und optional eine Beschreibung ein.
   b. Wählen Sie für die Dateneingabe eine AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

      Sie können bis zu 19 Dateneingaben hinzufügen.

      > **Note**
      >
      > Um erweiterte Regeln verwenden zu können, müssen Ihre Schemazuordnungen die folgenden Anforderungen erfüllen:

1. Jedes Eingabefeld muss einem eindeutigen Vergleichsschlüssel zugeordnet werden, es sei denn, die Felder sind gruppiert.
2. Wenn Eingabefelder gruppiert sind, können sie denselben Vergleichsschlüssel verwenden.

   Die folgende Schemazuordnung wäre beispielsweise für erweiterte Regeln gültig:

   ```
   firstName: { matchKey: 'name', groupName: 'name' }

   lastName: { matchKey: 'name', groupName: 'name' }
   ```

   In diesem Fall sind die `lastName` Felder `firstName` und zusammen gruppiert und haben denselben Namensvergleichsschlüssel, was zulässig ist.

   Überprüfen Sie Ihre Schemazuordnungen und aktualisieren Sie sie so, dass sie dieser Eins-zu-Eins-Abgleichsregel folgen, sofern die Felder nicht richtig gruppiert sind, um erweiterte Regeln zu verwenden.
3. Wenn Ihre Datentabelle eine DELETE-Spalte hat, muss der Typ der Schemazuordnung sein `String` und Sie können kein `matchKey` und haben`groupName`.

c. Die Option Daten normalisieren ist standardmäßig ausgewählt, sodass Dateneingaben vor dem Abgleich normalisiert werden. Wenn Sie Daten nicht normalisieren möchten, deaktivieren Sie die Option Daten normalisieren.

> **Note**
>
> Die Normalisierung wird unter Schema-Mapping erstellen nur für die folgenden Szenarien unterstützt:
>
> - Wenn die folgenden Namensuntertypen gruppiert sind: Vorname, zweiter Vorname, Nachname.
> - Wenn die folgenden Adressuntertypen gruppiert sind: Straße 1, Straße 2, Straße 3, Stadt, Bundesland, Land , Postleitzahl.
> - Wenn die folgenden Telefonuntertypen gruppiert sind: Telefonnummer, Telefonvorwahl.

d. Um die Zugriffsberechtigungen für den Dienst festzulegen, wählen Sie eine Option aus und ergreifen Sie die empfohlene Aktion.

Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname für die Servicerolle lautet `entityresolution-matching-workflow-<timestamp>` . • Sie müssen über Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, können Sie die Option Diese Daten sind mit einem KMS-Schlüssel verschlüsselt auswählen und dann einen AWS KMS Schlüssel eingeben, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.

Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt , wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn keine Servicerollen vorhanden sind, ist die Option „Eine vorhanden e Servicerolle verwenden“ nicht verfügbar. 2. Zeigen Sie die Servicerolle an, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

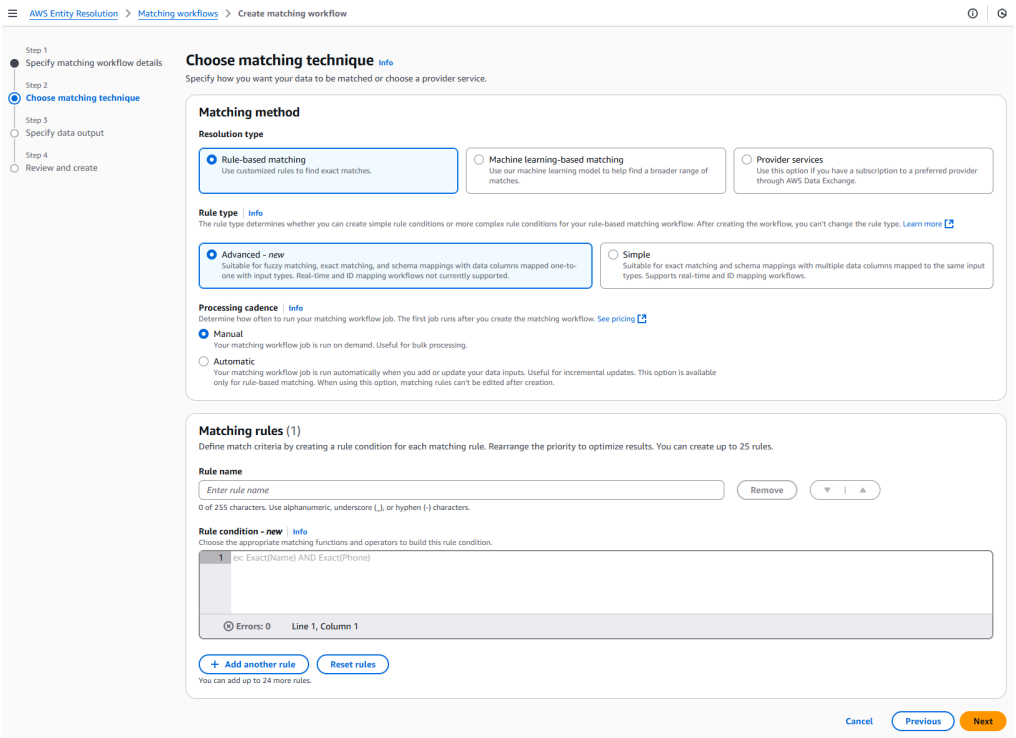
e. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel-Wert-Paar ein.

f. Wählen Sie Weiter aus.

5. Für Schritt 2: Wählen Sie das passende Verfahren aus:

a. Wählen Sie als Vergleichsmethode die Option Rule-based Abgleich aus.

b. Wählen Sie als Regeltyp die Option Erweitert aus.



c. Wählen Sie unter Verarbeitungsrhythmus eine der folgenden Optionen aus.

- Wählen Sie Manuell, um einen Workflow bei Bedarf für eine Massenaktualisierung auszuführen
- Wählen Sie Automatisch, um einen Workflow auszuführen, sobald sich neue Daten in Ihrem S3-Bucket befinden

> **Note**
>
> Wenn Sie Automatisch wählen, stellen Sie sicher, dass Sie EventBridge Amazon-Benachrichtigungen für Ihren S3-Bucket aktiviert haben. Anweisungen zur Aktivierung EventBridge von Amazon mithilfe der S3-Konsole finden Sie unter Enabling Amazon EventBridge im Amazon S3-Benutzerhandbuch.

d. Geben Sie für Übereinstimmungsregeln einen Regelnamen ein und erstellen Sie dann die Regelbedingung, indem Sie die entsprechenden passenden Funktionen und Operatoren aus der Dropdownliste auswählen, die Ihrem Ziel entsprechen.

Sie können bis zu 25 Regeln erstellen.

> **Note**
>
> AWS Entity Resolution unterstützt auch transitiven Abgleich, bei dem Datensätze auf allen Regelebenen verarbeitet werden, um Übereinstimmungsgruppen transitiv zu verbinden. Transitiver Abgleich ist als Funktion verfügbar. API-only Wenn transitiver Abgleich aktiviert ist, wird der Modifikator EmptyValues =Ignore nicht unterstützt. Weitere Informationen finden Sie unter Verwendung von transitivem Matching.

Sie müssen eine Fuzzy-Matching-Funktion (Cosine, Levenshtein oder Soundex) mit einer Exact-Matching-Funktion (Exact,) mithilfe des AND-Operators kombinieren. ExactManyToMany

Anhand der folgenden Tabelle können Sie je nach Ihrem Ziel entscheiden, welche Art von Funktion oder Operator Sie verwenden möchten.

Ihr Ziel	Empfohlene Funktion oder Bediener	Empfohlener optionaler Modifikator	Vorteile
Ordnen Sie identische Zeichenfolgen mit genauen Daten zu, passen Sie jedoch nicht zu leeren Werten.	Exact (Genau)	EmptyValues=Prozess	
Ordne identische Zeichenketten den korrekten Daten zu und ignoriere leere Werte.	Exakt (***matchKey***)	EmptyValues=Ignorieren	

Ihr Ziel	Empfohlene Funktion oder Bediener	Empfohlener optionaler Modifikator	Vorteile
Ordnet mehrere Datensätze mit den passenden Schlüsseln zu. Geeignet für flexible Kombinationen. Limit: 15 Kombinationsschlüssel	ExactManyToMany(*matchKey*, *matchKey*, ...)	n/a	
Misst die Ähnlichkeit zwischen numerischen Repräsentationen von Daten, ohne dass bei leeren Werten eine Übereinstimmung erzielt wird. Geeignet für Text, Zahlen oder eine Mischung aus beidem.	Kosinus	EmptyValues=Prozess	Einfach, effizient. Funktioniert gut mit langem Text, wenn er mit TF-IDF Gewichtung kombiniert wird. Gut für exakte wortbasierte Übereinstimmungen.

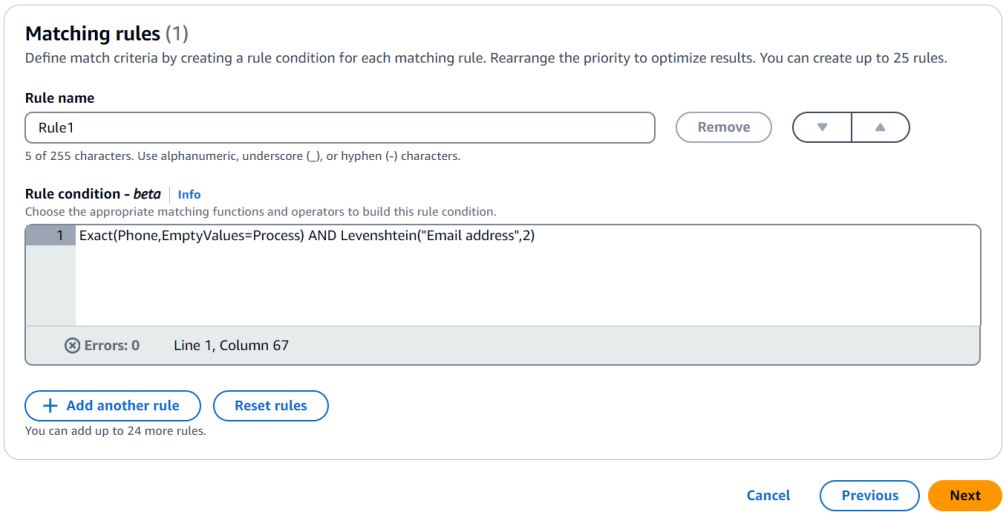
Ihr Ziel	Empfohlene Funktion oder Bediener	Empfohlener optionaler Modifikator	Vorteile
Messen Sie die Ähnlichkeit zwischen numerischen Darstellungen von Daten und ignorieren Sie leere Werte.	Kosinus (*matchKey*,*thresh* ,...)	EmptyValues=Ignorieren	Behandelt Tippfehler, Rechtschreibfehler und Transpositionen gut. Wirksam bei einer Vielzahl von PII-Typen.
Zählen Sie die Mindestanzahl der Änderungen, die erforderlich sind, um ein Wort in ein anderes zu ändern, aber passen Sie nicht mit leeren Werten zusammen. Geeignet für Text mit leichten Unterschieden in der Schreibweise.	Levenshtein	EmptyValues=Prozess	Gut für kurze Zeichenketten (z. B. Namen oder Telefonnummern).
Zählen Sie die Mindestanzahl der Änderungen, die erforderlich sind, um ein Wort in ein anderes umzuwandeln, und ignorieren Sie leere Werte.	Levenshtein (*matchKey*,,*thresh* ...)	EmptyValues=Ignorieren	

Ihr Ziel	Empfohlene Funktion oder Bediener	Empfohlener optionaler Modifikator	Vorteile
Vergleichen und vergleichen Sie Textzeichenfolgen danach, wie ähnlich sie klingen, aber bei leeren Werten stimmen sie nicht überein. Geeignet für Text mit Variationen in der Schreibweise oder Aussprache.	Soundex	EmptyValues=Prozess	Effektiv für den phonetischen Abgleich, um ähnlich klingende Wörter zu identifizieren. Schnell und rechnerisch kostengünstig. Gut geeignet, um Namen mit ähnlicher Aussprache, aber unterschiedlicher Schreibweise abzugleichen.
Vergleichen und ordnen Sie Textzeichenfolgen danach, wie ähnlich sie klingen, und ignorieren Sie leere Werte.	Soundex () ***matchKey***	EmptyValues=Ignorieren	
Funktionen kombinieren.	UND	n/a	
Separate Funktionen.	ODER	n/a	
Gruppieren Sie Bedingungen, um verschachtelte Bedingungen zu erstellen.	(…)	n/a	

Example Regelbedingung, die auf Telefonnummern und E-Mails zutrifft

Im Folgenden finden Sie ein Beispiel für eine Regelbedingung, die Datensätze zu Telefonnummern (Vergleichsschlüssel für Telefonnummern) und E-Mail-Adressen (Vergleichstaste für E-Mail-Adressen) abgleicht:

```
Exact(Phone,EmptyValues=Process) AND Levenshtein("Email address",2)
```



Die Taste „Telefonabgleich“ verwendet die Funktion „Exakte Übereinstimmung“, um identische Zeichenfolgen abzugleichen. Die Taste „Telefonabgleich“ verarbeitet leere Werte beim Abgleich mithilfe des Modifikators EmptyValues =Process.

Der Schlüssel „E-Mail-Adresse abgleichen“ verwendet die Levenshtein-Matching-Funktion, um Daten mit Rechtschreibfehlern abzugleichen. Dabei wird der Standardschwellenwert 2 für den Levenshtein-Entfernungsalgorithmus verwendet. Der Suchschlüssel „E-Mail“ verwendet keine optionalen Modifikatoren.

Der AND-Operator kombiniert die Exact-Matching-Funktion und die Levenshtein-Matching-Funktion.

Example Regelbedingung, die verwendet wird, um den ExactManyToMany Matchkey-Abgleich durchzuführen

Im Folgenden finden Sie ein Beispiel für eine Regelbedingung, die Datensätze in drei Adressfeldern (HomeAddressVergleichsschlüssel, BillingAddress

Vergleichsschlüssel und ShippingAddress Vergleichsschlüssel) vergleicht, um potenzielle Übereinstimmungen zu finden, indem überprüft wird, ob einige davon identische Werte haben.

Der `ExactManyToMany` Operator wertet alle möglichen Kombinationen der angegebenen Adressfelder aus, um genaue Übereinstimmungen zwischen zwei oder mehr Adressen zu ermitteln. Beispielsweise würde er erkennen, ob die Adresse entweder dem `BillingAddress` oder `HomeAddress` entsprich`ShippingAddress`, oder ob alle drei Adressen exakt übereinstimmen.

```
ExactManyToMany(HomeAddress, BillingAddress, ShippingAddress)
```

Example Regelbedingung, die Clustering verwendet

Beim erweiterten regelbasierten Abgleich mit Fuzzy-Bedingungen gruppiert das System Datensätze zunächst anhand exakter Übereinstimmungen in Cluster. Sobald diese ersten Cluster gebildet sind, wendet das System Fuzzy-Matching-Filter an, um weitere Treffer innerhalb jedes Clusters zu identifizieren. Für eine optimale Leistung sollten Sie auf der Grundlage Ihrer Datenmuster exakte Übereinstimmungsbedingungen auswählen, um klar definierte Anfangscluster zu erstellen.

Im Folgenden finden Sie ein Beispiel für eine Regelbedingung, die mehrere exakte Übereinstimmungen mit einer Fuzzy-Match-Anforderung kombiniert. Es verwendet `AND` Operatoren, um zu überprüfen`FullName`, ob die drei Felder — Geburtsdatum (`DOB`) und `Address` — zwischen den Datensätzen exakt übereinstimmen. Es ermöglicht auch geringfügige Variationen im `InternalID` Feld unter Verwendung einer Levenshtein-Distanz von. 1 Die Levenshtein-Distanz misst die Mindestanzahl von Änderungen an einem Zeichen, die erforderlich sind, um eine Zeichenfolge in eine andere umzuwandeln. Ein Abstand von 1 bedeutet, `InternalIDs` dass es sich um Übereinstimmungen handelt, die sich nur um ein Zeichen unterscheiden (wie ein einziger Tippfehler, Löschen oder Einfügen). Diese Kombination von Bedingungen hilft bei der Identifizierung von Datensätzen, die mit großer Wahrscheinlichkeit dieselbe Entität repräsentieren, selbst wenn der Bezeichner kleine Abweichungen aufweist.

```
Exact(FullName) AND Exact(DOB) AND Exact(Address) and
 Levenshtein(InternalID, 1)
```

e. Wählen Sie Weiter aus.

6. Für Schritt 3: Geben Sie die Datenausgabe und das Format an:

   a. Wählen Sie für Datenausgabeziel und -format den Amazon S3-Speicherort für die Datenausgabe aus und geben Sie an, ob das Datenformat Normalisierte Daten oder Originaldaten sein soll.

   b. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen möchten, geben Sie den AWS KMS Schlüssel-ARN ein.

   c. Sehen Sie sich die vom System generierte Ausgabe an.

   d. Entscheiden Sie für die Datenausgabe, welche Felder Sie einbeziehen, ausblenden oder maskieren möchten, und ergreifen Sie dann die empfohlenen Maßnahmen, die auf Ihren Zielen basieren.

Ihr Ziel	Empfohlene Aktion
Felder einbeziehen	Behalten Sie den Ausgabestatus „Eingeschlossen“ bei.
Felder ausblenden (von der Ausgabe ausschließen)	Wählen Sie das Ausgabefeld aus und wählen Sie dann Ausblenden.
Felder maskieren	Wählen Sie das Ausgabefeld und dann Hash-Ausgabe.
Setzen Sie die vorherigen Einstellungen zurück	Klicken Sie auf Reset (Zurücksetzen).

   e. Wählen Sie Weiter aus.

7. Für Schritt 4: Prüfen und erstellen Sie:

   a. Überprüfen Sie die Auswahl, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Create and run aus.

   Es wird eine Meldung angezeigt, die darauf hinweist, dass der entsprechende Workflow erstellt und der Job gestartet wurde.

8. Sehen Sie sich auf der Seite mit den Details des passenden Workflows auf der Registerkarte Metriken unter Letzte Job-Metriken Folgendes an:

- Die Job-ID.
- Der Status des passenden Workflow-Jobs: In Warteschlange, In Bearbeitung, Abgeschlossen, Fehlgeschlagen
- Die Zeit, in der der Workflow-Job abgeschlossen wurde.
- Die Anzahl der verarbeiteten Datensätze.
- Die Anzahl der Datensätze, die nicht verarbeitet wurden.
- Die generierten eindeutigen Match-IDs.
- Die Anzahl der Eingabedatensätze.

Sie können auch die Job-Metriken für übereinstimmende Workflow-Jobs, die zuvor ausgeführt wurden, im Auftragsverlauf anzeigen.

9. Nachdem der passende Workflow-Job abgeschlossen ist (Status ist abgeschlossen), können Sie zur Registerkarte Datenausgabe wechseln und dann Ihren Amazon S3-Standort auswählen, um die Ergebnisse anzuzeigen.
10. (Nur manueller Verarbeitungstyp) Wenn Sie einen Rule-based passenden Workflow mit dem Verarbeitungstyp Manuell erstellt haben, können Sie den passenden Workflow jederzeit ausführen, indem Sie auf der Seite mit den passenden Workflow-Details die Option Workflow ausführen auswählen.
11. (Nur automatische Verarbeitungsart) Wenn Ihre Datentabelle eine DELETE-Spalte enthält, dann:

    - Datensätze, die `true` in der DELETE-Spalte auf gesetzt sind, werden gelöscht.
    - Datensätze, die `false` in der DELETE-Spalte auf gesetzt sind, werden in S3 aufgenommen.

    Weitere Informationen finden Sie unter Schritt 1: Bereiten Sie Datentabellen von Erstanbietern vor.

API

Um einen regelbasierten Matching-Workflow zu erstellen, verwenden Sie den Advanced Regeltyp mithilfe der API

> **Note**
>
> Standardmäßig verwendet der Workflow die Standardverarbeitung (Batch-) Verarbeitung. Um die inkrementelle (automatische) Verarbeitung zu verwenden, müssen Sie sie explizit konfigurieren.

1. Öffnen Sie ein Terminal oder eine Eingabeaufforderung, um die API-Anfrage zu stellen.
2. Erstellen Sie eine POST-Anfrage an den folgenden Endpunkt:

```
/matchingworkflows
```

3. Stellen Sie im Anforderungsheader das Content-type auf ein application/json.

> **Note**
>
> Eine vollständige Liste der unterstützten Programmiersprachen finden Sie in der AWS Entity Resolution API-Referenz .

4. Geben Sie für den Anforderungstext die folgenden erforderlichen JSON-Parameter an:

```
{
   "description": "string",
   "incrementalRunConfig": {
      "incrementalRunType": "string"
   },
   "inputSourceConfig": [
      {
         "applyNormalization": boolean,
         "inputSourceARN": "string",
         "schemaName": "string"
      }
   ],
   "outputSourceConfig": [
      {
         "applyNormalization": boolean,
```

```
         "KMSArn": "string",
         "output": [
            {
               "hashed": boolean,
               "name": "string"
            }
         ],
         "outputS3Path": "string"
      }
   ],
   "resolutionTechniques": {
      "providerProperties": {
         "intermediateSourceConfiguration": {
            "intermediateS3Path": "string"
         },
         "providerConfiguration": JSON value,
         "providerServiceArn": "string"
      },
      "resolutionType": "RULE_MATCHING",
      "ruleBasedProperties": {
         "attributeMatchingModel": "string",
         "matchPurpose": "string",
         "rules": [
            {
               "matchingKeys": [ "string" ],
               "ruleName": "string"
            }
         ]
      },
      "ruleConditionProperties": {
         "rules": [
            {
               "condition": "string",
               "ruleName": "string"
            }
         ]
      }
   },
   "roleArn": "string",
   "tags": {
      "string" : "string"
   },
   "workflowName": "string"
```

```
}
```

Wobei Folgendes gilt:

- `workflowName`(erforderlich) — Muss eindeutig sein und zwischen 1—255 Zeichen müssen dem Muster [a-z A-Z _0-9-] * entsprechen
- `inputSourceConfig`(erforderlich) — Liste mit 1—20 Eingangsquellenkonfigurationen
- `outputSourceConfig`(erforderlich) — Genau eine Ausgangsquellenkonfiguration
- `resolutionTechniques`(erforderlich) — Stellen Sie „RULE_MATCHING“ als ResolutionType für den regelbasierten Abgleich ein
- `roleArn`(erforderlich) — IAM-Rollen-ARN für die Workflow-Ausführung
- `ruleConditionProperties`(erforderlich) — Liste der Regelbedingungen und der Name der passenden Regel.

Zu den optionalen Parametern gehören:

- `description`— Bis zu 255 Zeichen
- `incrementalRunConfig`— Inkrementelle Konfiguration des Lauftyps
- `tags`— Bis zu 200 Schlüssel-Wert-Paare

5. (Optional) Um die inkrementelle Verarbeitung anstelle der standardmäßigen Standardverarbeitung (Batch) zu verwenden, fügen Sie dem Anforderungstext den folgenden Parameter hinzu:

```
"incrementalRunConfig": {
   "incrementalRunType": "AUTOMATIC"
}
```

6. Senden Sie die Anforderung .
7. Bei Erfolg erhalten Sie eine Antwort mit dem Statuscode 200 und einem JSON-Text, der Folgendes enthält:

```
{
   "workflowArn": "string",
   "workflowName": "string",
   // Plus all configured workflow details
}
```

8. Wenn der Anruf nicht erfolgreich ist, erhalten Sie möglicherweise eine der folgenden Fehlermeldungen:

   - 400 — ConflictException wenn der Workflow-Name bereits existiert
   - 400 — ValidationException wenn die Eingabe die Überprüfung nicht besteht
   - 402 — ExceedsLimitException wenn Kontolimits überschritten werden
   - 403 — AccessDeniedException wenn Sie nicht über ausreichenden Zugriff verfügen
   - 429 — ThrottlingException wenn die Anfrage gedrosselt wurde
   - 500 — InternalServerException wenn ein interner Servicefehler vorliegt

Verwendung von transitivem Matching

AWS Entity Resolution Verwendet standardmäßig einen Wasserfallabgleich, bei dem Datensätze, die auf einer höheren Regelebene übereinstimmen, von nachfolgenden Regeln ausgeschlossen werden. Das bedeutet, dass nur Datensätze, die keine Übereinstimmung aufweisen, von der nächsten Regel ausgewertet werden. Dieser Ansatz eignet sich zwar gut für den Abgleich aus einer einzigen Quelle, kann jedoch zu Problemen führen, wenn Sie mehrere Datenquellen mit unterschiedlichen Attributen haben.

Beim Wasserfall-Ansatz müssen Sie möglicherweise die gesamte Abgleichslogik in einer einzigen übermäßig freizügigen Regel kombinieren, um Datensätze quellenübergreifend abzugleichen. Dies kann zu Überübereinstimmungen führen, bei denen Datensätze, bei denen es sich nicht um echte Übereinstimmungen handelt, fälschlicherweise gruppiert werden.

Transitiver Abgleich löst dieses Problem, indem alle Datensätze auf allen Regelebenen verarbeitet werden. Sobald ein Datensatz mit einer Regel übereinstimmt, ist seine Abgleichs-ID festgelegt. Der Datensatz kann jedoch weiterhin als Link dienen, um Datensätze, die nicht übereinstimmen, aus späteren Regeln mit Übereinstimmungsgruppen aus früheren Regeln zu verbinden. Diese Funktion ist derzeit nur über die API verfügbar.

Wie funktioniert transitives Matching

Beim transitiven Abgleich wird für jede Übereinstimmungsgruppe in der aktuellen Regel das folgende Verfahren zur Auflösung der Match-ID verwendet:

- Das System prüft, ob ein Datensatz in der Gruppe bereits eine Übereinstimmungs-ID aus einer früheren Regelebene hat.
- Wenn eine Match-ID existiert, erbt die gesamte Gruppe diese frühere Match-ID.

- Wenn mehrere Kandidaten vorhanden sind, wird die kleinste Match-ID aus der frühesten Regelebene ausgewählt.
- Wenn keine vorherige Übereinstimmung existiert, wird der Gruppe eine neue Match-ID zugewiesen.

Transitiven Abgleich (API) aktivieren

> **Important**
>
> Transitiver Abgleich ist eine API-only Funktion. Sie können den transitiven Abgleich nicht über die AWS Entity Resolution Konsole aktivieren.

Um den transitiven Abgleich zu verwenden, müssen Sie mithilfe der API einen neuen Matching-Workflow mit dem Regeltyp „Erweitert“ erstellen. `CreateMatchingWorkflow` Sie können einem vorhandenen Workflow keinen transitiven Abgleich hinzufügen.

Nehmen Sie den `matchingConfig` Parameter mit `enableTransitiveMatching` set auf `true` in den Anforderungstext auf auf auf. Das folgende Beispiel zeigt einen vollständigen `CreateMatchingWorkflow` Anforderungstext mit aktiviertem transitiven Abgleich:

```
{
   "workflowName": "my-transitive-workflow",
   "inputSourceConfig": [
      {
         "inputSourceARN": "arn:aws:glue:us-east-1:123456789012:table/my-database/my-
table",
         "schemaName": "my-schema",
         "applyNormalization": true
      }
   ],
   "outputSourceConfig": [
      {
         "outputS3Path": "s3://my-bucket/output/",
         "output": [
            {
               "name": "name",
               "hashed": false
            }
         ]
```

```
      }
   ],
   "resolutionTechniques": {
      "resolutionType": "RULE_MATCHING",
      "ruleConditionProperties": {
         "rules": [
            {
               "ruleName": "Rule1",
               "condition": "Exact(Email) AND Exact(Phone)"
            },
            {
               "ruleName": "Rule2",
               "condition": "Exact(Name) AND Exact(Address)"
            }
         ]
      }
   },
   "matchingConfig": {
      "enableTransitiveMatching": true
   },
   "roleArn": "arn:aws:iam::123456789012:role/my-er-role"
}
```

> **Important**
>
> Der `enableTransitiveMatching` Parameter ist unveränderlich. Sie können diesen Parameter nur bei der Workflow-Erstellung festlegen und danach nicht mehr ändern.

Bewährte Methoden für die Reihenfolge von Regeln

Wenn Sie transitiven Abgleich verwenden, ist die Reihenfolge der Regeln von entscheidender Bedeutung. Folgen Sie diesen bewährten Methoden:

- Ordnen Sie die Regeln von der spezifischsten (höchste Konfidenz) bis zur unspezifischsten Reihenfolge an.
- Ordnen Sie für eindeutige Identifikationsattribute wie SSN oder Geburtsdatum die Regeln in benachbarten Paaren an — eine Regel, die das Attribut enthält, und die nächste Regel ohne es. Auf diese Weise kann das System Datensätze, denen diese Attribute fehlen, ordnungsgemäß behandeln.

- Beachten Sie, dass sich die Anzahl der Regeln auf die Workflow-Latenz auswirkt, da Datensätze auf allen Regelebenen verarbeitet werden.

Einschränkungen

Beim transitiven Abgleich gelten die folgenden Einschränkungen:

- Nur für Advanced Matching-Workflows verfügbar. Nicht verfügbar für Matching-Workflows vom Typ „Einfache Regeln“ oder auf maschinellem Lernen basierende Workflows.
- Der Modifikator EmptyValues =Ignore wird nicht unterstützt, wenn transitiver Abgleich aktiviert ist. Der transitive Abgleich beinhaltet eine integrierte Behandlung leerer Werte, die Überübereinstimmungen verhindert.
- Die Workflow-Laufzeit steigt proportional mit der Anzahl der definierten Regeln, da Datensätze auf allen Regelebenen verarbeitet werden.
- Die `enableTransitiveMatching` Einstellung kann nur während der Workflow-Erstellung konfiguriert werden. Um transitives Matching verwenden zu können, müssen Sie einen neuen Workflow erstellen.
- Sie sind dafür verantwortlich, die Regeln korrekt anzuordnen. Regeln mit mehr Attributen müssen vor Regeln mit weniger Attributen stehen. Eine falsche Reihenfolge kann dazu führen, dass Datensätze mit unterschiedlichen Werten für eindeutige Felder (wie Geburtsdatum oder SSN) falsch gruppiert werden.

Deaktivieren des transitiven Abgleichs

Die Einstellung `enableTransitiveMatching` ist unveränderlich. Sie können diese Einstellung nicht ändern, nachdem Sie einen Workflow erstellt haben.

Um den transitiven Abgleich zu deaktivieren, müssen Sie einen neuen Matching-Workflow ohne den `enableTransitiveMatching` Parameter erstellen oder ihn `false` in der `CreateMatchingWorkflow` API-Anforderung auf setzen. Es gibt keine AWS Entity Resolution Konsolenoption zum Deaktivieren des transitiven Abgleichs.

Gehen Sie wie folgt vor, um einen transitiven Matching-Workflow durch einen nicht-transitiven Workflow zu ersetzen:

1. Erstellen Sie einen neuen Matching-Workflow mithilfe der `CreateMatchingWorkflow` API ohne den `matchingConfig` Parameter oder mit `enableTransitiveMatching` set auf. `false`

2. Führen Sie den neuen Workflow aus, um sicherzustellen, dass er die erwarteten Ergebnisse liefert.
3. Löschen Sie den alten transitiven Matching-Workflow, falls er nicht mehr benötigt wird. Weitere Informationen finden Sie unter Einen passenden Workflow löschen.

Leistungsaspekte

Transitive Matching-Workflows sind langsamer als nicht-transitive Workflows, da Datensätze auf allen Regelebenen verarbeitet werden, anstatt nach ihrer ersten Übereinstimmung ausgeschlossen zu werden. Die folgenden Faktoren wirken sich auf die Leistung aus:

Anzahl der Regeln

: Mehr Regeln führen zu mehr Verarbeitungszeit. Jede zusätzliche Regelebene fügt Merge-Iterationen hinzu, da das System Match-IDs auf allen Ebenen weitergeben muss.

Batch- und inkrementelle Verarbeitung

: Inkrementelle Workflows haben einen höheren Overhead als Batch-Workflows in großem Maßstab. Größere Basis-Datensatzspeicher erfordern mehr Merge-Iterationen, um Match-IDs auf bestehende und neue Datensätze zu übertragen.

Verzerrte Datenverteilung

: Datensätze mit schiefen Verteilungen, wie z. B. große Übereinstimmungsgruppen, erhöhen den Overhead. Wenn viele Datensätze mit derselben Vergleichsgruppe verknüpft sind, benötigt das System mehr transitive Verknüpfungen, um alle Verbindungen aufzulösen.

Wir empfehlen, transitive Matching-Workflows mit repräsentativen Datenmengen zu testen, bevor Sie sie in der Produktion verwenden. Dies hilft Ihnen, die Leistungsmerkmale Ihrer spezifischen Daten- und Regelkonfiguration zu verstehen.

Erstellen eines regelbasierten Matching-Workflows mit dem Regeltyp Einfach

Voraussetzungen

Bevor Sie einen regelbasierten Abgleichs-Workflow erstellen, müssen Sie:

1. Erstellen Sie eine Schemazuordnung. Weitere Informationen finden Sie unter Eine Schemazuordnung erstellen.

2. Wenn Sie Connect Customer Customer Profiles als Ausgabeziel verwenden, stellen Sie sicher, dass Sie die entsprechenden Berechtigungen konfiguriert haben.

Das folgende Verfahren zeigt, wie Sie mithilfe der AWS Entity Resolution Konsole oder der API einen regelbasierten Matching-Workflow mit dem Regeltyp Simple erstellen. `CreateMatchingWorkflow`

Console

So erstellen Sie einen regelbasierten Matching-Workflow mit dem Einfach Regeltyp mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Passende Workflows in der oberen rechten Ecke die Option Passenden Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Passende Workflow-Details angeben wie folgt vor:
   a. Geben Sie einen passenden Workflow-Namen und optional eine Beschreibung ein.
   b. Wählen Sie für die Dateneingabe eine AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

      Sie können bis zu 19 Dateneingaben hinzufügen.
   c. Die Option Daten normalisieren ist standardmäßig ausgewählt, sodass Dateneingaben vor dem Abgleich normalisiert werden. Wenn Sie Daten nicht normalisieren möchten, deaktivieren Sie die Option Daten normalisieren.

      > **Note**
      >
      > Die Normalisierung wird unter Schema-Mapping erstellen nur für die folgenden Szenarien unterstützt:
      >
      > - Wenn die folgenden Namensuntertypen gruppiert sind: Vorname, zweiter Vorname, Nachname.
      > - Wenn die folgenden Adressuntertypen gruppiert sind: Straße 1, Straße 2, Straße 3, Stadt, Bundesland, Land , Postleitzahl.

- Wenn die folgenden Telefonuntertypen gruppiert sind: Telefonnummer, Telefonvorwahl.

d. Um die Zugriffsberechtigungen für den Dienst festzulegen, wählen Sie eine Option aus und ergreifen Sie die empfohlene Aktion.

Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname für die Servicerolle lautet `entityresolution-matching-workflow-<timestamp>` . • Sie müssen über Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, können Sie die Option Diese Daten sind mit einem KMS-Schlüssel verschlüsselt auswählen und dann einen AWS KMS Schlüssel eingeben, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.

Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt , wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn keine Servicerollen vorhanden sind, ist die Option „Eine vorhanden e Servicerolle verwenden“ nicht verfügbar. 2. Zeigen Sie die Servicerolle an, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

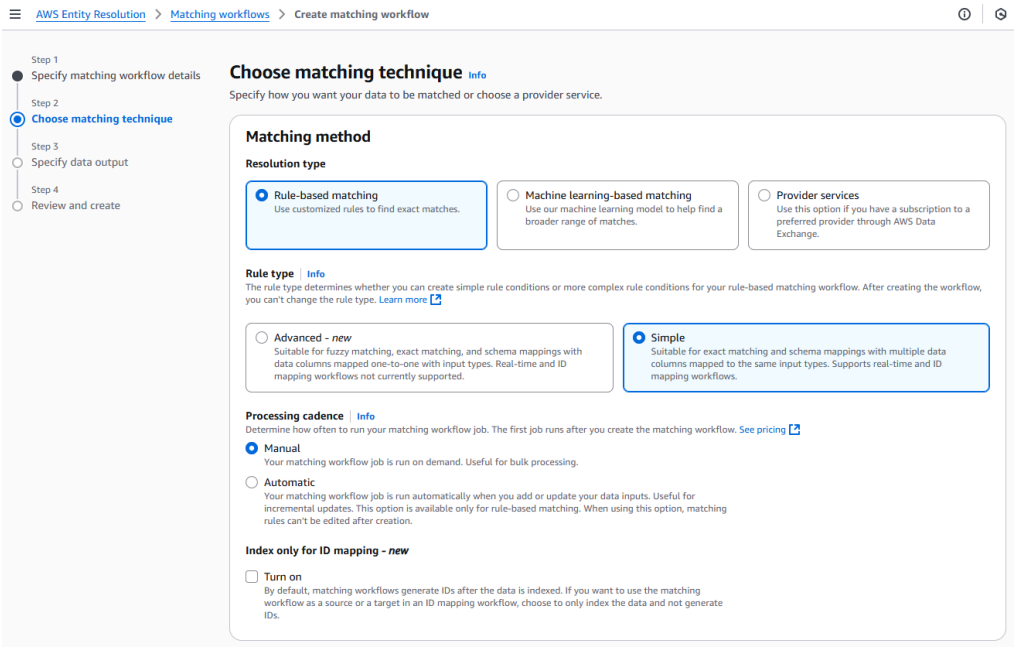
e. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel-Wert-Paar ein.

f. Wählen Sie Weiter aus.

5. Für Schritt 2: Wählen Sie das passende Verfahren aus:

a. Wählen Sie als Vergleichsmethode die Option Rule-based Abgleich aus.

b. Wählen Sie als Regeltyp die Option Einfach aus.



c. Wählen Sie für den Verarbeitungsrhythmus eine der folgenden Optionen aus.

- Wählen Sie Manuell, um einen Workflow bei Bedarf für eine Massenaktualisierung auszuführen
- Wählen Sie Automatisch, um einen Workflow auszuführen, sobald sich neue Daten in Ihrem S3-Bucket befinden

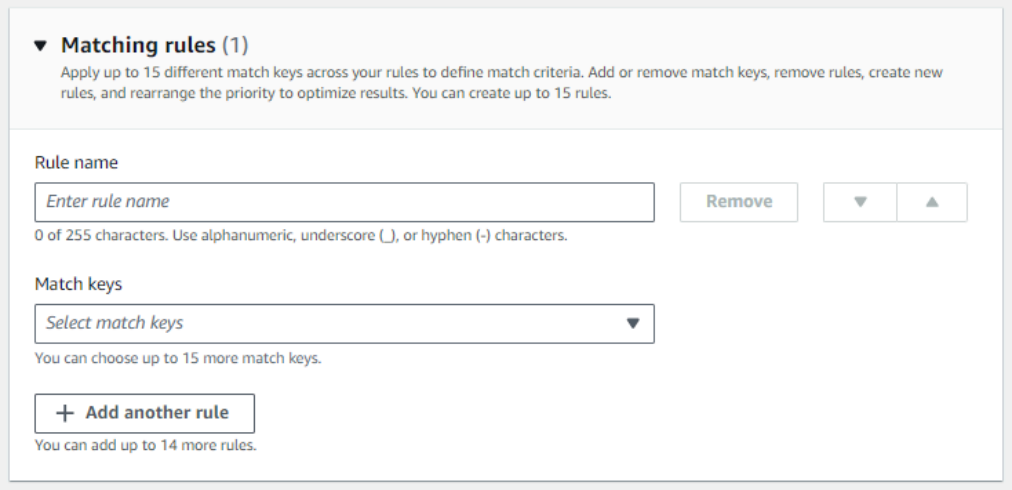
> **Note**
>
> Wenn Sie Automatisch wählen, stellen Sie sicher, dass Sie EventBridge Amazon-Benachrichtigungen für Ihren S3-Bucket aktiviert haben. Anweisungen zur Aktivierung EventBridge von Amazon mithilfe der S3-Konsole finden Sie unter Enabling Amazon EventBridge im Amazon S3-Benutzerhandbuch.

d. (Optional) Wenn nur der Index für die ID-Zuordnung verwendet wird, können Sie wählen, ob Sie die Möglichkeit aktivieren möchten, nur die Daten zu indizieren und keine IDs zu generieren.

   Standardmäßig generieren übereinstimmende Workflows IDs, nachdem die Daten indexiert wurden.

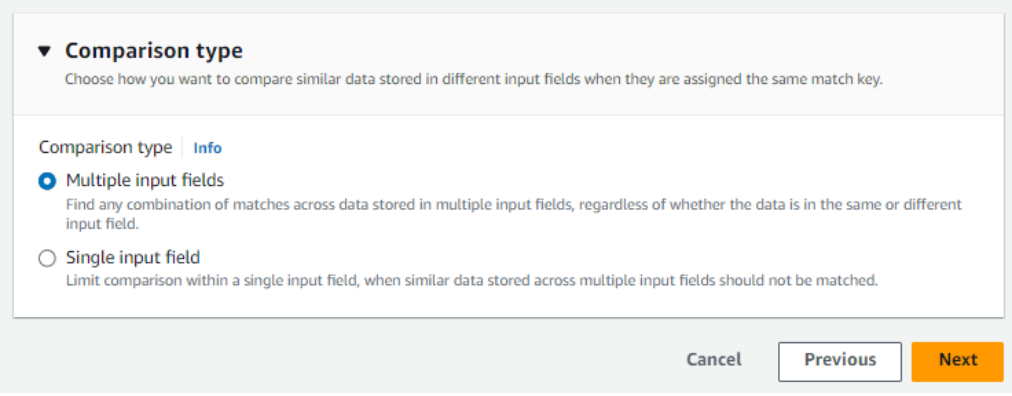
e. Geben Sie für Übereinstimmungsregeln einen Regelnamen ein und wählen Sie dann die Abgleichsschlüssel für diese Regel aus.

Sie können bis zu 15 Regeln erstellen und bis zu 15 verschiedene Vergleichsschlüssel auf Ihre Regeln anwenden, um Übereinstimmungskriterien zu definieren.



f. Wählen Sie für den Vergleichstyp je nach Ziel eine der folgenden Optionen aus.

Ihr Ziel	Empfohlene Option
Finden Sie eine beliebige Kombination von Übereinstimmungen in Daten, die in mehreren Eingabefeldern gespeichert sind	Mehrere Eingabefelder
Beschränken Sie den Vergleich auf ein einziges Eingabefeld	Einzelnes Eingabefeld



g. Wählen Sie Weiter aus.

6. Für Schritt 3: Geben Sie die Datenausgabe und das Format an:

   a. Wählen Sie für Datenausgabeziel und -format den Amazon S3-Speicherort für die Datenausgabe aus und geben Sie an, ob das Datenformat Normalisierte Daten oder Originaldaten sein soll.

   b. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen möchten, geben Sie den AWS KMS Schlüssel-ARN ein.

   c. Sehen Sie sich die vom System generierte Ausgabe an.

   d. Entscheiden Sie für die Datenausgabe, welche Felder Sie einbeziehen, ausblenden oder maskieren möchten, und ergreifen Sie dann die empfohlenen Maßnahmen, die auf Ihren Zielen basieren.

Ihr Ziel	Empfohlene Aktion
Felder einbeziehen	Behalten Sie den Ausgabestatus „Eingeschlossen“ bei.
Felder ausblenden (aus der Ausgabe ausschließen)	Wählen Sie das Ausgabefeld aus und wählen Sie dann Ausblenden.
Felder maskieren	Wählen Sie das Ausgabefeld und dann Hash-Ausgabe.
Setzen Sie die vorherigen Einstellungen zurück	Klicken Sie auf Reset (Zurücksetzen).

   e. Wählen Sie Weiter aus.

7. Für Schritt 4: Prüfen und erstellen Sie:

   a. Überprüfen Sie die Auswahl, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Create and run aus.

   Es wird eine Meldung angezeigt, die darauf hinweist, dass der entsprechende Workflow erstellt und der Job gestartet wurde.

8. Sehen Sie sich auf der Seite mit den Details des passenden Workflows auf der Registerkarte Metriken unter Letzte Job-Metriken Folgendes an:

- Die Job-ID.
- Der Status des passenden Workflow-Jobs: In Warteschlange, In Bearbeitung, Abgeschlossen, Fehlgeschlagen
- Die Zeit, in der der Workflow-Job abgeschlossen wurde.
- Die Anzahl der verarbeiteten Datensätze.
- Die Anzahl der Datensätze, die nicht verarbeitet wurden.
- Die generierten eindeutigen Match-IDs.
- Die Anzahl der Eingabedatensätze.

Sie können auch die Job-Metriken für übereinstimmende Workflow-Jobs, die zuvor ausgeführt wurden, im Auftragsverlauf anzeigen.

9. Nachdem der passende Workflow-Job abgeschlossen ist (Status ist abgeschlossen), können Sie zur Registerkarte Datenausgabe wechseln und dann Ihren Amazon S3-Standort auswählen, um die Ergebnisse anzuzeigen.
10. (Nur manueller Verarbeitungstyp) Wenn Sie einen Rule-based passenden Workflow mit dem Verarbeitungstyp Manuell erstellt haben, können Sie den passenden Workflow jederzeit ausführen, indem Sie auf der Seite mit den passenden Workflow-Details die Option Workflow ausführen auswählen.

API

Um einen regelbasierten Matching-Workflow zu erstellen, verwenden Sie den Einfach Regeltyp mithilfe der API

> **Note**
>
> Standardmäßig verwendet der Workflow die Standardverarbeitung (Batch-) Verarbeitung. Um die inkrementelle (automatische) Verarbeitung zu verwenden, müssen Sie sie explizit konfigurieren.

1. Öffnen Sie ein Terminal oder eine Eingabeaufforderung, um die API-Anfrage zu stellen.
2. Erstellen Sie eine POST-Anfrage an den folgenden Endpunkt:

```
/matchingworkflows
```

3. Stellen Sie im Anforderungsheader das Content-type auf ein application/json.

> **Note**
>
> Eine vollständige Liste der unterstützten Programmiersprachen finden Sie in der AWS Entity Resolution API-Referenz .

4. Geben Sie für den Anforderungstext die folgenden erforderlichen JSON-Parameter an:

```
{
   "description": "string",
   "incrementalRunConfig": {
      "incrementalRunType": "string"
   },
   "inputSourceConfig": [
      {
         "applyNormalization": boolean,
         "inputSourceARN": "string",
         "schemaName": "string"
      }
   ],
   "outputSourceConfig": [
      {
         "applyNormalization": boolean,
         "KMSArn": "string",
         "output": [
            {
               "hashed": boolean,
               "name": "string"
            }
         ],
         "outputS3Path": "string"
      }
   ],
   "resolutionTechniques": {
      "providerProperties": {
         "intermediateSourceConfiguration": {
            "intermediateS3Path": "string"
         },
         "providerConfiguration": JSON value,
```

```
            "providerServiceArn": "string"
         },
         "resolutionType": "RULE_MATCHING",
         "ruleBasedProperties": {
            "attributeMatchingModel": "string",
            "matchPurpose": "string",
            "rules": [
               {
                  "matchingKeys": [ "string" ],
                  "ruleName": "string"
               }
            ]
         },
         "ruleConditionProperties": {
            "rules": [
               {
                  "condition": "string",
                  "ruleName": "string"
               }
            ]
         }
      },
      "roleArn": "string",
      "tags": {
         "string" : "string"
      },
      "workflowName": "string"
}
```

Wobei Folgendes gilt:

- `workflowName`(erforderlich) — Muss eindeutig sein und zwischen 1—255 Zeichen müssen dem Muster [a-z A-Z _0-9-] * entsprechen
- `inputSourceConfig`(erforderlich) — Liste mit 1—20 Eingangsquellenkonfigurationen
- `outputSourceConfig`(erforderlich) — Genau eine Ausgangsquellenkonfiguration
- `resolutionTechniques`(erforderlich) — Für regelbasierten Abgleich auf „RULE_MATCHING“ setzen
- `roleArn`(erforderlich) — IAM-Rollen-ARN für die Workflow-Ausführung
- `ruleConditionProperties`(erforderlich) — Liste der Regelbedingungen und der Name der passenden Regel.

Zu den optionalen Parametern gehören:

- `description`— Bis zu 255 Zeichen
- `incrementalRunConfig`— Inkrementelle Konfiguration des Lauftyps
- `tags`— Bis zu 200 Schlüssel-Wert-Paare

5. (Optional) Um die inkrementelle Verarbeitung anstelle der standardmäßigen Standardverarbeitung (Batch) zu verwenden, fügen Sie dem Anforderungstext den folgenden Parameter hinzu:

```
"incrementalRunConfig": {
   "incrementalRunType": "AUTOMATIC"
}
```

6. Senden Sie die Anforderung .
7. Bei Erfolg erhalten Sie eine Antwort mit dem Statuscode 200 und einem JSON-Text, der Folgendes enthält:

```
{
   "workflowArn": "string",
   "workflowName": "string",
   // Plus all configured workflow details
}
```

8. Wenn der Anruf nicht erfolgreich ist, erhalten Sie möglicherweise eine der folgenden Fehlermeldungen:

- 400 — ConflictException wenn der Workflow-Name bereits existiert
- 400 — ValidationException wenn die Eingabe die Überprüfung nicht besteht
- 402 — ExceedsLimitException wenn Kontolimits überschritten werden
- 403 — AccessDeniedException wenn Sie nicht über ausreichenden Zugriff verfügen
- 429 — ThrottlingException wenn die Anfrage gedrosselt wurde
- 500 — InternalServerException wenn ein interner Servicefehler vorliegt

Erstellung eines Matching-Workflows, der auf maschinellem Lernen basiert

Der auf maschinellem Lernen basierende Abgleich ist ein voreingestellter Prozess, bei dem versucht wird, Datensätze aus allen von Ihnen eingegebenen Daten abzugleichen. Der auf maschinellem Lernen basierende Matching-Workflow ermöglicht es Ihnen, Klartextdaten zu vergleichen, um mithilfe eines maschinellen Lernmodells eine Vielzahl von Übereinstimmungen zu finden.

> **Note**
>
> Das Modell für maschinelles Lernen unterstützt den Vergleich von Hash-Daten nicht.

Wenn Ihre Daten AWS Entity Resolution verarbeitet werden, weist es Folgendes zu:

- Eine Match-ID für jeden Datensatz.
- Wenn ein Datensatz mit einem oder mehreren anderen Datensätzen in Ihren Daten übereinstimmt:
  - Der Prozentsatz des Konfidenzniveaus auf Gruppenebene, der entspricht.
  - Der Prozentsatz des Konfidenzniveaus auf Rekordebene (nur inkrementeller Abgleich). ML-based

Sie können die Ergebnisse eines ML-based Matching-Workflows als Eingabe für den Datendienstanbieter-Abgleich verwenden oder umgekehrt, um Ihre spezifischen Ziele zu erreichen. Sie können beispielsweise einen ML-based Abgleich durchführen, um zuerst in Ihren eigenen Datensätzen nach Übereinstimmungen in Ihren Datenquellen zu suchen. Wenn für eine Teilmenge keine Übereinstimmung gefunden wurde, können Sie dann einen vom Provider Service erstellten Abgleich ausführen, um nach weiteren Übereinstimmungen zu suchen.

Voraussetzungen

Bevor Sie einen ML-based passenden Workflow erstellen, müssen Sie:

1. Erstellen Sie eine Schemazuordnung. Weitere Informationen finden Sie unter Eine Schemazuordnung erstellen.
2. Wenn Sie Connect Customer Customer Profiles als Ausgabeziel verwenden, stellen Sie sicher, dass Sie die entsprechenden Berechtigungen konfiguriert haben.

So erstellen Sie einen ML-based passenden Workflow:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Passende Workflows in der oberen rechten Ecke die Option Passenden Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Passende Workflow-Details angeben wie folgt vor:

   a. Geben Sie einen passenden Workflow-Namen und optional eine Beschreibung ein.

   b. Wählen Sie für die Dateneingabe eine AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

      Sie können bis zu 20 Dateneingaben hinzufügen.

   c. Die Option Daten normalisieren ist standardmäßig ausgewählt, sodass Dateneingaben vor dem Abgleich normalisiert werden. Wenn Sie Daten nicht normalisieren möchten, deaktivieren Sie die Option Daten normalisieren.

      Der auf maschinellem Lernen basierende Abgleich normalisiert Name nur, und. Phone Email

   d. Um die Zugriffsberechtigungen für den Dienst festzulegen, wählen Sie eine Option aus und ergreifen Sie die empfohlene Aktion.

Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname für die Servicerolle lautet `entityresolution-matching-workflow-<timestamp>` . • Sie müssen über Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese

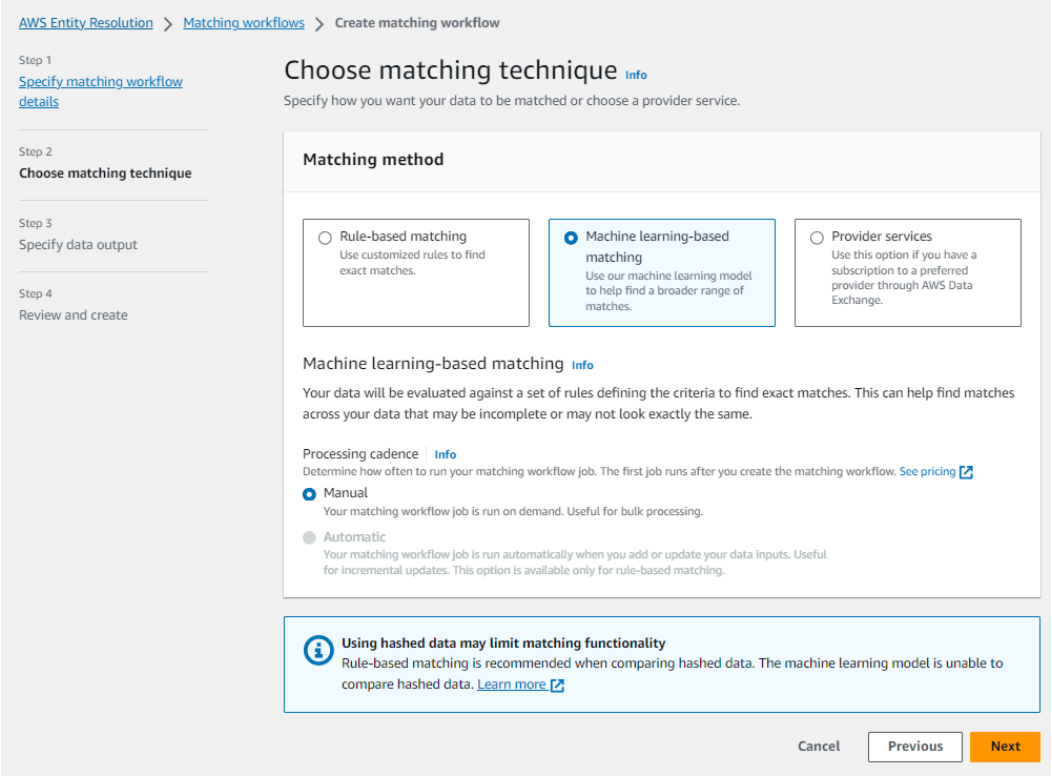
Option	Empfohlene Aktion
	Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn keine Servicerollen vorhanden sind, ist die Option „Eine vorhandene Servicerolle verwenden“ nicht verfügbar. 2. Zeigen Sie die Servicerolle an, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

e. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel-Wert-Paar ein.

f. Wählen Sie Weiter aus.

5. Für Schritt 2: Wählen Sie das passende Verfahren aus:

   a. Wählen Sie als Abgleichmethode die Option Auf maschinellem Lernen basierender Abgleich aus.



   b. Wählen Sie für den Verarbeitungsrhythmus eine der folgenden Optionen aus.

      - Wählen Sie Manuell, um einen Batch-Matching-Workflow auszuführen, der die gesamten Daten in Ihrem S3-Bucket verarbeitet.
      - Wählen Sie Automatisch, um einen Workflow für den inkrementellen Abgleich auszuführen, der nur die inkrementellen Daten in Ihrem S3-Bucket verarbeitet.

   c. Wählen Sie Weiter aus.

6. Für Schritt 3: Geben Sie die Datenausgabe und das Format an:

   a. Wählen Sie für Datenausgabeziel und -format den Amazon S3-Speicherort für die Datenausgabe aus und geben Sie an, ob das Datenformat Normalisierte Daten oder Originaldaten sein soll.

   b. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen möchten, geben Sie den AWS KMS Schlüssel-ARN ein.

   c. Sehen Sie sich die vom System generierte Ausgabe an.

d. Entscheiden Sie für die Datenausgabe, welche Felder Sie einbeziehen, ausblenden oder maskieren möchten, und ergreifen Sie dann die empfohlenen Maßnahmen auf der Grundlage Ihrer Ziele.

Ihr Ziel	Empfohlene Option
Felder einbeziehen	Behalten Sie den Ausgabestatus „Eingeschlossen“ bei.
Felder ausblenden (von der Ausgabe ausschließen)	Wählen Sie das Ausgabefeld aus und wählen Sie dann Ausblenden.
Felder maskieren	Wählen Sie das Ausgabefeld und dann Hash-Ausgabe.
Setzen Sie die vorherigen Einstellungen zurück	Klicken Sie auf Reset (Zurücksetzen).

e. Wählen Sie Weiter aus.

7. Für Schritt 4: Prüfen und erstellen Sie:

   a. Überprüfen Sie die Auswahl, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Create and run aus.

      Es wird eine Meldung angezeigt, die darauf hinweist, dass der entsprechende Workflow erstellt und der Job gestartet wurde.

8. Sehen Sie sich auf der Seite mit den Details des passenden Workflows auf der Registerkarte Metriken unter Letzte Job-Metriken Folgendes an:

   - Die Job-ID.
   - Der Status des passenden Workflow-Jobs: In Warteschlange, In Bearbeitung, Abgeschlossen, Fehlgeschlagen
   - Die Zeit, in der der Workflow-Job abgeschlossen wurde.
   - Die Anzahl der verarbeiteten Datensätze.
   - Die Anzahl der Datensätze, die nicht verarbeitet wurden.
   - Die generierten eindeutigen Match-IDs.

- Die Anzahl der Eingabedatensätze.

Sie können auch die Job-Metriken für übereinstimmende Workflow-Jobs, die zuvor ausgeführt wurden, im Auftragsverlauf anzeigen.

9. Nachdem der passende Workflow-Job abgeschlossen ist (Status ist abgeschlossen), können Sie zur Registerkarte Datenausgabe wechseln und dann Ihren Amazon S3-Standort auswählen, um die Ergebnisse anzuzeigen. Diese Informationen werden vom passenden Workflow-Job generiert und in der Ausgabe enthalten.

Ausgabefeld	Description
Match-ID	ID, die von jedem übereinstimmenden Datensatz generiert AWS Entity Resolution und auf ihn angewendet wird.
ConfidenceLevel	Matching-group-level Konfidenz, die angewendet wird, wenn ein übereinst immender Datensatz identifiziert wird.
RecordConfidenceLevel	Record-level Konfidenz, die auf jeden Datensatz angewendet wird, wenn ein übereinstimmender Datensatz identifiziert wird. Nur inkrementeller Abgleich durch maschinelles Lernen.
InputSourceARN	Amazon-Ressourcenname (ARN), der für einen AWS Glue Workflow generiert wurde.
HashingProtocol	Sicherer Hash-Algorithmus 256-Bit (SHA256). Gibt eine 32-Byte-Zeichenfolge für Hash-Ausgaben aus.

10. (Nur manueller Verarbeitungstyp) Wenn Sie einen auf maschinellem Lernen basierenden Matching-Workflow mit dem Verarbeitungstyp Manuell erstellt haben, können Sie den passenden Workflow jederzeit ausführen, indem Sie auf der Seite mit den passenden Workflow-Details die Option Workflow ausführen auswählen.

Erstellen eines auf dem Provider-Service basierenden Matching-Workflows

???Mithilfe des dienstbasierten Abgleichs von Anbietern können Sie Ihre bekannten Identifikatoren Ihrem bevorzugten Datendienstanbieter zuordnen.

AWS Entity Resolution unterstützt derzeit die folgenden Datenanbieterdienste:

- LiveRamp
- TransUnion
- Unified ID 2.0

Weitere Informationen zu den unterstützten Anbieterdiensten finden Sie unterVorbereiten von Eingabedaten von Drittanbietern.

Sie können ein öffentliches Abonnement für diese Anbieter nutzen AWS Data Exchange oder direkt mit dem Datenanbieter ein privates Angebot aushandeln. Weitere Informationen zum Erstellen eines neuen Abonnements oder zur Wiederverwendung eines bestehenden Abonnements für einen Anbieterdienst finden Sie unterSchritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange.

In den folgenden Abschnitten wird beschrieben, wie Sie einen anbieterbasierten Matching-Workflow erstellen.

Topics

- Erstellen Sie einen passenden Workflow mit LiveRamp
- Erstellen Sie einen passenden Workflow mit TransUnion
- Einen passenden Workflow mit UID 2.0 erstellen

Erstellen Sie einen passenden Workflow mit LiveRamp

Der LiveRamp Dienst stellt eine Kennung zur Verfügung, die als RampID bezeichnet wird. Die RampID ist eine der am häufigsten verwendeten IDs auf Demand-Side-Plattformen, um eine Zielgruppe für eine Werbekampagne zu gewinnen. Mithilfe eines passenden Workflows mit können Sie LiveRamp Hash-E-Mail-Adressen in RAMPIDs auflösen.

> **Note**
>
> AWS Entity Resolution unterstützt die RAMPID-Zuweisung PII-based .

Voraussetzungen

Bevor Sie einen passenden Workflow mit erstellen LiveRamp, müssen Sie:

1. Erstellen Sie eine Schemazuordnung. Weitere Informationen finden Sie unter Eine Schemazuordnung erstellen.
2. Haben Sie ein Abonnement für den LiveRamp Dienst
3. Haben Sie die entsprechenden Berechtigungen für den Amazon S3-Daten-Staging-Bucket konfiguriert, in den die entsprechende Workflow-Ausgabe vorübergehend geschrieben werden soll

Bevor Sie einen ID-Mapping-Workflow mit erstellen LiveRamp, fügen Sie dem S3-Daten-Staging-Bucket die folgenden Berechtigungen hinzu.

JSON

```
{
    "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>/*"
            ]
        }
    ]
}
```

Ersetzen Sie jeden *<user input placeholder>* durch Ihre Informationen.

staging-bucket	Amazon S3-Bucket, in dem Ihre Daten vorübergehend gespeichert werden, während ein auf einem Provider-Service basierender Workflow ausgeführt wird.

So erstellen Sie einen passenden Workflow mit LiveRamp:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter **Workflows** die Option **Matching** aus.
3. Wählen Sie auf der **Seite** Passende Workflows in der oberen rechten Ecke die Option Passenden Workflow erstellen aus.
4. Gehen Sie für **Schritt 1: Passende Workflow-Details** angeben wie folgt vor:

    a. Geben Sie einen **passenden Workflow-Namen** und optional eine **Beschreibung** ein.

b. Wählen Sie für die Dateneingabe eine AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

   Sie können bis zu 20 Dateneingaben hinzufügen.

c. Die Option Daten normalisieren ist standardmäßig ausgewählt, sodass Dateneingaben vor dem Abgleich normalisiert werden.

   > **Note**
   >
   > Die Normalisierung wird unter Schema-Mapping erstellen nur für die folgenden Szenarien unterstützt:
   >
   > - Wenn die folgenden Namensuntertypen gruppiert sind: Vorname, zweiter Vorname, Nachname.
   > - Wenn die folgenden Adressuntertypen gruppiert sind: Straße 1, Straße 2: Straße, Adresse 3, Name der Stadt, Bundesland, Land, Postleitzahl.
   > - Wenn die folgenden Telefonuntertypen gruppiert sind: Telefonnummer, Telefonvorwahl.

   Wenn Sie das reine E-Mail-Auflösungsverfahren verwenden, deaktivieren Sie die Option Daten normalisieren, da nur Hash-E-Mails für Eingabedaten verwendet werden.

d. Um die Zugriffsberechtigungen für den Dienst festzulegen, wählen Sie eine Option und ergreifen Sie die empfohlene Aktion.

Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname für die Servicerolle lautet `entityresolution-matching-workflow-<timestamp>` . • Sie müssen über Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.

Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn keine Servicerollen vorhanden sind, ist die Option „Eine vorhandene Servicerolle verwenden“ nicht verfügbar. 2. Zeigen Sie die Servicerolle an, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

e. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel-Wert-Paar ein.

f. Wählen Sie Weiter aus.

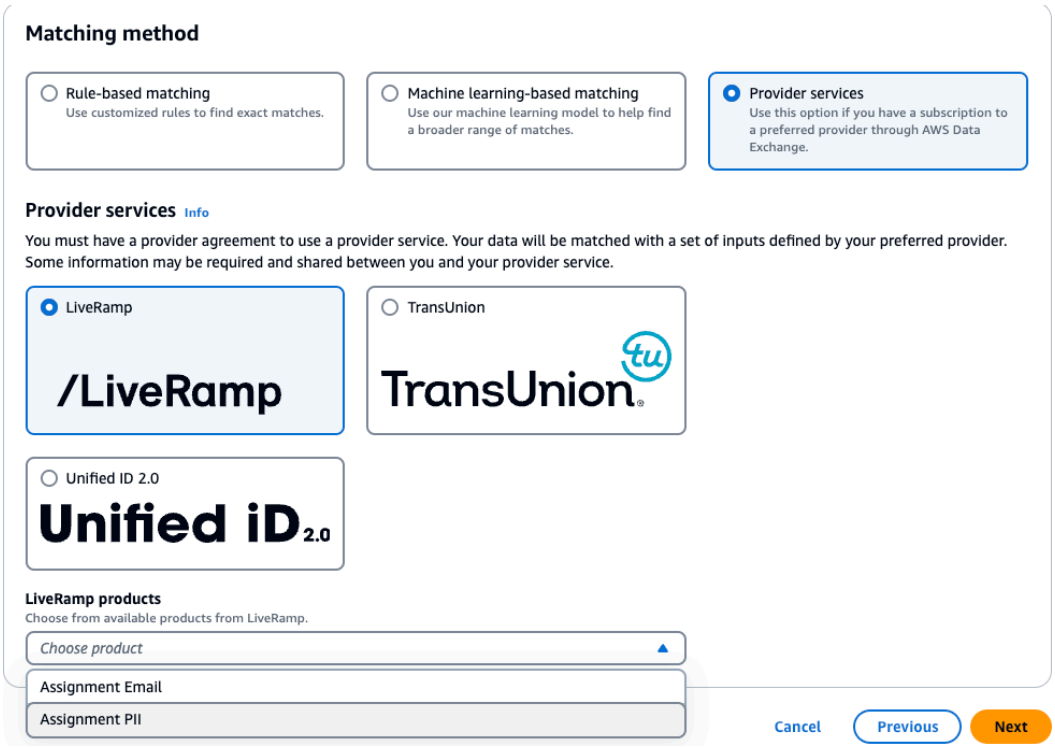
5. Für Schritt 2: Wählen Sie das passende Verfahren aus:

a. Wählen Sie als Vergleichsmethode die Option Provider-Dienste aus.

b. Wählen Sie für Anbieterdienste die Option LiveRamp.

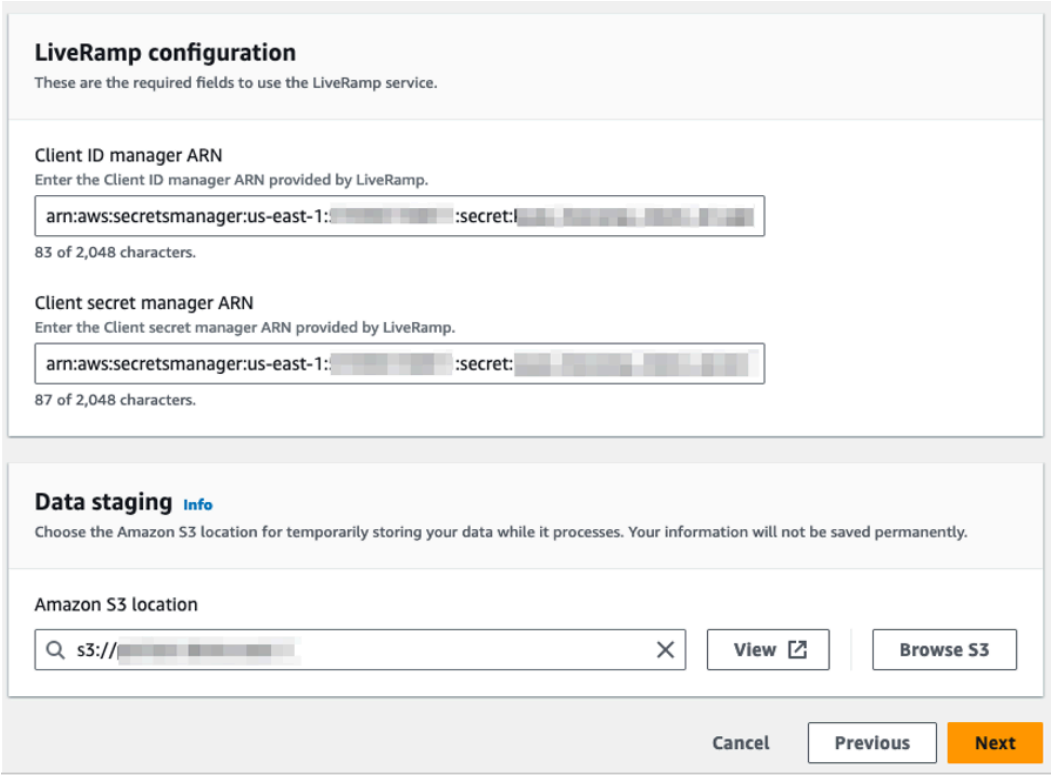
> **Note**
>
> Stellen Sie sicher, dass das Format und die Normalisierung Ihrer Dateneingabedatei den Richtlinien des Anbieterdienstes entsprechen.
> Weitere Informationen zu den Richtlinien zur Formatierung von Eingabedateien für den Matching-Workflow finden Sie in der Dokumentation unter Identitätsauflösung über ADX durchführen. LiveRamp

c. Wählen Sie für LiveRamp Produkte ein Produkt aus der Dropdownliste aus.



> **Note**
>
> Wenn Sie Assignment PII wählen, müssen Sie bei der Entitätsauflösung mindestens eine Spalte ohne Identifikationsnummer angeben. Zum Beispiel GESCHLECHT.

d. Geben Sie für die LiveRamp Konfiguration einen Client-ID-Manager-ARN und einen Client Secret Manager-ARN ein.



e. Wählen Sie für das Daten-Staging den Amazon S3-Speicherort für die temporäre Speicherung Ihrer Daten während der Verarbeitung.

   Sie benötigen die Genehmigung für den Amazon S3-Speicherort für das Daten-Staging. Weitere Informationen finden Sie unter Erstellen einer Workflow-Jobrolle für AWS Entity Resolution.

f. Wählen Sie Weiter aus.

6. Für Schritt 3: Geben Sie die Datenausgabe an:

   a. Wählen Sie für Datenausgabeziel und -format den Amazon S3-Speicherort für die Datenausgabe aus und geben Sie an, ob das Datenformat Normalisierte Daten oder Originaldaten sein soll.

   b. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen möchten, geben Sie den AWS KMS Schlüssel-ARN ein.

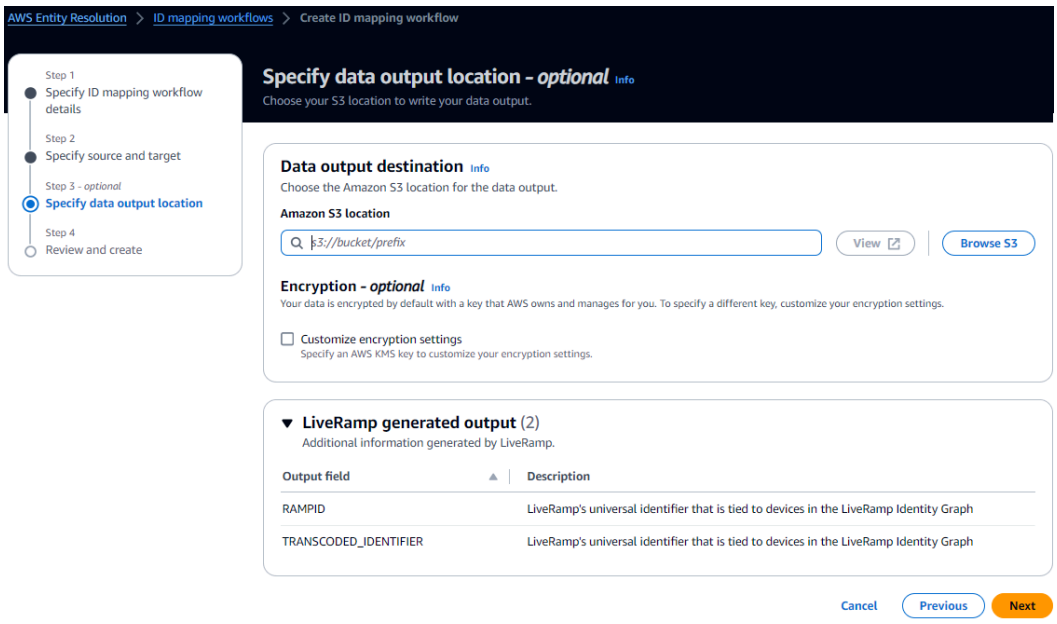
   c. Sehen Sie sich die LiveRamp generierte Ausgabe an.

      Dies sind die zusätzlichen Informationen, die von generiert wurden LiveRamp.

   d. Entscheiden Sie für die Datenausgabe, welche Felder Sie einbeziehen, ausblenden oder maskieren möchten, und ergreifen Sie dann die empfohlenen Maßnahmen, die auf Ihren Zielen basieren.

> **Note**
>
> Wenn Sie ausgewählt haben LiveRamp, wird aufgrund von LiveRamp Datenschutzfiltern, die personenbezogene Daten (PII) entfernen, für einige Felder der Ausgabestatus Nicht verfügbar angezeigt.

Dein Ziel	Empfohlene Option
Felder einbeziehen	Behalten Sie den Ausgabestatus „Eingeschlossen“ bei.
Felder ausblenden (von der Ausgabe ausschließen)	Wählen Sie das Ausgabefeld aus und wählen Sie dann Ausblenden.
Felder maskieren	Wählen Sie das Ausgabefeld und dann Hash-Ausgabe.
Setzen Sie die vorherigen Einstellungen zurück	Klicken Sie auf Reset (Zurücksetzen).



e. Wählen Sie Weiter aus.

7. Für Schritt 4: Prüfen und erstellen Sie:

   a. Überprüfen Sie die Auswahl, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Create and run aus.

      Es wird eine Meldung angezeigt, die darauf hinweist, dass der entsprechende Workflow erstellt und der Job gestartet wurde.

8. Sehen Sie sich auf der Seite mit den Details des passenden Workflows auf der Registerkarte Metriken unter Letzte Job-Metriken Folgendes an:

   - Die Job-ID.
   - Der Status des passenden Workflow-Jobs: In Warteschlange, In Bearbeitung, Abgeschlossen, Fehlgeschlagen
   - Die Zeit, in der der Workflow-Job abgeschlossen wurde.
   - Die Anzahl der verarbeiteten Datensätze.
   - Die Anzahl der Datensätze, die nicht verarbeitet wurden.
   - Die generierten eindeutigen Match-IDs.
   - Die Anzahl der Eingabedatensätze.

   Sie können auch die Job-Metriken für übereinstimmende Workflow-Jobs, die zuvor ausgeführt wurden, im Auftragsverlauf anzeigen.

9. Nachdem der passende Workflow-Job abgeschlossen ist (Status ist abgeschlossen), können Sie zur Registerkarte Datenausgabe wechseln und dann Ihren Amazon S3-Standort auswählen, um die Ergebnisse anzuzeigen.

Erstellen Sie einen passenden Workflow mit TransUnion

Wenn Sie den TransUnion Service abonniert haben, können Sie das Kundenverständnis verbessern, indem Sie kundenbezogene Datensätze, die auf unterschiedlichen Kanälen gespeichert sind, mit E-Schlüsseln für TransUnion Person und Haushalt sowie über 200 Datenattributen verknüpfen, abgleichen und erweitern.

Der TransUnion Dienst stellt Identifikatoren zur Verfügung, die als Personen- und Haushalts-ID bezeichnet TransUnion werden. TransUnion ermöglicht die ID-Zuweisung (auch als Codierung bezeichnet) bekannter Identifikatoren wie Name, Adresse, Telefonnummer und E-Mail-Adresse.

Voraussetzungen

Bevor Sie einen passenden Workflow mit erstellen LiveRamp, müssen Sie:

1. Erstellen Sie eine Schemazuordnung. Weitere Informationen finden Sie unter Eine Schemazuordnung erstellen.
2. Haben Sie ein Abonnement für den TransUnion Dienst
3. Haben Sie die entsprechenden Berechtigungen für den Amazon S3-Daten-Staging-Bucket konfiguriert, in den die entsprechende Workflow-Ausgabe vorübergehend geschrieben werden soll

Bevor Sie einen passenden Workflow mit erstellen TransUnion, fügen Sie dem S3-Daten-Staging-Bucket die folgenden Berechtigungen hinzu.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::381491956555: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::381491956555:root"
            },
            "Action": [
```

```
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket>",
                "arn:aws:s3:::<staging-bucket>/*"
            ]
        }
    ]
}
```

Ersetzen Sie jeden *<user input placeholder>* durch Ihre Informationen.

staging-bucket	Amazon S3-Bucket, in dem Ihre Daten vorübergehend gespeichert werden, während ein auf einem Provider-Service basierender Workflow ausgeführt wird.

So erstellen Sie einen passenden Workflow mit TransUnion:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Passende Workflows in der oberen rechten Ecke die Option Passenden Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Passende Workflow-Details angeben wie folgt vor:

    a. Geben Sie einen passenden Workflow-Namen und optional eine Beschreibung ein.

    b. Wählen Sie für die Dateneingabe eine AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

    Sie können bis zu 20 Dateneingaben hinzufügen.

c. Die Option Daten normalisieren ist standardmäßig ausgewählt, sodass Dateneingaben vor dem Abgleich normalisiert werden. Wenn Sie Daten nicht normalisieren möchten, deaktivieren Sie die Option Daten normalisieren.

> **Note**
>
> Die Normalisierung wird unter Schema-Mapping erstellen nur für die folgenden Szenarien unterstützt:
>
> - Wenn die folgenden Namensuntertypen gruppiert sind: Vorname, zweiter Vorname, Nachname.
> - Wenn die folgenden Adressuntertypen gruppiert sind: Straße 1, Straße 2: Straße, Adresse 3, Name der Stadt, Bundesland, Land, Postleitzahl.
> - Wenn die folgenden Telefonuntertypen gruppiert sind: Telefonnummer, Telefonvorwahl.

d. Um die Zugriffsberechtigungen für den Dienst festzulegen, wählen Sie eine Option aus und ergreifen Sie die empfohlene Aktion.

Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname für die Servicerolle lautet `entityresolution-matching-workflow-<timestamp>` . • Sie müssen über Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.

Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn keine Servicerollen vorhanden sind, ist die Option „Eine vorhandene Servicerolle verwenden“ nicht verfügbar. 2. Zeigen Sie die Servicerolle an, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

e. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel-Wert-Paar ein.

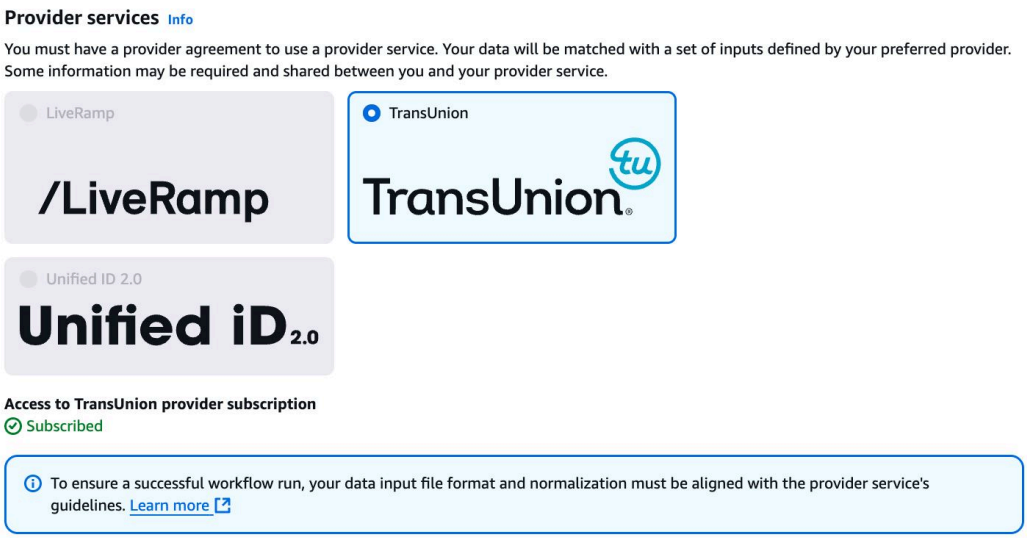
f. Wählen Sie Weiter aus.

5. Für Schritt 2: Wählen Sie das passende Verfahren aus:

a. Wählen Sie als Vergleichsmethode die Option Provider-Dienste aus.

b. Wählen Sie für Provider-Dienste die Option TransUnion.

> **Note**
>
> Stellen Sie sicher, dass das Format und die Normalisierung Ihrer Dateneingabedatei den Richtlinien des Anbieterdienstes entsprechen.



c. Wählen Sie für das Daten-Staging den Amazon S3-Standort für die temporäre Speicherung Ihrer Daten während der Verarbeitung.

   Sie benötigen die Genehmigung für den Amazon S3-Speicherort für das Daten-Staging. Weitere Informationen finden Sie unter the section called “Eine Workflow-Jobrolle erstellen”.

6. Wählen Sie Weiter aus.
7. Für Schritt 3: Datenausgabe angeben:

   a. Wählen Sie für Datenausgabeziel und -format den Amazon S3-Speicherort für die Datenausgabe aus und geben Sie an, ob das Datenformat Normalisierte Daten oder Originaldaten sein soll.

   b. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen möchten, geben Sie den AWS KMS Schlüssel-ARN ein.

   c. Sehen Sie sich die TransUnion generierte Ausgabe an.

      Dies sind die zusätzlichen Informationen, die von generiert wurden TransUnion.

d. Entscheiden Sie für die Datenausgabe, welche Felder Sie einbeziehen, ausblenden oder maskieren möchten, und ergreifen Sie dann die empfohlenen Maßnahmen, die auf Ihren Zielen basieren.

Ihr Ziel	Empfohlene Option
Felder einbeziehen	Behalten Sie den Ausgabestatus „Eingeschlossen“ bei.
Felder ausblenden (von der Ausgabe ausschließen)	Wählen Sie das Ausgabefeld aus und wählen Sie dann Ausblenden.
Felder maskieren	Wählen Sie das Ausgabefeld und dann Hash-Ausgabe.
Setzen Sie die vorherigen Einstellungen zurück	Klicken Sie auf Reset (Zurücksetzen).

e. Sehen Sie sich für die vom System generierte Ausgabe alle Felder an, die enthalten sind.

f. Wählen Sie Weiter aus.

8. Für Schritt 4: Prüfen und erstellen Sie:

   a. Überprüfen Sie die Auswahl, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Create and run aus.

      Es wird eine Meldung angezeigt, die darauf hinweist, dass der entsprechende Workflow erstellt und der Job gestartet wurde.

9. Sehen Sie sich auf der Seite mit den Details des passenden Workflows auf der Registerkarte Metriken unter Letzte Job-Metriken Folgendes an:

   - Die Job-ID.
   - Der Status des passenden Workflow-Jobs: In Warteschlange, In Bearbeitung, Abgeschlossen, Fehlgeschlagen
   - Die Zeit, in der der Workflow-Job abgeschlossen wurde.
   - Die Anzahl der verarbeiteten Datensätze.
   - Die Anzahl der Datensätze, die nicht verarbeitet wurden.

- Die generierten eindeutigen Match-IDs.
- Die Anzahl der Eingabedatensätze.

Sie können auch die Job-Metriken für übereinstimmende Workflow-Jobs anzeigen, die zuvor im Jobverlauf ausgeführt wurden.

10. Nachdem der passende Workflow-Job abgeschlossen ist (Status ist abgeschlossen), können Sie zur Registerkarte Datenausgabe wechseln und dann Ihren Amazon S3-Standort auswählen, um die Ergebnisse anzuzeigen.

Einen passenden Workflow mit UID 2.0 erstellen

Wenn Sie ein Abonnement für den Unified ID 2.0-Dienst haben, können Sie Werbekampagnen mit deterministischer Identität aktivieren und sich auf die Interoperabilität mit vielen UID2-enabled Teilnehmern im gesamten Werbeökosystem verlassen. Weitere Informationen finden Sie unter Unified ID 2.0-Überblick.

Der Unified ID 2.0-Dienst stellt die unformatierte UID 2 bereit, die für die Erstellung von Werbekampagnen auf der The Trade Desk-Plattform verwendet wird. UID 2.0 wird mithilfe eines Open-Source-Frameworks generiert.

In einem Workflow können Sie entweder **`Email Address`** oder **`Phone number`** für die Raw-UID2-Generierung verwenden, aber nicht beide. Wenn beide in der Schemazuordnung vorhanden sind, wählt der Workflow das Feld aus **`Email Address`** und das **`Phone number`** wird ein Pass-Through-Feld sein. Um beide zu unterstützen, erstellen Sie eine neue Schemazuordnung, bei der zwar zugeordnet, aber **`Email Address`** nicht zugeordnet **`Phone number`** wird. Erstellen Sie dann einen zweiten Workflow mit dieser neuen Schemazuordnung.

> **Note**
>
> Raw-UID2 werden durch Hinzufügen von Salzen aus Salzeimern erzeugt, die etwa einmal im Jahr rotiert werden, sodass auch die Roh-UID2 mit rotiert wird. Daher wird empfohlen, die Roh-UID2 täglich zu aktualisieren. Weitere Informationen finden Sie unter https://unifiedid.com/docs/getting-started/gs-faqs #how -often-shouldd-uid2s-be-refreshed-for-incremental-updates.

Voraussetzungen

Bevor Sie einen passenden Workflow mit UID 2.0 erstellen, müssen Sie:

1. Erstellen Sie eine Schemazuordnung. Weitere Informationen finden Sie unter Eine Schemazuordnung erstellen.
2. Haben Sie ein Abonnement für den UID 2.0-Dienst

Um einen passenden Workflow mit UID 2.0 zu erstellen:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Passende Workflows in der oberen rechten Ecke die Option Passenden Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Passende Workflow-Details angeben wie folgt vor:

   a. Geben Sie einen passenden Workflow-Namen und optional eine Beschreibung ein.

   b. Wählen Sie für die Dateneingabe eine AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

      Sie können bis zu 20 Dateneingaben hinzufügen.

   c. Lassen Sie die Option Daten normalisieren aktiviert, sodass Dateneingaben (**`Email Address`**oder**`Phone number`**) vor dem Abgleich normalisiert werden.

      Weitere Informationen zur **`Email Address`** Normalisierung finden Sie in der UID 2.0-Dokumentation unter Normalisierung von E-Mail-Adressen.

      Weitere Informationen zur Normalisierung finden Sie unter **`Phone number`** Normalisierung von Telefonnummern in der UID 2.0-Dokumentation.

   d. Um die Zugriffsberechtigungen für den Dienst festzulegen, wählen Sie eine Option aus und ergreifen Sie die empfohlene Aktion.

Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle.

Option	Empfohlene Aktion
	• Der Standardname für die Servicerolle lautet `entityresolution-matching-workflow-<timestamp>` . • Sie müssen über Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.

Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn keine Servicerollen vorhanden sind, ist die Option „Eine vorhandene Servicerolle verwenden“ nicht verfügbar. 2. Zeigen Sie die Servicerolle an, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

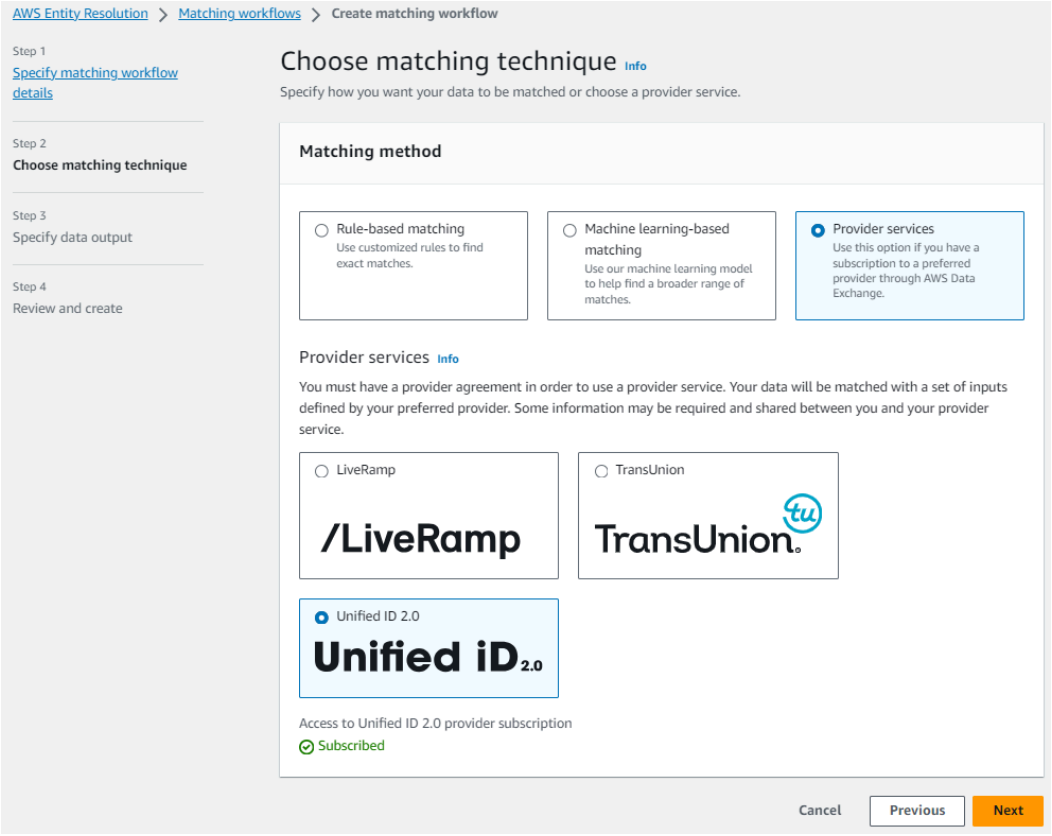
e. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel-Wert-Paar ein.

f. Wählen Sie Weiter aus.

5. Für Schritt 2: Wählen Sie das passende Verfahren aus:

a. Wählen Sie als Vergleichsmethode die Option Provider-Dienste aus.

b. Wählen Sie für Provider-Dienste die Option Unified ID 2.0 aus.



c. Wählen Sie Weiter aus.

6. Für Schritt 3: Datenausgabe angeben:

a. Wählen Sie für Datenausgabeziel und -format den Amazon S3-Speicherort für die Datenausgabe aus und geben Sie an, ob das Datenformat Normalisierte Daten oder Originaldaten sein soll.

b. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen möchten, geben Sie den AWS KMS Schlüssel-ARN ein.

c. Sehen Sie sich die von Unified ID 2.0 generierte Ausgabe an.

Dies ist eine Liste aller zusätzlichen Informationen, die von UID 2.0 generiert wurden

d. Entscheiden Sie für die Datenausgabe, welche Felder Sie einbeziehen, ausblenden oder maskieren möchten, und ergreifen Sie dann die empfohlenen Maßnahmen, die auf Ihren Zielen basieren.

Ihr Ziel	Empfohlene Option
Felder einbeziehen	Behalten Sie den Ausgabestatus „Eingeschlossen“ bei.
Felder ausblenden (von der Ausgabe ausschließen)	Wählen Sie das Ausgabefeld aus und wählen Sie dann Ausblenden.
Felder maskieren	Wählen Sie das Ausgabefeld und dann Hash-Ausgabe.
Setzen Sie die vorherigen Einstellungen zurück	Klicken Sie auf Reset (Zurücksetzen).

e. Sehen Sie sich für die vom System generierte Ausgabe alle Felder an, die enthalten sind.

f. Wählen Sie Weiter aus.

7. Für Schritt 4: Prüfen und erstellen Sie:

   a. Überprüfen Sie die Auswahl, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Create and run aus.

      Es wird eine Meldung angezeigt, die darauf hinweist, dass der entsprechende Workflow erstellt und der Job gestartet wurde.

8. Sehen Sie sich auf der Seite mit den Details des passenden Workflows auf der Registerkarte Metriken unter Letzte Job-Metriken Folgendes an:

   - Die Job-ID.
   - Der Status des passenden Workflow-Jobs: In Warteschlange, In Bearbeitung, Abgeschlossen, Fehlgeschlagen
   - Die Zeit, in der der Workflow-Job abgeschlossen wurde.
   - Die Anzahl der verarbeiteten Datensätze.
   - Die Anzahl der Datensätze, die nicht verarbeitet wurden.
   - Die generierten eindeutigen Match-IDs.
   - Die Anzahl der Eingabedatensätze.

Sie können auch die Job-Metriken für übereinstimmende Workflow-Jobs, die zuvor ausgeführt wurden, im Auftragsverlauf anzeigen.

9. Nachdem der passende Workflow-Job abgeschlossen ist (Status ist abgeschlossen), können Sie zur Registerkarte Datenausgabe wechseln und dann Ihren Amazon S3-Standort auswählen, um die Ergebnisse anzuzeigen.

Bearbeitung eines passenden Workflows

Durch die Bearbeitung des Matching-Workflows können Sie Ihre Prozesse zur Auflösung von Entitäten auf dem neuesten Stand halten und auf die sich im Laufe der Zeit ändernden Anforderungen Ihres Unternehmens reagieren. Möglicherweise möchten Sie die Abgleichskriterien, Techniken oder Datenausgaben anpassen, um die Genauigkeit und Effizienz des Prozesses zur Auflösung von Entitäten zu verbessern. Wenn Sie Probleme oder Fehler in den Ergebnissen des aktuellen Workflows feststellen, kann Ihnen die Bearbeitung helfen, diese Probleme zu diagnostizieren und zu lösen.

So bearbeiten Sie einen passenden Workflow:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie den passenden Workflow aus.
4. Wählen Sie auf der Seite mit den passenden Workflow-Details in der oberen rechten Ecke die Option Workflow bearbeiten aus.
5. Nehmen Sie auf der Seite Passende Workflow-Details angeben alle erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
6. Nehmen Sie auf der Seite „Vergleichstechnik auswählen“ die erforderlichen Änderungen vor und klicken Sie dann auf Weiter.

> **Important**
>
> Sie können den Verarbeitungsrhythmus von „Manuell“ auf „Automatisch“ ändern, aber nachdem Sie ihn auf „Automatisch“ geändert haben, können Sie ihn nicht mehr auf „Manuell“ ändern.

Wenn der Verarbeitungsrhythmus bereits auf Automatisch eingestellt ist, können Sie ihn nicht auf Manuell ändern.

7. Nehmen Sie auf der Seite „Datenausgabe angeben“ die erforderlichen Änderungen vor und wählen Sie dann Weiter.
8. Nehmen Sie auf der Seite Überprüfen und speichern alle erforderlichen Änderungen vor und wählen Sie dann Speichern aus.

Einen passenden Workflow löschen

Wenn ein passender Workflow nicht mehr verwendet wird oder veraltet ist, kann das Löschen dazu beitragen, dass dein Workspace organisiert und übersichtlich bleibt. Wenn du einen neuen, verbesserten Workflow entwickelt hast, der einen älteren ersetzt, kannst du durch das Löschen des alten Workflows sicherstellen, dass du nur die aktuellsten Prozesse verwendest.

So löschst du einen passenden Workflow:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie den passenden Workflow aus.
4. Wählen Sie auf der Seite mit den passenden Workflow-Details in der oberen rechten Ecke Löschen aus.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Ändern oder Generieren einer Match-ID für einen regelbasierten Matching-Workflow

Eine Match-ID ist die Kennung, die von jedem abgeglichenen Datensatz generiert AWS Entity Resolution und auf ihn angewendet wird, nachdem ein passender Workflow ausgeführt wurde. Dies ist Teil der passenden Workflow-Metadaten, die in der Ausgabe enthalten sind.

Wenn Sie Datensätze für einen bestehenden Kunden aktualisieren oder Ihrem Datensatz einen neuen Kunden hinzufügen müssen, können Sie die AWS Entity Resolution Konsole oder die `GenerateMatchId` API verwenden. Das Ändern einer vorhandenen Match-ID trägt dazu bei, die

Konsistenz bei der Aktualisierung von Kundeninformationen aufrechtzuerhalten. Das Generieren einer neuen Match-ID ist erforderlich, wenn Sie Ihrem System zuvor unbekannte Kunden hinzufügen.

> **Note**
>
> Es fallen zusätzliche Gebühren an, unabhängig davon, ob Sie die Konsole oder die API verwenden. Die gewählte Verarbeitungsart wirkt sich sowohl auf die Genauigkeit als auch auf die Reaktionszeit des Vorgangs aus.

> **Real-time übereinstimmende Anforderungen**
>
> Um die `GenerateMatchId` API in einem erweiterten regelbasierten Matching-Workflow aufzurufen, setzen `enableRealTimeMatching` Sie den Wert auf. `true` Für einfache Matching-Workflows ist der Abgleich in Echtzeit immer verfügbar, und Sie müssen dieses Kennzeichen nicht setzen.
> Sie können den Echtzeitabgleich nicht für Workflows aktivieren, die eines der folgenden Elemente verwenden:
>
> - Fuzzy-Attribute:`Cosine`, oder `Soundex` `Levenshtein`
> - `EmptyValues=Ignore`
>
> Wenn auf gesetzt `enableRealTimeMatching` ist`true`, kann der Workflow nicht zusammen mit der StartMatchingJob API verwendet werden, um Workflow-Jobs auszuführen.

> **Important**
>
> Wenn Sie die AWS Entity Resolution Berechtigungen für Ihren S3-Bucket entziehen, während ein Job in Bearbeitung ist, AWS Entity Resolution verarbeitet und berechnet die Ausgabe der Ergebnisse an S3 trotzdem, kann die Ergebnisse jedoch nicht an Ihren Bucket liefern. Um dieses Problem zu vermeiden, stellen Sie sicher, dass Ihr AWS Entity Resolution Unternehmen über die richtigen Berechtigungen zum Schreiben in Ihren S3-Bucket verfügt, bevor Sie einen Job starten. Wenn Berechtigungen während der Verarbeitung entzogen werden, wird AWS Entity Resolution versucht, die Ergebnisse bis zu 30 Tage nach

Abschluss des Auftrags erneut zu liefern, sobald Sie die richtigen Bucket-Berechtigungen wiederhergestellt haben.

Das folgende Verfahren führt Sie Schritt für Schritt durch das Suchen oder Generieren einer Match-ID, das Auswählen eines Verarbeitungstyps und das Anzeigen der Ergebnisse.

Console

So ändern oder generieren Sie eine Match-ID mithilfe der Konsole

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie den regelbasierten Matching-Workflow aus, der verarbeitet wurde (Auftragsstatus ist Abgeschlossen).
4. Wählen Sie auf der Seite mit den passenden Workflow-Details die Registerkarte „IDs abgleichen“.
5. Wählen Sie Match-ID ändern oder generieren aus.

   > **Note**
   >
   > Die Option Match-ID ändern oder generieren ist nur für passende Workflows verfügbar, die den automatischen Verarbeitungsrhythmus verwenden. Wenn Sie den manuellen Verarbeitungsrhythmus ausgewählt haben, wird diese Option als inaktiv angezeigt. Um diese Option zu verwenden, bearbeiten Sie Ihren Arbeitsablauf so, dass der automatische Verarbeitungsrhythmus verwendet wird. Weitere Informationen zum Bearbeiten von Workflows finden Sie unterBearbeitung eines passenden Workflows.

6. Wählen Sie die AWS Glue Tabelle aus der Dropdownliste aus.

   Wenn der Workflow nur eine AWS Glue Tabelle enthält, ist diese standardmäßig ausgewählt.

7. Wählen Sie den Verarbeitungstyp.

   - Konsistent — Sie können eine vorhandene Match-ID nachschlagen oder sofort eine neue Match-ID generieren und speichern. Diese Option hat die höchste Genauigkeit und die langsamere Reaktionszeit.

- Hintergrund (wie `EVENTUAL` in der API dargestellt) — Sie können eine vorhandene Match-ID nachschlagen oder sofort eine neue Match-ID generieren. Der aktualisierte Datensatz wird im Hintergrund gespeichert. Diese Option reagiert zunächst schnell, und die vollständigen Ergebnisse sind später in S3 verfügbar.
- Schnelle ID-Generierung (wie `EVENTUAL_NO_LOOKUP` in der API dargestellt) — Sie können eine neue Match-ID erstellen, ohne nach einer vorhandenen suchen zu müssen. Der aktualisierte Datensatz wird im Hintergrund gespeichert. Diese Option reagiert am schnellsten. Sie wird nur für eindeutige Datensätze empfohlen.

8. Für Datensatzattribute

   a. Geben Sie den Wert für die eindeutige ID ein.

   b. Geben Sie für jeden Abgleichsschlüssel einen Wert ein, der anhand der in Ihrem Workflow konfigurierten Regeln mit vorhandenen Datensätzen übereinstimmt.

9. Wählen Sie „Match-ID suchen und Datensatz speichern“.

   Es wird eine Erfolgsmeldung angezeigt, die besagt, dass entweder die Match-ID gefunden wurde oder eine neue Match-ID generiert und der Datensatz gespeichert wurde.

10. Sehen Sie sich in der Erfolgsmeldung die entsprechende Match-ID und die zugehörige Regel an, die im passenden Workflow gespeichert wurde.

11. (Optional) Um die Match-ID zu kopieren, wählen Sie Kopieren.

API

Um eine Match-ID mithilfe der API zu ändern oder zu generieren

> **Note**
>
> Um diese API erfolgreich aufrufen zu können, müssen Sie zunächst einen regelbasierten Matching-Workflow mithilfe der StartMatchingJob API erfolgreich ausgeführt haben. Eine vollständige Liste der unterstützten Programmiersprachen finden Sie im Abschnitt Siehe auch von. GenerateMatchId

1. Öffnen Sie ein Terminal oder eine Eingabeaufforderung, um die API-Anfrage zu stellen.
2. Erstellen Sie eine POST-Anfrage an den folgenden Endpunkt:

```
/matchingworkflows/workflowName/generateMatches
```

3. Stellen Sie im Anforderungsheader das Content-type auf ein application/json.
4. Geben Sie in der Anforderungs-URI Ihre an`workflowName`.

   Das `workflowName` muss:

   - Zwischen 1 und 255 Zeichen lang sein
   - Entspricht dem Muster [a-z A-Z _0-9-] *
5. Geben Sie für den Anforderungstext den folgenden JSON-Code an:

```
{
   "processingType": "string",
   "records": [
      {
         "inputSourceARN": "string",
         "recordAttributeMap": {
            "string" : "string"
         },
         "uniqueId": "string"
      }
   ]
}
```

   Wobei Folgendes gilt:

   - `processingType`(optional) — Die Standardeinstellung ist. `CONSISTENT` Wählen Sie einen der folgenden Werte:
     - `CONSISTENT`- Für höchste Genauigkeit bei langsamerer Reaktionszeit
     - `EVENTUAL`- Für eine schnellere Erstreaktion mit Hintergrundverarbeitung
     - `EVENTUAL_NO_LOOKUP`- Für die schnellste Reaktion, wenn bekannt ist, dass Datensätze eindeutig sind
   - `records`(erforderlich) — Array, das genau ein Datensatzobjekt enthält
6. Senden Sie die Anforderung .

   Bei Erfolg erhalten Sie eine Antwort mit dem Statuscode 200 und einem JSON-Text, der Folgendes enthält:

```
{
   "failedRecords": [
      {
         "errorMessage": "string",
         "inputSourceARN": "string",
         "uniqueId": "string"
      }
   ],
   "matchGroups": [
      {
         "matchId": "string",
         "matchRule": "string",
         "records": [
            {
               "inputSourceARN": "string",
               "recordId": "string"
            }
         ]
      }
   ]
}
```

Wenn der Anruf nicht erfolgreich ist, erhalten Sie möglicherweise eine der folgenden Fehlermeldungen:

- 403 — AccessDeniedException wenn Sie nicht über ausreichenden Zugriff verfügen
- 404 — ResourceNotFoundException wenn die Ressource nicht gefunden werden kann
- 429 — ThrottlingException wenn die Anfrage gedrosselt wurde
- 400 — ValidationException wenn die Eingabe die Überprüfung nicht besteht
- 500 — InternalServerException wenn ein interner Servicefehler vorliegt

Suche nach einer Match-ID für einen regelbasierten Matching-Workflow

Nachdem Sie einen regelbasierten Abgleichsworkflow abgeschlossen haben, können Sie die Match-ID und die zugehörige Regel für jeden verarbeiteten Datensatz abrufen. Anhand dieser Informationen können Sie nachvollziehen, wie Datensätze abgeglichen wurden und welche Regeln angewendet

wurden. Das folgende Verfahren zeigt, wie Sie entweder über die AWS Entity Resolution Konsole oder die `GetMatchID` API auf diese Daten zugreifen.

Console

So suchen Sie mithilfe der Konsole nach einer Match-ID

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie den regelbasierten Matching-Workflow aus, der verarbeitet wurde (Auftragsstatus ist Abgeschlossen).
4. Wählen Sie auf der Seite mit den passenden Workflow-Details die Registerkarte „IDs abgleichen“.
5. Wählen Sie Match-ID nachschlagen aus.

> **Note**
>
> Die Option Match-ID nachschlagen ist nur für passende Workflows verfügbar, die den automatischen Verarbeitungsrhythmus verwenden. Wenn Sie den manuellen Verarbeitungsrhythmus ausgewählt haben, wird diese Option als inaktiv angezeigt. Um diese Option zu verwenden, bearbeiten Sie Ihren Arbeitsablauf so, dass der automatische Verarbeitungsrhythmus verwendet wird. Weitere Informationen zum Bearbeiten von Workflows finden Sie unterBearbeitung eines passenden Workflows.

6. Führen Sie eine der folgenden Aktionen aus:

Wenn...	Dann...
Diesem Workflow ist nur eine Schemazuordnung zugeordnet.	Zeigen Sie die Schemazuordnung an, die standardmäßig ausgewählt ist.
Diesem Workflow ist mehr als eine Schemazuordnung zugeordnet.	Wählen Sie die Schemazuordnung aus der Dropdownliste aus.

7. Geben Sie für Datensatzattribute den Wert für einen vorhandenen Match-Schlüssel ein, um nach jedem vorhandenen Datensatz zu suchen.

> **Tip**
>
> Geben Sie so viele Werte wie möglich ein, um die Match-ID leichter zu finden.

8. Die Option Daten normalisieren ist standardmäßig ausgewählt, sodass Dateneingaben vor dem Abgleich normalisiert werden. Wenn Sie Daten nicht normalisieren möchten, deaktivieren Sie die Option Daten normalisieren.
9. Wenn Sie die Vergleichsregeln anzeigen möchten, erweitern Sie das Feld Übereinstimmungsregeln anzeigen.
10. Wählen Sie Look up.

    Es wird eine Erfolgsmeldung angezeigt, die besagt, dass die Match-ID gefunden wurde.
11. Zeigen Sie die entsprechende Match-ID und die zugehörige Regel an, die gefunden wurde.

API

Um mithilfe der API nach einer Match-ID zu suchen

> **Note**
>
> Um diese API erfolgreich aufrufen zu können, müssen Sie zunächst einen regelbasierten Matching-Workflow mithilfe der StartMatchingJob API erfolgreich ausgeführt haben. Eine vollständige Liste der unterstützten Programmiersprachen finden Sie im Abschnitt Siehe auch der GetMatch ID-API.

1. Öffnen Sie ein Terminal oder eine Eingabeaufforderung, um die API-Anfrage zu stellen.
2. Erstellen Sie eine POST-Anfrage an den folgenden Endpunkt:

```
/matchingworkflows/workflowName/matches
```

3. Stellen Sie im Anforderungsheader das Content-type auf ein application/json.
4. Geben Sie in der Anforderungs-URI Ihre an`workflowName`.

   Das `workflowName` muss:

   - Zwischen 1 und 255 Zeichen lang sein

- Entspricht dem Muster [a-z A-Z _0-9-] *

5. Geben Sie für den Anforderungstext den folgenden JSON-Code an:

```
{
   "applyNormalization": boolean,
   "record": {
      "string" : "string"
   }
}
```

Wobei Folgendes gilt:

`applyNormalization`(optional) — Auf setzen, `true` um die im Schema definierten Attribute zu normalisieren

`record`(erforderlich) — Der Datensatz, für den die Match-ID abgerufen werden soll

6. Senden Sie die Anforderung .

Bei Erfolg erhalten Sie eine Antwort mit dem Statuscode 200 und einem JSON-Text, der Folgendes enthält:

```
{
   "matchId": "string",
   "matchRule": "string"
}
```

Das `matchId` ist der eindeutige Bezeichner für diese Gruppe von übereinstimmenden Datensätzen und `matchRule` gibt an, nach welcher Regel der Datensatz abgeglichen wurde.

Wenn der Anruf nicht erfolgreich ist, erhalten Sie möglicherweise eine der folgenden Fehlermeldungen:

- 403 — AccessDeniedException wenn Sie keinen ausreichenden Zugriff haben
- 404 — ResourceNotFoundException wenn die Ressource nicht gefunden werden kann
- 429 — ThrottlingException wenn die Anfrage gedrosselt wurde
- 400 — ValidationException wenn die Eingabe die Überprüfung nicht besteht
- 500 — InternalServerException wenn ein interner Servicefehler vorliegt

Löschen von Datensätzen aus einem regelbasierten oder passenden Workflow ML-based

Wenn Sie die Datenverwaltungsvorschriften einhalten müssen, können Sie die Datensätze entweder aus einem regelbasierten oder aus einem passenden Workflow löschen. ML-based

Um Datensätze aus einem regelbasierten oder passenden Workflow zu löschen ML-based

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter. https://console.aws.amazon.com/entityresolution/
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie den regelbasierten oder ML-based passenden Workflow aus.
4. Wählen Sie auf der Seite mit den passenden Workflow-Details in der Dropdownliste Aktionen die Option Eindeutige IDs löschen aus.
5. Geben Sie im Abschnitt Eindeutige IDs die eindeutige ID ein, die Sie löschen möchten.

   Sie können bis zu 10 eindeutige IDs eingeben.
6. Geben Sie die Eingabequelle an, aus der die eindeutigen IDs gelöscht werden sollen.

   Wenn es nur eine Eingabequelle für den Workflow gibt, wird die Eingabequelle standardmäßig aufgeführt.

   Wenn Sie nur eine Eingabequelle angeben, werden die eindeutigen IDs in anderen Eingabequellen nicht beeinflusst.
7. Wählen Sie „Eindeutige IDs löschen“.

Fehlerbehebung bei passenden Workflows

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Ausführung von passenden Workflows auftreten können.

Ich habe nach der Ausführung eines passenden Workflows eine Fehlerdatei erhalten

Häufige Ursache

Ein passender Workflow kann mehrere Durchläufe haben und die Ergebnisse (Erfolge oder Fehler) werden in einen Ordner mit dem `jobId` Namen geschrieben.

Die erfolgreichen Ergebnisse eines Abgleichsworkflows werden in einen `success` Ordner geschrieben, der mehrere Dateien enthält, und jede Datei enthält eine Teilmenge der erfolgreichen Datensätze.

Die Fehler für einen passenden Workflow werden in einen `error` Ordner mit mehreren Feldern geschrieben, von denen jedes eine Teilmenge der Fehlerdatensätze enthält.

Die Fehlerdatei kann aus den folgenden Gründen erstellt werden:

- Die eindeutige ID lautet:
  - Null
  - fehlt in einer Datenzeile
  - fehlt in einem Datensatz in der Datentabelle
  - wiederholt in einer anderen Datenzeile in der Datentabelle
  - nicht angegeben
  - innerhalb derselben Quelle nicht eindeutig
  - nicht einzigartig in mehreren Quellen
  - überschneidet sich zwischen den Quellen
  - mehr als 38 Zeichen (nur regelbasierter Matching-Workflow)
- Eines der Felder in der Schemazuordnung enthält einen reservierten Namen:
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - ID abgleichen
  - HashingProtocol
  - ConfidenceLevel
  - Quelle

> **Note**
>
> Wenn der Datensatz in der Fehlerdatei aus den oben genannten Gründen erstellt wurde, wird Ihnen eine Gebühr berechnet, da dadurch Bearbeitungskosten für den Service anfallen. Wenn der Eintrag in der Fehlerdatei auf einen internen Serverfehler zurückzuführen ist, werden Ihnen keine Gebühren berechnet.

Auflösung

Um dieses Problem zu lösen

1. Prüfen Sie, ob die Unique ID gültig ist.

   Wenn die eindeutige ID nicht gültig ist, aktualisieren Sie die eindeutige ID in Ihrer Datentabelle, speichern Sie die neue Datentabelle, erstellen Sie eine neue Schemazuordnung und führen Sie den entsprechenden Workflow erneut aus.
2. Prüfen Sie, ob eines der Felder in der Schemazuordnung einen reservierten Namen enthält.

   Wenn eines der Felder einen reservierten Namen enthält, erstellen Sie eine neue Schemazuordnung mit einem neuen Namen und führen Sie den entsprechenden Workflow erneut aus.

Eingabedaten mithilfe eines ID-Zuordnungs-Workflows zuordnen

Ein ID-Mapping-Workflow ist ein Datenverarbeitungsjob, der Daten aus einer Eingabedatenquelle einem Eingabedatenziel auf der Grundlage der angegebenen ID-Zuordnungsmethode zuordnet. Er erzeugt eine ID-Zuordnungstabelle.

Ein ID-Zuordnungs-Workflow erfordert eine Eingabedatenquelle und ein Eingabedatenziel. Ihre Dateneingabequelle und Ihr Ziel hängen von der Art der ID-Zuordnung ab, die Sie durchführen möchten. Es gibt zwei Möglichkeiten, die ID-Zuordnung durchzuführen: regelbasierte Dienste oder Anbieterdienste:

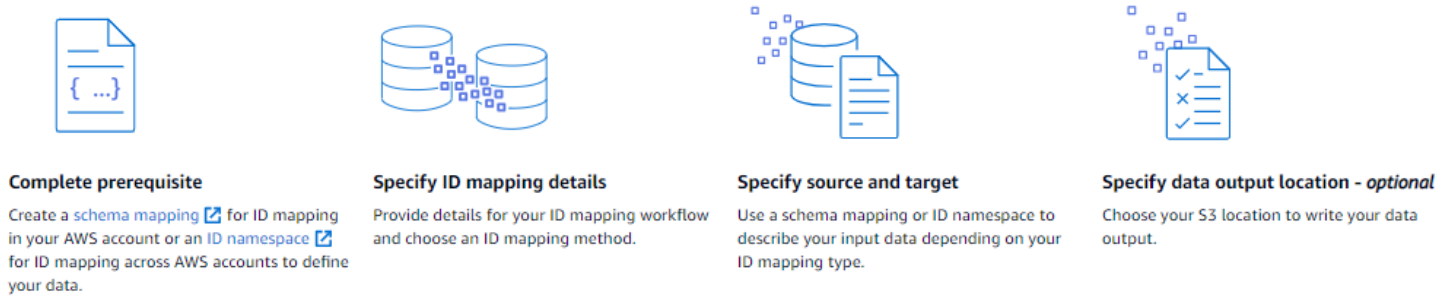
- Rule-based ID-Zuordnung — Sie verwenden Abgleichsregeln, um Erstanbieter-Daten von einer Quelle in ein Ziel zu übersetzen.
- ID-Zuordnung von Providerdiensten — Sie verwenden den LiveRamp Provider-Service, um Daten von Drittanbietern von einer Quelle in ein Ziel zu übersetzen.

> **Note**
>
> Der Workflow zur ID-Zuordnung von Providerdiensten in AWS Entity Resolution ist derzeit in integriert LiveRamp. Wenn Sie über ein Abonnement für den LiveRamp Dienst verfügen, können Sie einen ID-Zuordnungs-Workflow für LiveRamp die Transcodierung erstellen. Mit der LiveRamp Transcodierung können Sie eine Reihe von Quell-RampIDs in eine beliebige Ziel-RampID übersetzen. Indem Sie die RampID als Token zur Darstellung Ihrer Kunden verwenden, können Sie vermeiden, Kundendaten direkt an Werbeplattformen weiterzugeben.
> Weitere Informationen finden Sie auf der Dokumentationswebsite unter Perform Translation Through ADX. LiveRamp

Sie können eine ID-Zuordnung zwischen zwei Datensätzen in einem der folgenden Szenarien durchführen:

- In Ihrem eigenen AWS-Konto
- Über zwei verschiedene AWS-Konten

Das folgende Diagramm fasst zusammen, wie Sie einen ID-Mapping-Workflow einrichten.



Themen

- Workflow für die ID-Zuordnung für einen AWS-Konto
- Workflow zur ID-Zuordnung über zwei AWS-Konten
- Ausführen eines Workflows zur ID-Zuordnung
- Ausführen eines benutzerdefinierten ID-Zuordnungs-Workflows
- Bearbeitung eines Workflows zur ID-Zuordnung
- Löschen eines Workflows zur ID-Zuordnung
- Hinzufügen oder Aktualisieren einer Ressourcenrichtlinie für einen ID-Zuordnungs-Workflow

Workflow für die ID-Zuordnung für einen AWS-Konto

Ein ID-Zuordnungs-Workflow für einen AWS-Konto ermöglicht es Ihnen, die ID-Zuordnung zwischen zwei Datensätzen selbst durchzuführen. AWS-Konto

Bevor Sie selbst einen ID-Zuordnungs-Workflow erstellen AWS-Konto, müssen Sie zunächst die Voraussetzungen erfüllen.

Nachdem Sie einen ID-Zuordnungs-Workflow erstellt und ausgeführt haben, können Sie die Ausgabe (die ID-Zuordnungstabelle) anzeigen und für Analysen verwenden.

Die folgenden Themen führen Sie durch eine Reihe von Schritten zum Erstellen eines ID-Mapping-Workflows in demselben AWS-Konto.

Themen

- Voraussetzungen
- Erstellen eines Workflows zur ID-Zuordnung (regelbasiert)

- Erstellen eines Workflows für die ID-Zuordnung (Provider-Services)

Voraussetzungen

Bevor Sie AWS-Konto mit der ID-Zuordnungsmethode Rule-basedoder der ID-Zuordnungsmethode für Provider Services einen Workflow für eine ID erstellen, müssen Sie zunächst wie folgt vorgehen:

- Führen Sie die Aufgaben unter Einrichtung aus AWS Entity Resolution.
- Führen Sie die Aufgaben in ausEingabedatentabellen vorbereiten, je nachdem, welche Art von Eingabedaten Sie verwenden.
- Erstellen Sie ein Schema-Mapping oder Erstellen Sie einen passenden Workflow.
- (Nur ID-Zuordnung von Provider-Services) Bevor Sie einen ID-Mapping-Workflow mit erstellen LiveRamp, müssen Sie einen Amazon Simple Storage Service (Amazon S3) -Daten-Staging-Bucket auswählen, in den Sie vorübergehend die ID-Zuordnungs-Workflow-Ausgabe schreiben möchten.

  Wenn Sie den LiveRamp Provider-Service zum Übersetzen von Daten von Drittanbietern verwenden, fügen Sie die folgende Berechtigungsrichtlinie hinzu, mit der Sie auf den Daten-Staging-Bucket zugreifen können.

  JSON

```
{
    "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>/*"
            ]
        }
    ]
}
```

Ersetzen Sie in der vorherigen Berechtigungsrichtlinie jede *<user input placeholder>* durch Ihre eigenen Informationen.

staging-bucket	Der Amazon S3 S3-Bucket, in dem Ihre Daten vorübergehend gespeichert werden, während ein auf Anbieterdiensten basierender Workflow ausgeführt wird.

Erstellen eines Workflows zur ID-Zuordnung (regelbasiert)

In diesem Thema wird beschrieben, wie Sie einen ID-Zuordnungs-Workflow für einen Workflow erstellen AWS-Konto , der Abgleichsregeln verwendet, um Erstanbieter-Daten von einer Quelle in ein Ziel zu übersetzen.

So erstellen Sie einen regelbasierten ID-Zuordnungs-Workflow für ein AWS-Konto

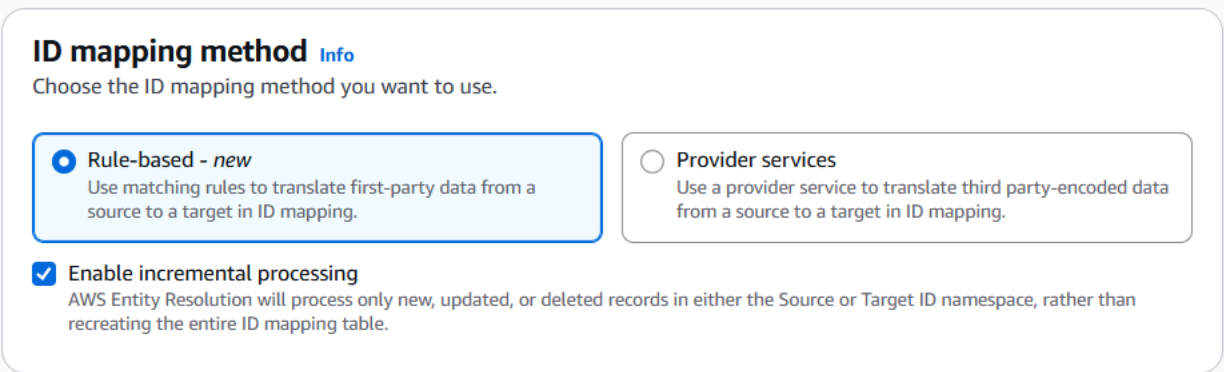
1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter. https://console.aws.amazon.com/entityresolution/

2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie auf der Seite mit den Workflows für die ID-Zuordnung in der oberen rechten Ecke die Option ID-Mapping-Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Workflow-Details für die ID-Zuordnung angeben wie folgt vor.

    a. Geben Sie einen Workflow-Namen für die ID-Zuordnung und optional eine Beschreibung ein.

    b. Wählen Sie für die ID-Zuordnungsmethode Rule-based.

    c. (Optional) Um nur neue, aktualisierte oder gelöschte Datensätze im Workflow zu verarbeiten, wählen Sie Inkrementelle Verarbeitung aktivieren aus.



    AWS Entity Resolution verarbeitet nur neue, aktualisierte oder gelöschte Datensätze im Quell- oder Ziel-ID-Namespace, anstatt die gesamte ID-Zuordnungstabelle neu zu erstellen.

    Wenn Sie die inkrementelle Verarbeitung wählen und Ihre Datentabelle eine DELETE-Spalte enthält, werden Datensätze je nach dem Wert der DELETE-Spalte unterschiedlich AWS Entity Resolution behandelt.

    - Datensätze, die als `true` in der DELETE-Spalte markiert sind, werden aus der ID-Zuordnungstabelle entfernt.
    - Datensätze, die `false` in der Spalte DELETE markiert sind, werden in Amazon S3 aufgenommen.

    Wenn Sie diese Option nicht ausgewählt lassen, AWS Entity Resolution wird der standardmäßige ID-Mapping-Workflow für die Batch-Verarbeitung in der ID-Zuordnungstabelle ausgeführt.

d. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

e. Wählen Sie Weiter aus.

5. Gehen Sie für Schritt 2: Quelle und Ziel angeben wie folgt vor.

a. Wählen Sie unter Quelle das Szenario aus, das auf Sie zutrifft, und ergreifen Sie dann die empfohlene Maßnahme.

Szenario	Empfohlene Aktion
Verwenden Sie im ID-Zuordnungs-Workflow Ihre eigene AWS Glue Datenbank -, AWS Glue Tabellen- und Schemazuordnung.	1. Wählen Sie Schema-Mapping. 2. Wählen Sie eine AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus. Sie können bis zu 19 Dateneingaben hinzufügen.
Verwenden Sie einen vorhandenen Abgleichsworkflow, der auf die Datensatzdaten verweist, die Sie im ID-Zuordnungs-Workflow verwenden möchten.	1. Wählen Sie Matching Workflow aus. 2. Wählen Sie einen vorhandenen Matching-Workflow aus der Drop-down-Liste aus.

b. Wählen Sie für Target einen vorhandenen Matching-Workflow aus der Drop-down-Liste aus.

c. Gehen Sie für Regelparameter wie folgt vor.

i. Geben Sie die Regelsteuerelemente an, indem Sie je nach Quelltyp eine der folgenden Optionen auswählen.

Source type (Quellentyp)	Empfohlene Aktion
Passender Arbeitsablauf	Geben Sie die Regelsteuerelemente an, indem Sie auswählen, ob eine Quelle, ein Ziel oder beide Regeln in einem ID-Mapping-Workflow bereitstellen können.

Source type (Quellentyp)	Empfohlene Aktion
	Regelsteuerelemente müssen zwischen der Quelle und dem Ziel kompatibel sein, um in einem ID-Mapping-Workflow verwendet werden zu können. Wenn beispielsweise ein Quell-ID-Namespace Regeln auf das Ziel beschränkt, der Ziel-ID-Namespace die Regeln jedoch auf die Quelle beschränkt, führt dies zu einem Fehler.
Schemazuordnung	Überspringen Sie diesen Schritt.

ii. Für Vergleichs- und Abgleichsparameter wird der Vergleichstyp automatisch auf Mehrere Eingabefelder gesetzt.

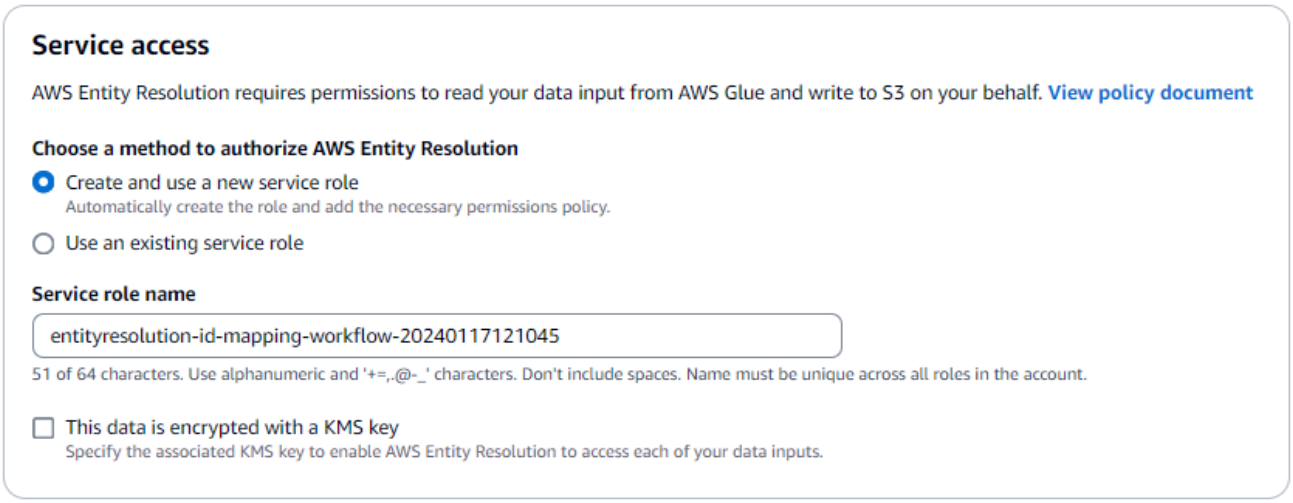
Dies liegt daran, dass beide Teilnehmer diese Option zuvor ausgewählt hatten.

d. Geben Sie den Datensatzabgleichstyp an, indem Sie je nach Ziel eine der folgenden Optionen auswählen.

Ihr Ziel	Empfohlene Option
Beschränken Sie den Datensatzabgleichstyp so, dass für jeden übereinstimmenden Datensatz im Ziel nur ein übereinstimmender Datensatz in der Quelle gespeichert wird, wenn Sie den ID-Mapping-Workflow erstellen.	Eine Quelle zu einem Ziel
Beschränken Sie den Datensatzabgleichstyp auf das Speichern aller übereinstimmenden Datensätze in der Quelle für jeden übereinstimmenden Datensatz im Ziel, wenn Sie den ID-Mapping-Workflow erstellen.	Viele Quellen für ein Ziel

> **Note**
>
> Sie müssen kompatible Einschränkungen für die Quell- und Ziel-ID-Namespaces angeben.

e. Um die Dienstzugriffsberechtigungen anzugeben, wählen Sie eine Option und ergreifen Sie die empfohlene Maßnahme.



Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautet`entityresolution-id-mapping-workflow-<timestamp>` . • Sie benötigen die erforderlichen Berechtigungen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.

Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

6. Wählen Sie Weiter aus.
7. Gehen Sie für Schritt 3: Speicherort für die Datenausgabe angeben — optional — wie folgt vor.
   a. Gehen Sie für das Datenausgabeziel wie folgt vor:
      i. Wählen Sie den Amazon S3 S3-Standort für die Datenausgabe.
      ii. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel-ARN ein oder wählen Sie AWS KMS Schlüssel erstellen.
   b. Wählen Sie Weiter aus.

8. Gehen Sie für Schritt 4: Überprüfen und erstellen wie folgt vor.

    a. Überprüfen Sie die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

    b. Wählen Sie Erstellen aus.

    Es wird eine Meldung angezeigt, die darauf hinweist, dass der Workflow für die ID-Zuordnung erstellt wurde.

Nachdem Sie den ID-Zuordnungs-Workflow erstellt haben, können Sie einen ID-Zuordnungs-Workflow ausführen.

Erstellen eines Workflows für die ID-Zuordnung (Provider-Services)

In diesem Thema wird beschrieben, wie Sie AWS-Konto mithilfe eines Provider-Dienstes namens einen ID-Zuordnungs-Workflow für eine Person erstellen LiveRamp. LiveRamp übersetzt einen Satz von Quell-RampIDs in einen anderen Satz, wobei entweder verwaltete oder abgeleitete RampIDs verwendet werden.

So erstellen Sie einen auf Anbieterdiensten basierenden ID-Zuordnungs-Workflow für einen AWS-Konto

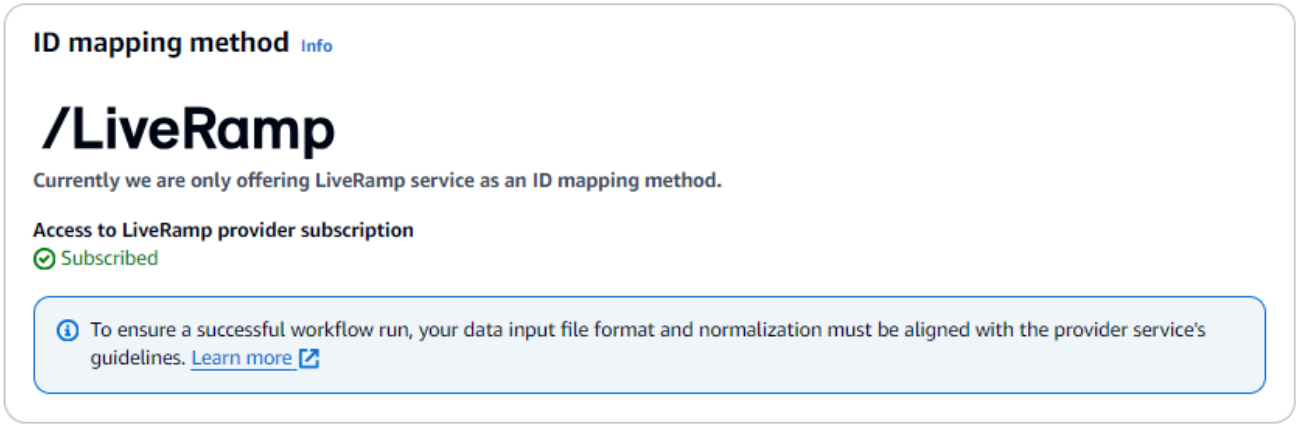
1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie auf der Seite mit den Workflows für die ID-Zuordnung in der oberen rechten Ecke die Option ID-Mapping-Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Workflow-Details für die ID-Zuordnung angeben wie folgt vor.

    a. Geben Sie einen Workflow-Namen für die ID-Zuordnung und optional eine Beschreibung ein.

    b. Wählen Sie für die ID-Zuordnungsmethode Provider Services aus.

    AWS Entity Resolution bietet derzeit den LiveRamp Provider-Service als ID-Zuordnungsmethode an. Wenn Sie ein Abonnement für haben LiveRamp, wird der Status

als Abonniert angezeigt. Weitere Informationen zum Abonnieren finden Sie LiveRamp unterSchritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange.



> **Note**
>
> Stellen Sie sicher, dass das Format Ihrer Dateneingabedatei den Richtlinien des Dienstanbieters entspricht. Weitere Informationen zu den Richtlinien zur Formatierung LiveRamp von Eingabedateien finden Sie unter Perform Translation Through ADX auf der LiveRamp Dokumentationswebsite.

c. Geben Sie für die LiveRamp Konfiguration die folgenden Werte ein, die Folgendes LiveRamp bieten:

- Kunden-ID-Manager ARN
- Kundengeheimverwalter ARN

d. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

e. Wählen Sie Weiter aus.

5. Gehen Sie für Schritt 2: Quelle und Ziel angeben wie folgt vor.

a. Wählen Sie unter Quelle das Szenario aus, das auf Sie zutrifft, und ergreifen Sie dann die empfohlene Maßnahme.

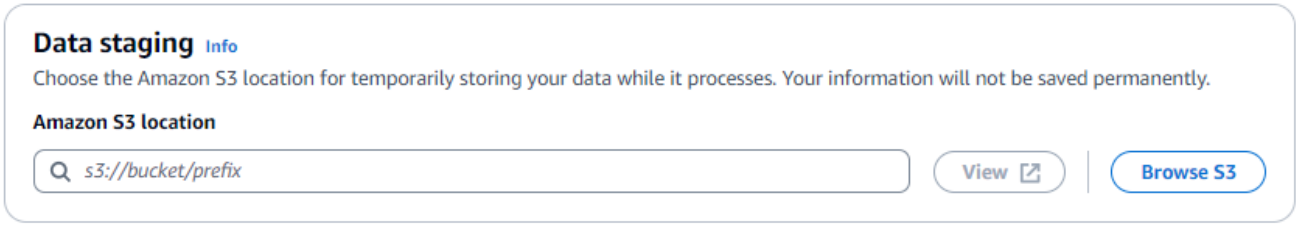
Szenario	Empfohlene Aktion
Verwenden Sie im ID-Zuordnungs-Workflow Ihre eigene AWS Glue Datenbank -, AWS Glue Tabellen- und Schemazuordnung.	1. Wählen Sie Schema-Mapping. 2. Wählen Sie eine AWS Glue Datenbank AWS-Region, die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus. Sie können bis zu 19 Dateneingaben hinzufügen.
Verwenden Sie einen vorhandenen Abgleichsworkflow, der auf die Datensatzdaten verweist, die Sie im ID-Zuordnungs-Workflow verwenden möchten.	1. Wählen Sie Matching Workflow aus. 2. Wählen Sie einen vorhandenen Matching-Workflow aus der Drop-down-Liste aus.

b. Führen Sie für Target je nach der von Ihnen ausgewählten ID-Zuordnungsmethode eine der folgenden Aktionen aus.

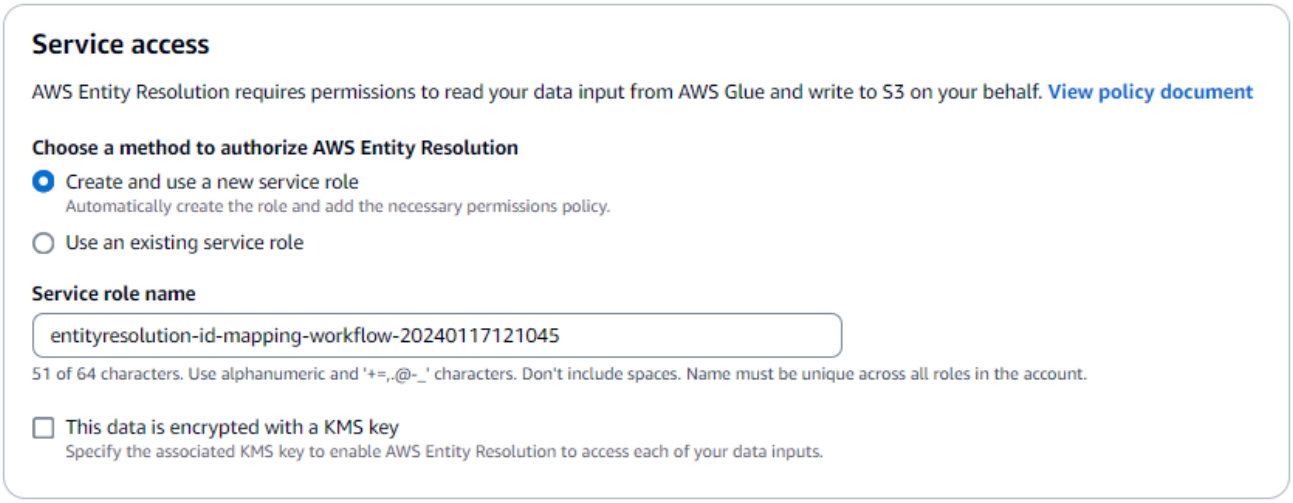
Methode der ID-Zuordnung	Empfohlene Aktion
Rule-based	Wählen Sie einen vorhandenen Matching-Workflow aus der Dropdownliste aus.
Dienste des Anbieters	Geben Sie die für die Transcodierung vorgesehene LiveRamp Client-Domänenkennung ein, die LiveRamp in der Zieldomäne bereitgestellt wird.

Methode der ID-Zuordnung	Empfohlene Aktion

c. Wählen Sie für Data Staging den Amazon S3 S3-Speicherort aus, an den Sie vorübergehend die Workflow-Ausgabe für die ID-Zuordnung schreiben möchten.



d. Um die Zugriffsberechtigungen für den Service festzulegen, wählen Sie eine Option und ergreifen Sie die empfohlene Maßnahme.

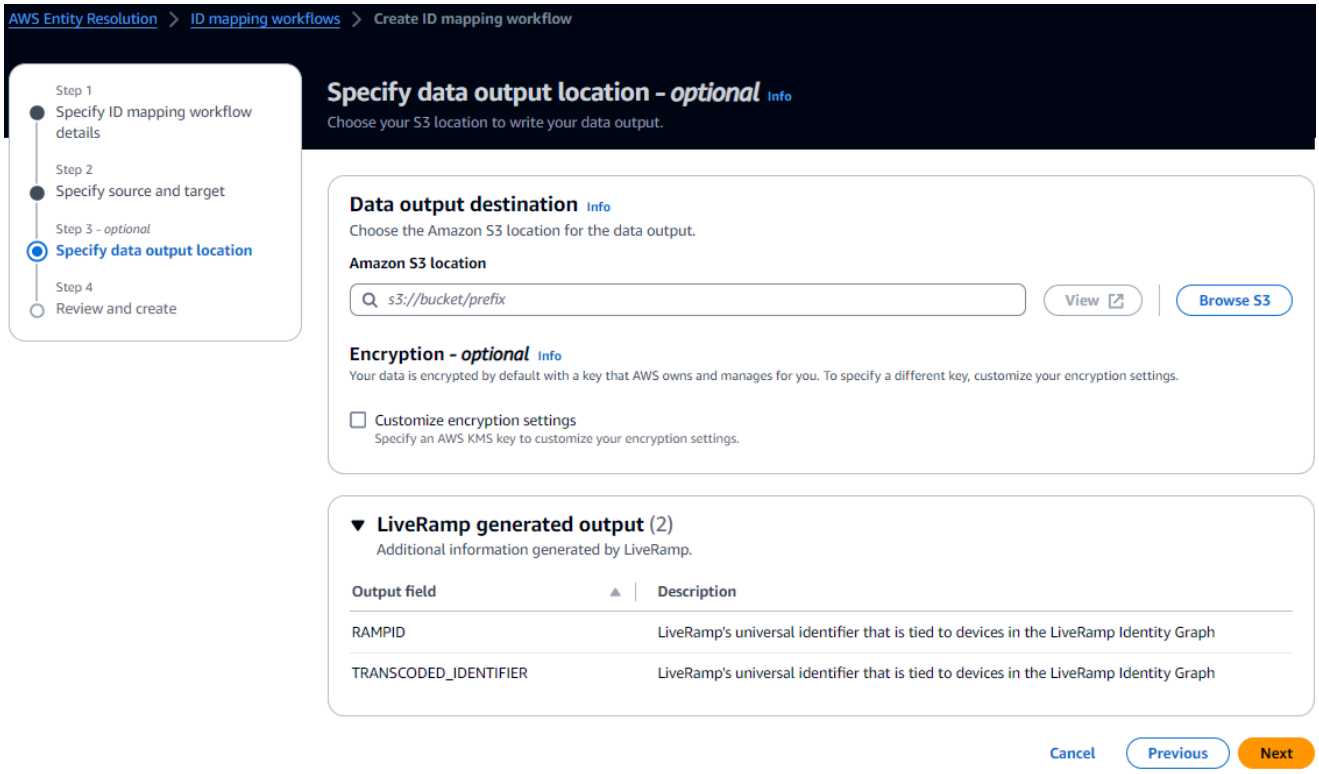


Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautet`entityresolution-id-mapping-workflow-<timestamp>` . • Sie benötigen die erforderlichen Berechtigungen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.

Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

6. Wählen Sie Weiter aus.
7. Gehen Sie für Schritt 3: Speicherort für die Datenausgabe angeben — optional — wie folgt vor.
   a. Gehen Sie für das Datenausgabeziel wie folgt vor:
      i. Wählen Sie den Amazon S3 S3-Standort für die Datenausgabe.
      ii. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel-ARN ein oder wählen Sie AWS KMS Schlüssel erstellen.
   b. Sehen Sie sich die LiveRamp generierte Ausgabe an.

c. Wählen Sie Weiter aus.



8. Gehen Sie für Schritt 4: Überprüfen und erstellen wie folgt vor.

   a. Überprüfen Sie die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Erstellen aus.

      Es wird eine Meldung angezeigt, die darauf hinweist, dass der Workflow für die ID-Zuordnung erstellt wurde.

9. Nachdem Sie den ID-Zuordnungs-Workflow erstellt haben, können Sie einen ID-Zuordnungs-Workflow ausführen.

Workflow zur ID-Zuordnung über zwei AWS-Konten

Ein zweifacher ID-Mapping-Workflow AWS-Konten ermöglicht es Ihnen, eine ID-Zuordnung zwischen zwei Datensätzen über zwei AWS-Konten durchzuführen. Dies erfolgt in der Regel zwischen Ihrem eigenen AWS-Konto und einem anderen AWS-Konto.

Ein Publisher kann beispielsweise einen ID-Mapping-Workflow erstellen, indem er seinen eigenen Ziel-ID-Namespace (in seinem eigenen AWS-Konto) und den Quell-ID-Namespace eines Werbetreibenden (in einem anderen) verwendet. AWS-Konto

Bevor Sie einen Workflow für die ID-Zuordnung erstellen, der zwei Elemente umfasst AWS-Konten, müssen Sie zunächst die Voraussetzungen erfüllen.

Nachdem Sie einen ID-Mapping-Workflow erstellt haben, können Sie die Ausgabe (die ID-Zuordnungstabelle) anzeigen und für Analysen verwenden.

Die folgenden Themen führen Sie durch eine Reihe von Schritten zur Erstellung eines Workflows für die ID-Zuordnung, der sich aus zwei Schritten zusammensetzt AWS-Konten:

Themen

- Voraussetzungen
- Erstellen eines Workflows zur ID-Zuordnung (regelbasiert)
- Erstellen eines Workflows für die ID-Zuordnung (Provider-Services)

Voraussetzungen

Bevor Sie einen Workflow für die ID-Zuordnung erstellen, der zwei Elemente AWS-Konten umfasst, müssen Sie zunächst wie folgt vorgehen:

- Führen Sie die Aufgaben unter au Einrichten AWS Entity Resolution.
- Erstellen Sie eine ID-Namespace-Quelle.
- Erstellen Sie ein ID-Namespace-Ziel.
- Erwerben Sie den ID-Namespace-ARN, wenn Sie eine ID-Namespace-Quelle von einer anderen verwenden. AWS-Konto
- (Nur Provider-Dienste) Für die Erstellung eines Workflows zur ID-Zuordnung, der zwei Elemente umfasst, ist eine Zugriffsberechtigung für LiveRamp den S3-Bucket und den vom Kunden verwalteten AWS Key Management Service Schlüssel (AWS KMS) AWS-Konten erforderlich.

  Bevor Sie einen ID-Mapping-Workflow für zwei AWS-Konten mit erstellen LiveRamp, fügen Sie die folgende Berechtigungsrichtlinie hinzu, die den LiveRamp Zugriff auf den S3-Bucket und den vom Kunden verwalteten Schlüssel ermöglicht.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::715724997226:root"
        },
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
        "Condition": {
            "StringEquals": {
            "kms:ViaService": "s3.us-east-1.amazonaws.com"
            }
        }
    }]
}
```

Ersetzen Sie in der vorherigen Berechtigungsrichtlinie jede *<user input placeholder>* durch Ihre eigenen Informationen.

<KMSKeyARN>	Der ARN eines vom AWS KMS Kunden verwalteten Schlüssels.

Erstellen eines Workflows zur ID-Zuordnung (regelbasiert)

Nachdem Sie die Voraussetzungen erfüllt haben, können Sie einen oder mehrere Workflows für die ID-Zuordnung erstellen, um mithilfe von Abgleichsregeln Erstanbieterdaten von einer Quelle in ein Ziel zu übersetzen.

Um einen regelbasierten Workflow für die ID-Zuordnung zu erstellen, der zwei Elemente umfasst AWS-Konten

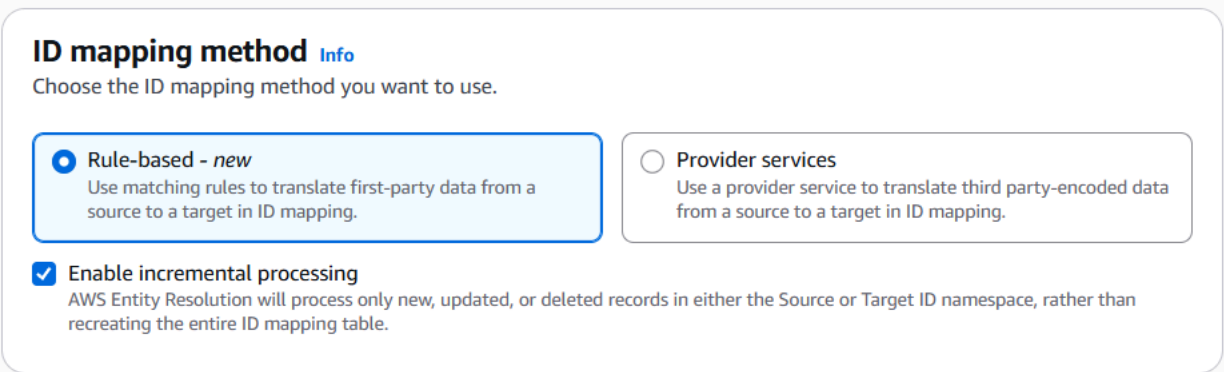
1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter. https://console.aws.amazon.com/entityresolution/

2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie auf der Seite mit den Workflows für die ID-Zuordnung in der oberen rechten Ecke die Option ID-Mapping-Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Workflow-Details für die ID-Zuordnung angeben wie folgt vor.

    a. Geben Sie einen Workflow-Namen für die ID-Zuordnung und optional eine Beschreibung ein.

    b. Wählen Sie für die ID-Zuordnungsmethode Rule-based.

    c. (Optional) Um nur neue, aktualisierte oder gelöschte Datensätze im Workflow zu verarbeiten, wählen Sie Inkrementelle Verarbeitung aktivieren aus.



    AWS Entity Resolution verarbeitet nur neue, aktualisierte oder gelöschte Datensätze im Quell- oder Ziel-ID-Namespace, anstatt die gesamte ID-Zuordnungstabelle neu zu erstellen.

    Wenn Sie die inkrementelle Verarbeitung wählen und Ihre Datentabelle eine DELETE-Spalte enthält, werden Datensätze je nach dem Wert der DELETE-Spalte unterschiedlich AWS Entity Resolution behandelt.

    - Datensätze, die als `true` in der DELETE-Spalte markiert sind, werden aus der ID-Zuordnungstabelle entfernt.
    - Datensätze, die `false` in der Spalte DELETE markiert sind, werden in Amazon S3 aufgenommen.

    Wenn Sie diese Option nicht ausgewählt lassen, AWS Entity Resolution wird der standardmäßige ID-Mapping-Workflow für die Batch-Verarbeitung in der ID-Zuordnungstabelle ausgeführt.

d. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

e. Wählen Sie Weiter aus.

5. Gehen Sie für Schritt 2: Quelle und Ziel angeben wie folgt vor.

a. Aktivieren Sie „Erweiterte Optionen“.

b. Wählen Sie für Quelle die Option Abgleichender Workflow aus und wählen Sie dann den vorhandenen Abgleichs-Workflow aus der Dropdownliste aus.

c. Wählen Sie für Target die Option Abgleichender Workflow aus und wählen Sie dann den vorhandenen Abgleichs-Workflow aus der Dropdownliste aus.

d. Geben Sie für Regelparameter die Regelsteuerelemente an, indem Sie auswählen, ob eine Quelle oder ein Ziel Regeln in einem ID-Mapping-Workflow bereitstellen kann.

   Regelsteuerelemente müssen zwischen der Quelle und dem Ziel kompatibel sein, um in einem ID-Mapping-Workflow verwendet werden zu können. Wenn beispielsweise ein Quell-ID-Namespace Regeln auf das Ziel beschränkt, der Ziel-ID-Namespace die Regeln jedoch auf die Quelle beschränkt, führt dies zu einem Fehler.

e. Gehen Sie wie folgt vor, um Vergleichsparameter und Vergleichsparameter zu ermitteln.

   i. Geben Sie den Vergleichstyp an, indem Sie eine Option auswählen, die auf Ihrem Ziel basiert.

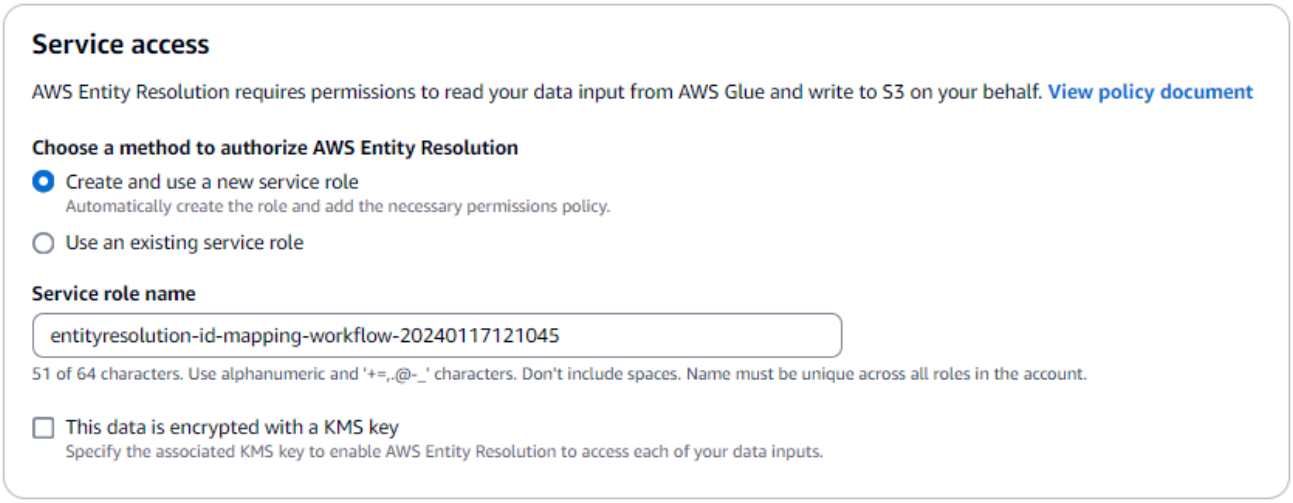
Ihr Ziel	Empfohlene Option
Suchen Sie nach einer beliebigen Kombination von Übereinstimmungen in Daten, die in mehreren Eingabefeldern gespeichert sind, unabhängig davon, ob sich die Daten im selben oder in einem anderen Eingabefeld befinden.	Mehrere Eingabefelder
Beschränken Sie den Vergleich innerhalb eines einzelnen Eingabefe ldes, wenn ähnliche Daten, die in mehreren Eingabefeldern gespeichert sind, nicht zugeordnet werden sollen.	Einzelnes Eingabefeld

ii. Geben Sie den Übereinstimmungstyp Datensatz an, indem Sie eine Option auswählen, die Ihrem Ziel entspricht.

Ihr Ziel	Empfohlene Option
Beschränken Sie den Datensatz abgleichstyp so, dass für jeden übereinst immenden Datensatz im Ziel nur ein übereinstimmender Datensatz in der Quelle gespeichert wird, wenn Sie den ID-Mapping-Workflow erstellen.	Eine Quelle zu einem Ziel
Beschränken Sie den Datensatz abgleichstyp auf das Speichern aller übereinstimmenden Datensätze in der Quelle für jeden übereinstimmenden Datensatz im Ziel, wenn Sie den ID-Mapping-Workflow erstellen.	Viele Quellen für ein Ziel

> **Note**
>
> Sie müssen kompatible Einschränkungen für die Quell- und Ziel-ID-Namespaces angeben.

f. Um die Dienstzugriffsberechtigungen anzugeben, wählen Sie eine Option und ergreifen Sie die empfohlene Maßnahme.



Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautet `entityresolution-id-mapping-workflow-<timestamp>` . • Sie benötigen die erforderlichen Berechtigungen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.

Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

6. Wählen Sie Weiter aus.
7. Gehen Sie für Schritt 3: Speicherort für die Datenausgabe angeben — optional — wie folgt vor.
   a. Gehen Sie für das Datenausgabeziel wie folgt vor.
      i. Wählen Sie den Amazon S3 S3-Standort für die Datenausgabe.
      ii. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel-ARN ein oder wählen Sie AWS KMS Schlüssel erstellen.
   b. Sehen Sie sich die LiveRamp generierte Ausgabe an.

c. Wählen Sie Weiter aus.

8. Gehen Sie für Schritt 4: Überprüfen und erstellen wie folgt vor.

   a. Überprüfen Sie die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Erstellen aus.

      Es wird eine Meldung angezeigt, die darauf hinweist, dass der Workflow für die ID-Zuordnung erstellt wurde.

Nachdem Sie den ID-Zuordnungs-Workflow erstellt haben, können Sie einen ID-Zuordnungs-Workflow ausführen.

Erstellen eines Workflows für die ID-Zuordnung (Provider-Services)

Nachdem Sie die Voraussetzungen erfüllt haben, können Sie mithilfe des LiveRamp Providerdienstes einen oder mehrere Workflows für die ID-Zuordnung erstellen. LiveRamp übersetzt einen Satz von Quell-RampIDs in einen anderen Satz, wobei entweder verwaltete oder abgeleitete RampIDs verwendet werden.

Um einen ID-Mapping-Workflow mit dem Provider-Service zu erstellen

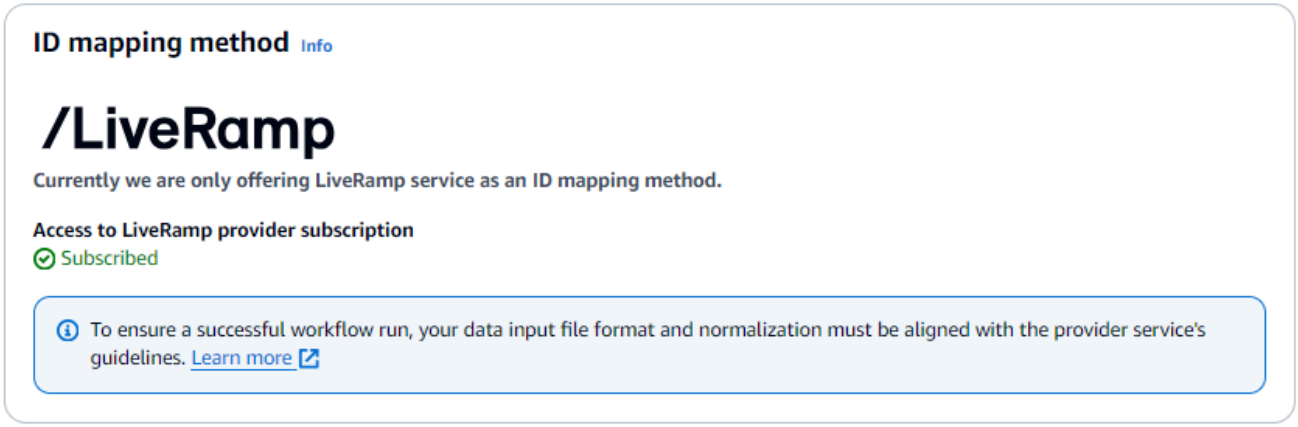
1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie auf der Seite mit den Workflows für die ID-Zuordnung in der oberen rechten Ecke die Option ID-Mapping-Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Workflow-Details für die ID-Zuordnung angeben wie folgt vor.

   a. Geben Sie einen Workflow-Namen für die ID-Zuordnung und optional eine Beschreibung ein.

   b. Wählen Sie für die ID-Zuordnungsmethode Provider Services aus.

      AWS Entity Resolution bietet derzeit den LiveRamp Provider-Service als ID-Zuordnungsmethode an. Wenn Sie ein Abonnement für haben LiveRamp, wird der Status

als Abonniert angezeigt. Weitere Informationen zum Abonnieren finden Sie LiveRamp unterSchritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange.



> **Note**
>
> Stellen Sie sicher, dass das Format Ihrer Dateneingabedatei den Richtlinien des Dienstanbieters entspricht. Weitere Informationen zu den Richtlinien zur Formatierung LiveRamp von Eingabedateien finden Sie unter Perform Translation Through ADX auf der LiveRamp Dokumentationswebsite.

c. Geben Sie für die LiveRamp Konfiguration die folgenden Werte ein, die Folgendes LiveRamp bieten:

- Kunden-ID-Manager ARN
- Kundengeheimverwalter ARN

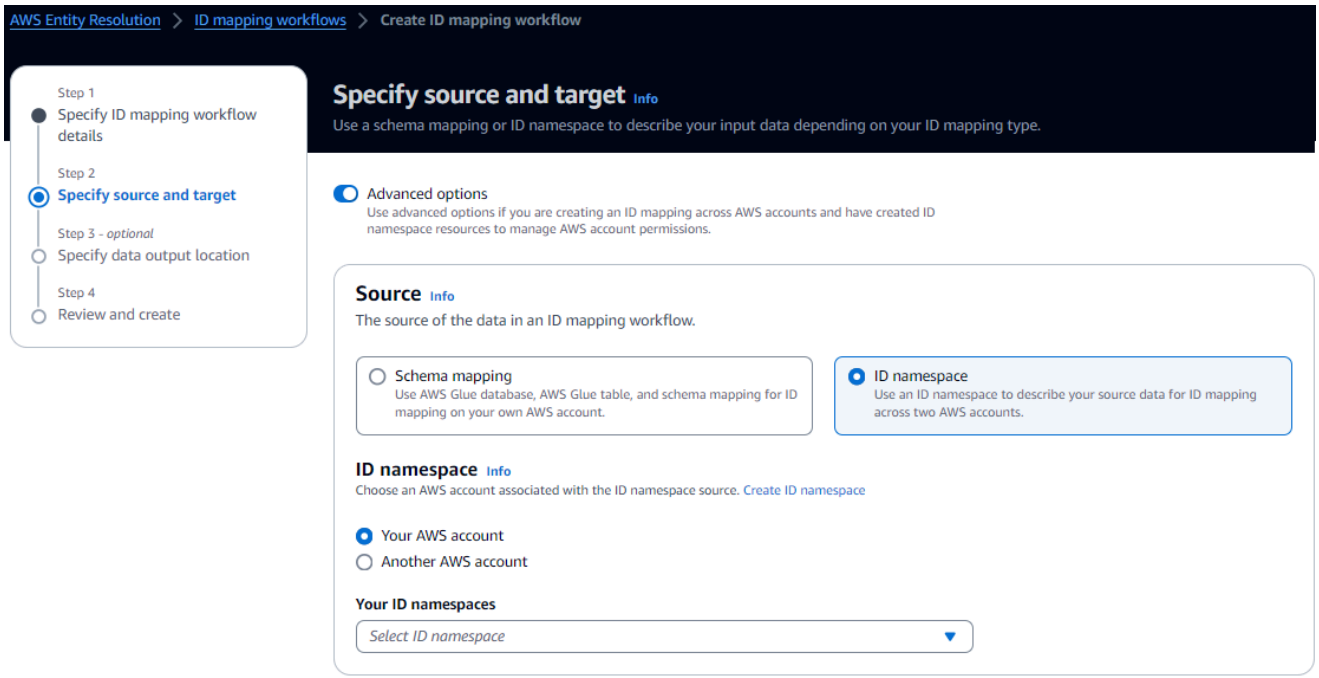
d. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

e. Wählen Sie Weiter aus.

5. Gehen Sie für Schritt 2: Quelle und Ziel angeben wie folgt vor.

a. Aktivieren Sie „Erweiterte Optionen“.

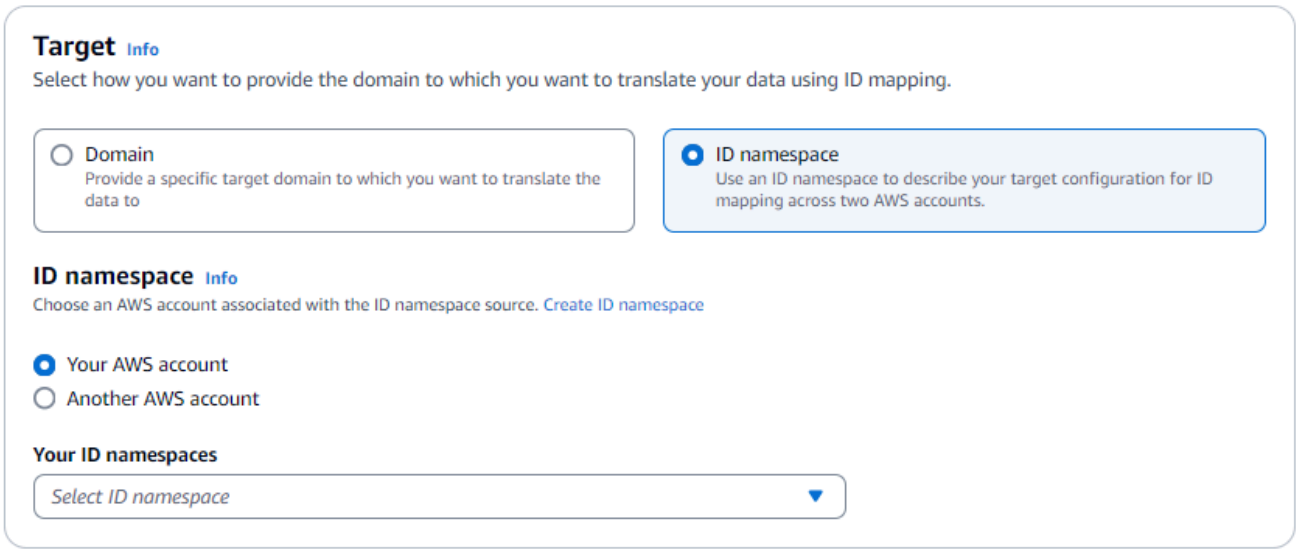
b. Wählen Sie als Quelle den ID-Namespace aus.



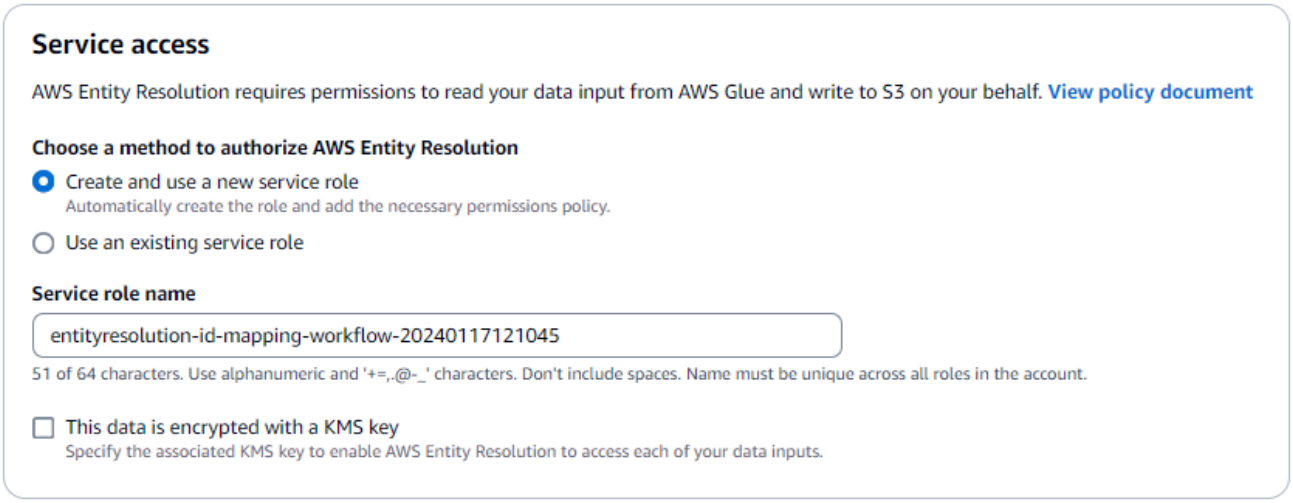
c. Identifizieren Sie für ID-Namespace, wo sich der ID-Namespace befindet, und ergreifen Sie dann die empfohlene Maßnahme.

Speicherort des ID-Namespaces	Empfohlene Aktion
Ihr eigener AWS-Konto	1. Wähle dein AWS-Konto. 2. Wählen Sie den ID-Namespace aus der Dropdownliste Ihre ID-Namespaces aus.
Der von jemand anderem AWS-Konto	1. Wähle einen anderen AWS-Konto. 2. Geben Sie den ID-Namespace ARN ein.

d. Wählen Sie für Target den ID-Namespace aus.



e. Um die Dienstzugriffsberechtigungen anzugeben, wählen Sie eine Option aus und ergreifen Sie die empfohlene Maßnahme.

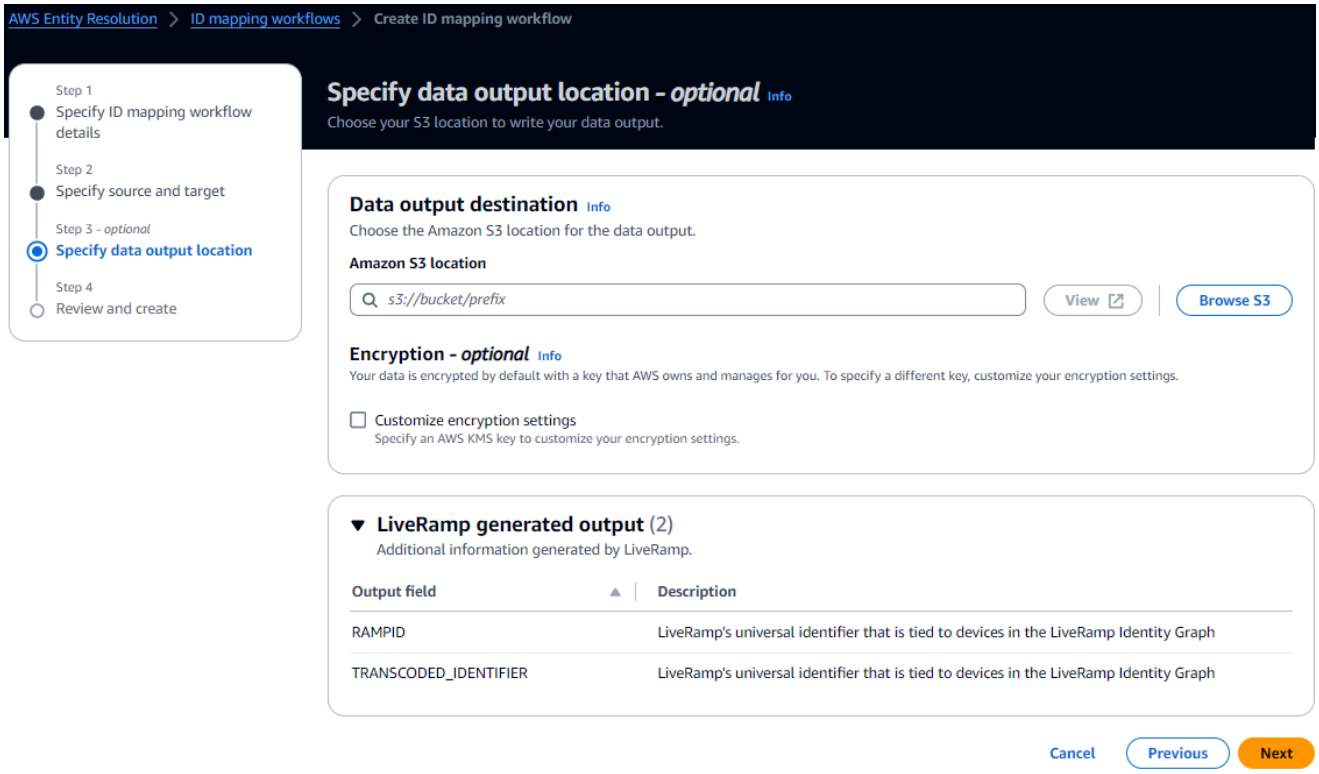


Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautet`entityresolution-id-mapping-workflow-<timestamp>` . • Sie benötigen die erforderlichen Berechtigungen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.

Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

6. Wählen Sie Weiter aus.
7. Gehen Sie für Schritt 3: Speicherort für die Datenausgabe angeben — optional — wie folgt vor.
   a. Gehen Sie für das Datenausgabeziel wie folgt vor.
      i. Wählen Sie den Amazon S3 S3-Standort für die Datenausgabe.
      ii. Wenn Sie unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel-ARN ein oder wählen Sie AWS KMS Schlüssel erstellen.
   b. Sehen Sie sich die LiveRamp generierte Ausgabe an.

c. Wählen Sie Weiter aus.



8. Gehen Sie für Schritt 4: Überprüfen und erstellen wie folgt vor.

   a. Überprüfen Sie die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie Erstellen aus.

      Es wird eine Meldung angezeigt, die darauf hinweist, dass der Workflow für die ID-Zuordnung erstellt wurde.

Nachdem Sie den ID-Zuordnungs-Workflow erstellt haben, können Sie einen ID-Zuordnungs-Workflow ausführen.

Ausführen eines Workflows zur ID-Zuordnung

Nachdem Sie einen ID-Mapping-Workflow für einen AWS-Konto oder einen ID-Zuordnungs-Workflow für zwei erstellt haben AWS-Konten, können Sie den ID-Zuordnungs-Workflow ausführen. Der ID-Zuordnungs-Workflow gibt eine CSV-Datei aus.

Um einen ID-Mapping-Workflow auszuführen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den Workflow für die ID-Zuordnung aus.
4. Wählen Sie auf der Detailseite des ID-Mapping-Workflows in der oberen rechten Ecke die Option Ausführen aus.
5. Sehen Sie sich auf der Seite mit den entsprechenden Workflow-Details auf der Registerkarte Metriken unter Metriken für den letzten Job Folgendes an:

    - Die Job-ID
    - Der Status des passenden Workflow-Jobs: In Warteschlange, In Bearbeitung, Abgeschlossen, Fehlgeschlagen
    - Der Ausführungstyp
    - Die Uhrzeit, zu der der Workflow-Job gestartet wurde
    - Die Zeit, in der der Workflow-Job abgeschlossen wurde
    - Die Dauer des Workflow-Jobs
    - Das Ausgabeziel
    - Die AWS KMS key
    - Die Servicerolle
    - Die Anzahl der Eingabedatensätze
    - Die Anzahl der eindeutigen Datensätze
    - Die Anzahl der geladenen neuen eindeutigen Datensätze
    - Die Anzahl der zugewiesenen Datensätze
    - Die Anzahl der entfernten zugewiesenen Datensätze
    - Die Anzahl der neu zugewiesenen Datensätze
    - Die Anzahl der zugewiesenen Quelldatensätze
    - Die Anzahl der neu zugewiesenen Quelldatensätze
    - Die Anzahl der entfernten zugewiesenen Quelldatensätze
    - Die Anzahl der zugewiesenen Zieldatensätze
    - Die Anzahl der neu zugewiesenen Zieldatensätze

- Die Anzahl der entfernten zugewiesenen Zieldatensätze
- Die Anzahl der verarbeiteten Delete-Datensätze
- Die Anzahl der verarbeiteten Datensätze
- Die Anzahl der nicht verarbeiteten Datensätze

Unter Jobverlauf können Sie auch die Job-Metriken für zuvor ausgeführte ID-Mapping-Workflow-Jobs anzeigen.

6. Nachdem der Workflow-Job für die ID-Zuordnung abgeschlossen ist (Status ist Abgeschlossen), wählen Sie Datenausgabe und dann Ihren Amazon S3 S3-Standort aus, um die Ergebnisse anzuzeigen.

   Nachdem Sie Ihre CSV-Datei erhalten haben, können Sie sie `RAMPID` mit der verbinden`TRANSCODED_ID`.

Ausführen eines benutzerdefinierten ID-Zuordnungs-Workflows

> **Note**
>
> Dieses Verfahren ist für Workflows innerhalb eines einzelnen Workflows AWS-Konto oder für Workflows AWS-Konten mit aktivierter inkrementeller Verarbeitung verfügbar, die sich über zwei Workflows erstrecken.

Wenn Sie einen ID-Mapping-Workflow ausführen, können Sie einen anderen Amazon S3 S3-Speicherort für Ihre Ausgabedaten angeben als den, der ursprünglich konfiguriert wurde. Sie können auch wählen, wie Ihre Daten verarbeitet werden sollen, indem Sie einen von drei Ausführungstypen auswählen: Batch (verarbeitet alle Daten), Inkrementell (verarbeitet nur neue oder geänderte Daten) oder Nur Löschen (verarbeitet nur Löschanfragen).

Um einen ID-Mapping-Workflow mit einem neuen Ausgabeziel auszuführen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den ID-Zuordnungs-Workflow aus, den Sie ausführen möchten.

4. Wählen Sie auf der Detailseite des ID-Zuordnungs-Workflows die Option Workflow ausführen und dann Mit neuem Ausgabeziel ausführen aus.
5. Konfigurieren Sie für das Datenausgabeziel Folgendes.

   a. Wählen Sie für Ausführungstyp eine der folgenden Optionen aus.

      - Batch — Verarbeitet die gesamte ID-Zuordnungstabelle.

        Empfohlen für die Ersteinrichtung, regelmäßige vollständige Aktualisierungen oder wenn signifikante Änderungen sowohl im Quell- als auch im Ziel-ID-Namespace auftreten.
      - Inkrementell — Verarbeitet nur neue, aktualisierte oder gelöschte Datensätze im Quell- oder Ziel-ID-Namespace.

        Empfohlen für häufige Updates, tägliche Datenläufe oder Datensynchronisierung in Echtzeit.
      - Nur löschen — Verarbeitet nur gelöschte Datensätze aus dem Target-ID-Namespace.

        Wird für die schnelle Synchronisation von Löschungen empfohlen.

   b. Wählen Sie den Amazon S3 S3-Standort für die Datenausgabe.
   c. Führen Sie für die Verschlüsselung einen der folgenden Schritte aus:

      - Behalten Sie die standardmäßigen Verschlüsselungseinstellungen bei
      - Wählen Sie Verschlüsselungseinstellungen anpassen und geben Sie entweder den AWS KMS Schlüssel-ARN ein oder wählen Sie AWS KMS Schlüssel erstellen.

6. Um die Zugriffsberechtigungen für den Dienst anzugeben, wählen Sie eine Option und ergreifen Sie die empfohlene Maßnahme.

Option	Empfohlene Aktion
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlini e für diese Tabelle. • Der Standardname der Servicerolle lautet`entityresolution-id-mapping-workflow-<timestamp>` .

Option	Empfohlene Aktion
	• Sie benötigen die erforderlichen Berechtigungen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, wählen Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

7. Klicken Sie auf Ausführen.
8. Sehen Sie sich auf der Seite mit den entsprechenden Workflow-Details auf der Registerkarte Metriken unter Metriken für den letzten Job Folgendes an:

- Die Job-ID
- Die Zeit, in der der Workflow-Job abgeschlossen wurde
- Der Status des passenden Workflow-Jobs: In Warteschlange, In Bearbeitung, Abgeschlossen, Fehlgeschlagen
- Die Anzahl der verarbeiteten Datensätze
- Die Anzahl der nicht verarbeiteten Datensätze
- Die Anzahl der Eingabedatensätze
- Die Anzahl der generierten eindeutigen Match-IDs.
- Die Anzahl der neu zugewiesenen Datensätze.
- Die Anzahl der neu zugewiesenen Zieldatensätze.
- Die Anzahl der neu zugewiesenen Quelldatensätze.
- Die Anzahl neu zugeordneter Quelldatensätze, die entfernt wurden.
- Die Anzahl der neu zugewiesenen Zieldatensätze, die entfernt wurden.
- Die Anzahl neu zugeordneter Datensätze, die entfernt wurden.

Unter Jobverlauf können Sie auch die Job-Metriken für zuvor ausgeführte ID-Mapping-Workflow-Jobs anzeigen.

9. Nachdem der Workflow-Job für die ID-Zuordnung abgeschlossen ist (Status ist Abgeschlossen), wählen Sie Datenausgabe und dann Ihren Amazon S3 S3-Standort aus, um die Ergebnisse anzuzeigen.

   Nachdem Sie Ihre CSV-Datei erhalten haben, können Sie sie `RAMPID` mit der verbinden`TRANSCODED_ID`.

Bearbeitung eines Workflows zur ID-Zuordnung

Durch die Bearbeitung des Workflows zur ID-Zuordnung können Sie Ihre Funktionen zur Auflösung von Entitäten auf dem neuesten Stand halten und an Ihre sich im Laufe der Zeit weiterentwickelnden Geschäftsanforderungen anpassen. Möglicherweise möchten Sie die Zuordnungsregeln, -techniken und -parameter anpassen. Sie können den Workflow optimieren, um genauere und zuverlässigere Ergebnisse beim ID-Abgleich zu erzielen. Möglicherweise möchten Sie auch neue Datenquellen hinzufügen, die Typen der zuzuordnenden IDs erweitern oder zusätzliche Übereinstimmungskriterien in den Workflow integrieren. Wenn Sie Probleme oder Fehler in den Ergebnissen der ID-Zuordnung

feststellen, kann Ihnen die Bearbeitung mit dem Workflow dabei helfen, diese Probleme zu diagnostizieren und zu lösen.

So bearbeiten Sie einen Workflow für die ID-Zuordnung:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den Workflow für die ID-Zuordnung aus.
4. Wählen Sie auf der Detailseite des ID-Mapping-Workflows in der oberen rechten Ecke die Option Bearbeiten aus.
5. Nehmen Sie auf der Seite mit den Details zum Workflow „ID-Zuordnung angeben“ alle erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
6. Nehmen Sie auf der Seite „Datenausgabe angeben“ die erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
7. Nehmen Sie auf der Seite Überprüfen und speichern die erforderlichen Änderungen vor und wählen Sie dann Speichern aus.

Löschen eines Workflows zur ID-Zuordnung

Wenn Sie einen ID-Zuordnungs-Workflow nicht mehr verwenden, kann das Löschen dieses Workflows helfen, Ihr Workflow-Management zu optimieren. Darüber hinaus kann das Löschen redundanter oder weniger effizienter Workflows zur ID-Zuordnung, die ähnlichen Zwecken dienen, Ihnen helfen, Ihre Prozesse zu konsolidieren.

So löschen Sie einen Workflow für die ID-Zuordnung:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den Workflow für die ID-Zuordnung aus.
4. Wählen Sie auf der Detailseite des ID-Mapping-Workflows in der oberen rechten Ecke die Option Löschen aus.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Hinzufügen oder Aktualisieren einer Ressourcenrichtlinie für einen ID-Zuordnungs-Workflow

Eine Ressourcenrichtlinie ermöglicht dem Ersteller der ID-Mapping-Ressource den Zugriff auf Ihre Workflow-Ressource für die ID-Mapping.

Um eine Ressourcenrichtlinie hinzuzufügen oder zu aktualisieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die AWS Entity Resolution Konsole unter https://console.aws.amazon.com/entityresolution/.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den Workflow für die ID-Zuordnung aus.
4. Wählen Sie auf der Detailseite des Workflows für die ID-Zuordnung die Registerkarte Berechtigungen aus.
5. Wählen Sie im Abschnitt Ressourcenrichtlinie die Option Bearbeiten aus.
6. Fügen Sie die Richtlinie im JSON-Editor hinzu oder aktualisieren Sie sie.
7. Wählen Sie Änderungen speichern aus.

AWS Entity Resolution Als Anbieter integrieren

AWS Entity Resolution Integrationen von Drittanbietern helfen Kunden dabei, die Privatsphäre der Verbraucher zu schützen und die Einhaltung der Gesetze zur Datenhoheit aufrechtzuerhalten. Drittanbieter wie Ramp LiveRamp IDs und TransUnion Fabrick setzen Verbraucher-Identifikatoren in Werbung IDs um. IDs Diese Werbekennungen werden häufig in Werbe- und Marketingtools verwendet, um zu verhindern, dass Verbraucherdaten in nicht verwaltete Systeme exportiert werden.AWS Dieser Abschnitt enthält Anleitungen für Anbieter zur Integration von Verbraucher-Identifikatoren AWS Entity Resolution zur Kodierung oder Transcodierung in Werbung IDs zur Verwendung in einem auf Anbieterdiensten basierenden Matching-Workflow.

Weitere Informationen zu den Anbieterdiensten, die derzeit integriert sind, finden Sie unter. AWS Entity ResolutionErstellen eines auf dem Provider-Service basierenden Matching-Workflows

Themen

- Voraussetzungen
- Verwendung der AWS Entity Resolution OpenAPI-Spezifikation
- Testen einer Anbieterintegration

Voraussetzungen

Bevor Sie die Integration als Dienstanbieter mit durchführen AWS Entity Resolution, müssen Sie die folgenden Anforderungen erfüllen.

Themen

- Einen Anbieterdienst auflisten unter AWS Data Exchange
- Identifizieren Sie Ihre Eigenschaften
- Fordern Sie die AWS Entity Resolution OpenAPI-Spezifikation an

Einen Anbieterdienst auflisten unter AWS Data Exchange

Als Drittanbieter müssen Sie Ihr Produkt im AWS Data Exchange (ADX) -Produktkatalog auflisten. Sobald Ihr Produkt im AWS Data Exchange Produktkatalog aufgeführt ist, können Abonnenten Ihr Produkt entweder über ein öffentliches oder ein privates Angebot abonnieren.

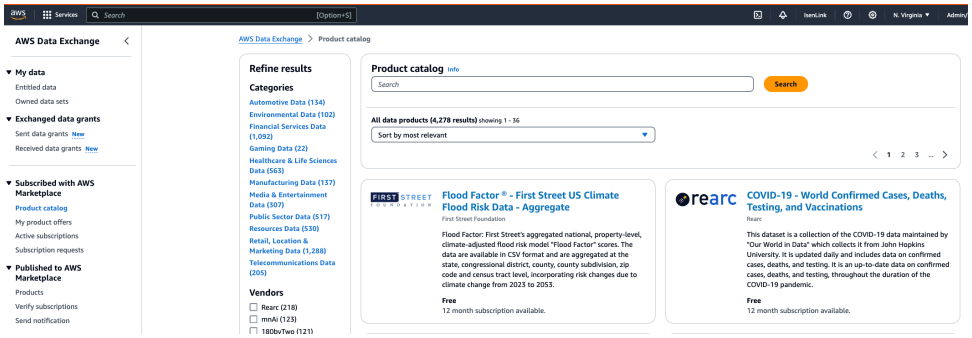
Um einen Anbieterdienst aufzulisten auf AWS Data Exchange

1. Wenn Sie ein neuer Anbieter von Datenprodukten bei sind AWS Data Exchange, führen Sie die Schritte im Abschnitt Erste Schritte als Anbieter im AWS Data Exchange Benutzerhandbuch durch.
2. Erstellen Sie einen REST-API-Datensatz und veröffentlichen Sie ein neues Produkt, das APIs On AWS Data Exchange enthält. Folgen Sie dazu den Schritten im Abschnitt So veröffentlichen Sie ein Produkt, das APIs im AWS Data Exchange Benutzerhandbuch enthalten ist. Sie können den Vorgang abschließen, indem Sie entweder die AWS Data Exchange Konsole oder die verwenden AWS Command Line Interface.

   Wenn Sie die Sichtbarkeit des Produkts auf Öffentlich festgelegt haben, steht das öffentliche Angebot allen Abonnenten zur Verfügung.

   Wenn Sie die Produktsichtbarkeit auf Privat festgelegt haben, führen Sie je nach Anwendungsfall die Schritte im Abschnitt Benutzerdefinierte Angebote erstellen im AWS Data Exchange Benutzerhandbuch aus.

   Die folgende Abbildung zeigt ein Beispiel für ein im Produktkatalog AWS Data Exchange verfügbares Produkt.



3. Sobald das Produkt im AWS Data Exchange Produktkatalog verfügbar ist, kann der Abonnent das Produkt auf folgende Weise abonnieren.

   - Abonnieren Sie das öffentliche Produkt.
   - Verwenden Sie ein privates Angebot (benutzerdefiniertes Angebot), das vom Anbieterdienst ausgestellt wurde.
   - Nutzen Sie ein BYOS-Angebot (Bring Your Own Subscription).

Weitere Informationen finden Sie unter Abonnieren und Zugreifen auf ein Produkt, das APIs im AWS Data Exchange Benutzerhandbuch enthalten ist.

Identifizieren Sie Ihre Eigenschaften

Bei den Attributen der Eingabedaten handelt es sich um die Typdefinitionen der Entitäten, die in einem Workflow aufgelöst werden sollen. Einige Beispiele für Attribute sind `FirstNameLastName`,`Email`, oder`Custom String`.

Wenn Sie Ihre Attribute identifizieren, sollten Sie alle Anforderungen oder Richtlinien beachten.

Example Beispiel

Im Folgenden finden Sie ein Beispiel für Validierungen zur Identifizierung von Anbieterattributen.

- Entweder das `LastName` Attribut `FirstName` oder ist obligatorisch.
- Wenn das `Email` Attribut vorhanden ist, muss es gehasht werden.

Als Anbieter müssen Sie die Attribute in Ihrem Anbieter-Serviceprodukt identifizieren und diese Attribute dann dem AWS Entity Resolution Business Development-Team unter `<aws-entity-resolution-bd@amazon .com>` zur weiteren Überprüfung mitteilen, bevor Sie fortfahren.

Fordern Sie die AWS Entity Resolution OpenAPI-Spezifikation an

AWS Entity Resolution hat eine OpenAPI-Spezifikation, die Sie als Anbieter als Handshake verwenden können, der die APIs an der Integration Beteiligten enthält. Weitere Informationen finden Sie unter Verwendung der AWS Entity Resolution OpenAPI-Spezifikation.

Um die OpenAPI-Definition anzufordern, wenden Sie sich an das AWS Entity Resolution Business Development Team unter `<aws-entity-resolution-bd@amazon .com>`.

Verwendung der AWS Entity Resolution OpenAPI-Spezifikation

Die OpenAPI-Spezifikation definiert alle damit verbundenen AWS Entity Resolution Protokolle. Diese Spezifikation ist notwendig, um die Integration zu implementieren.

Die OpenAPI-Definition enthält die folgenden API-Operationen:

- `POST AssignIdentities`
- `POST CreateJob`
- `GET GetJob`
- `POST StartJob`
- `POST MapIdentities`
- `GET Schema`

Um die OpenAPI-Spezifikation anzufordern, wenden Sie sich an das AWS Entity Resolution Business Development Team unter `<aws-entity-resolution-bd@amazon .com>`.

Die OpenAPI-Spezifikation unterstützt zwei Arten von Integrationen sowohl für die Kodierung als auch für die Transcodierung von Verbraucher-Identifikatoren: Batch-Verarbeitung und synchrone Verarbeitung. Nachdem Sie die OpenAPI-Spezifikation erhalten haben, implementieren Sie die Art der Verarbeitungsintegration für Ihren Anwendungsfall.

Themen

- Integration der Stapelverarbeitung
- Integration der synchronen Verarbeitung

Integration der Stapelverarbeitung

Die Integration der Stapelverarbeitung folgt einem asynchronen Entwurfsmuster. Nachdem ein Workflow initiiert wurde AWS Data Exchange, sendet er einen Job über einen Endpunkt der Anbieterintegration. Anschließend wartet der Workflow, bis dieser Job abgeschlossen ist, indem er regelmäßig den Auftragsstatus abfragt. Diese Lösung ist für Auftragsausführungen, die möglicherweise länger dauern und einen geringeren Anbieterdurchsatz haben, wünschenswerter. Der Anbieter nimmt den Speicherort des Datensatzes als Amazon S3 S3-Link auf, den er selbst verarbeiten und die Ergebnisse an einen vordefinierten S3-Ausgabeort schreiben kann.

Die Integration der Stapelverarbeitung wird mithilfe von drei API-Definitionen aktiviert. AWS Entity Resolution ruft den Provider-Endpunkt auf, der AWS Data Exchange in der folgenden Reihenfolge verfügbar ist:

1. `POST CreateJob`: Bei diesem API-Vorgang werden die Auftragsinformationen zur Verarbeitung an den Anbieter übermittelt. Diese Informationen beziehen sich auf die Art des Auftrags: Kodierung

oder Transcodierung, S3-Standorte, vom Kunden bereitgestelltes Schema und alle zusätzlichen erforderlichen Auftragseigenschaften.

Diese API gibt a zurück`JobId`, und der Status für den Job ist einer der folgenden: `PENDINGREADY`,`IN_PROGRESS`,`COMPLETE`, oder`FAILED`.

Beispielanforderung für die Kodierung

```
POST /jobs
{
  "actionType": "ID_ASSIGNMENT",
  "s3SourceLocation": "string",
  "s3TargetLocation": "string",
  "jobProperties": {
    "assignmentJobProperties": {
      "fieldMappings": [
        {
          "name": "string",
          "type": "NAME"
        }
      ]
    }
  },
  "customerSpecifiedJobProperties": {
    "property1": "string",
    "property2": "string"
  },
  "outputSourceConfiguration": {
    "KMSArn": "string"
  }
}
```

Beispielantwort

```
{
  "jobId": "string",
  "status": "PENDING"
}
```

2. `POST StartJob`: Diese API teilt dem Anbieter mit, dass er den Job auf der Grundlage der `JobId` bereitgestellten API starten soll. Auf diese Weise kann der Anbieter alle erforderlichen Validierungen von bis `CreateJob` durchführen. `StartJob`

Diese API gibt a`JobId`, das `Status` für den `JobstatusMessage`, das und zurück`statusCode`.

Beispielanforderung für die Kodierung

```
POST/jobs/{jobId}
{
  "customerSpecifiedJobProperties": {
    "property1": "string",
    "property2": "string"
  }
}
```

Beispielantwort

```
{
  "jobId": "string",
  "status": "PENDING",
  "statusMessage": "string",
  "statusCode": 200
}
```

3. `GET GetJob`: Diese API informiert darüber AWS Entity Resolution , ob der Job abgeschlossen wurde oder ob ein anderer Status vorliegt.

   Diese API gibt a`JobId`, das `Status` für den `JobstatusMessage`, das und zurück`statusCode`.

   Beispielanforderung für die Kodierung

   ```
   GET /jobs/{jobId}
   ```

   Beispielantwort

   ```
   {
     "jobId": "string",
     "status": "PENDING",
     "statusMessage": "string",
     "statusCode": 200
   }
   ```

Die vollständige Definition davon APIs ist in der AWS Entity Resolution OpenAPI-Spezifikation enthalten.

Integration der synchronen Verarbeitung

Die Lösung für die synchrone Verarbeitung ist für Anbieter, die eine Reaktionszeit nahezu in Echtzeit mit Reaktionszeit in Echtzeit mit höherem Durchsatz und höherem TPS haben, wünschenswerter. Dieser AWS Entity Resolution Workflow partitioniert den Datensatz und stellt mehrere API-Anfragen parallel. Der AWS Entity Resolution Workflow übernimmt dann das Schreiben der Ergebnisse an den gewünschten Ausgabespeicherort.

Dieser Prozess wird mithilfe einer der API-Definitionen aktiviert. AWS Entity Resolution ruft den Provider-Endpunkt auf, der verfügbar ist über AWS Data Exchange:

`POST AssignIdentities`: Diese API sendet Daten mithilfe einer `source_id` Kennung an den Anbieter, die mit diesem Datensatz `recordFields` verknüpft sind.

Diese API gibt die zurück`assignedRecords`.

Beispielanforderung für die Kodierung

```
POST /assignment
{
  "sourceRecords": [
    {
      "sourceId": "string",
      "recordFields": [
        {
          "name": "string",
          "type": "NAME",
          "value": "string"
        }
      ]
    }
  ]
}
```

Beispielantwort

```
{
  "assignedRecords": [
    {
```

```
      "sourceRecord": {
        "sourceId": "string",
        "recordFields": [
          {
            "name": "string",
            "type": "NAME",
            "value": "string"
          }
        ]
      },
      "identity": any
    }
  ]
}
```

Die vollständige Definition davon APIs ist in der AWS Entity Resolution OpenAPI-Spezifikation enthalten.

Je nachdem, welchen Ansatz der Anbieter AWS Entity Resolution wählt, erstellt der Anbieter dafür eine Konfiguration, die für die Initiierung der Kodierung oder Transcodierung verwendet wird. Darüber hinaus stehen diese Konfigurationen den Kunden zur Verfügung, die die APIs bereitgestellten AWS Entity Resolution Optionen verwenden.

Auf diese Konfiguration kann über einen Amazon-Ressourcennamen (ARN) zugegriffen werden, der sich daraus ergibt, wo das Anbieter-Serviceangebot gehostet AWS Data Exchange wird, und vom Typ des Anbieterdienstes. AWS Entity Resolution bezeichnet diesen ARN als`providerServiceARN`.

Testen einer Anbieterintegration

Eine Anbieterintegration AWS Entity Resolution hostet zwar Dienste für den Datenabgleich, ist jedoch eine wichtige Drittanbieterkomponente für den end-to-end Abgleichs-Workflow. Für die Anbieter wurden mehrere Tests definiert, AWS Entity Resolution die zusätzliche Sicherheitsvorkehrungen für den Fall bieten, dass diese Integration fehlschlägt. Dieser Ansatz bietet Anbietern die Möglichkeit, ihren Dienststatus anhand dieser end-to-end Testfälle zu überwachen.

Anbieter können ihre Testkonten und ihre eigenen Daten verwenden, um diese end-to-end Testfälle mithilfe des AWS Entity Resolution Software Development Kit (SDK) auszuführen. Wenn es Probleme von Anbietern gibt, AWS Entity Resolution verwendet es den bevorzugten Eskalationspfad, um das Problem zu eskalieren. Darüber hinaus müssen die Anbieter ihre eigene Überwachung der

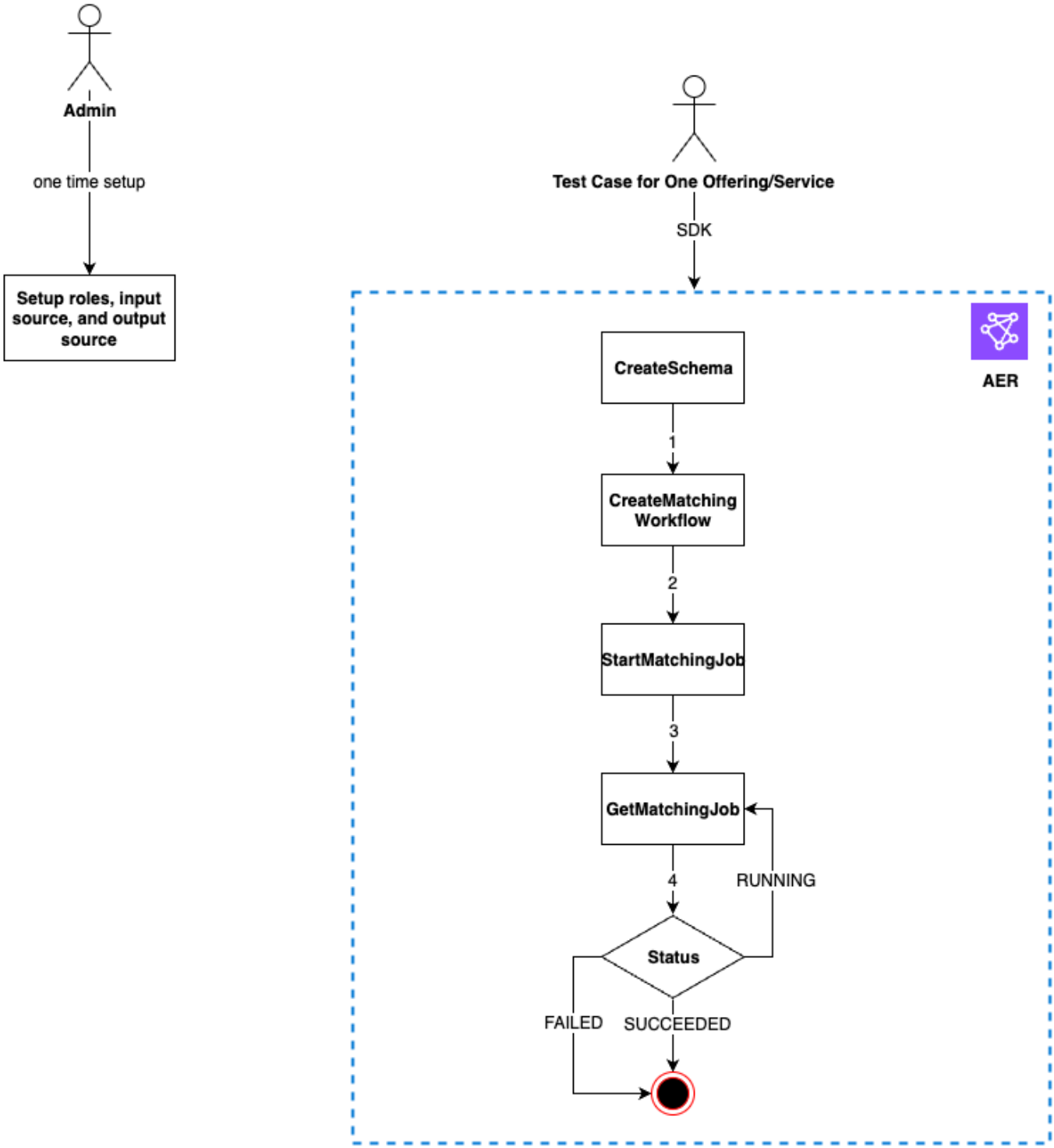
Testergebnisse einrichten. Die Anbieter müssen ihre Daten, die für AWS-Konto IDs die Durchführung dieser Tests verwendet werden, mit anderen teilen AWS Entity Resolution.

Eine erfolgreiche Ausführung bedeutet, dass ein Anbieter seine Daten einrichten und seinen eigenen Service nutzen kann und der Auftragsstatus ohne Fehler als Abgeschlossen zurückgegeben wird. AWS Entity Resolution Dies kann programmgesteuert mit dem APIs bereitgestellten Befehl von erreicht werden. AWS Entity Resolution

Anbieter können beispielsweise ihren S3-Bucket, ihre Eingabequelle, ihre Rollen, ihr Schema und ihre Workflows entsprechend ihren Diensten einrichten. Nachdem diese Einstellungen abgeschlossen sind, können Anbieter diese Workflows einmal täglich mit 200 Datensätzen ausführen, um ihren Service zu testen. Bei diesem Ansatz verwenden Anbieter das SDK ihrer Wahl und führen einen end-to-end Test für ihre Dienste durch, die AWS Data Exchange über ihre Testkonten angeboten werden. Von den Anbietern wird erwartet, dass sie diese Tests für jedes ihrer Angebote oder Dienste durchführen.

> **Note**
>
> Anbieter müssen AWS Entity Resolution die AWS-Konto ID (mit der sie `accountId`) diese Workflows ausführen) zu Testzwecken angeben. Darüber hinaus müssen die Anbieter diese Tests überwachen und sicherstellen, dass sie erfolgreich sind. Das bedeutet, dass die Anbieter die Benachrichtigung bei Ausfällen aktivieren und das Problem entsprechend beheben müssen.

Das folgende Diagramm zeigt einen typischen end-to-end Workflow-Testfall.



Um eine Anbieterintegration zu testen

1. (Einmaliges Setup) Richten Sie Ressourcen für ein, AWS Entity Resolution indem Sie die Verfahren unter befolgenEinrichten AWS Entity Resolution.

Nachdem Sie die einmaligen Einrichtungsverfahren abgeschlossen haben, sollten Sie Ihre Rollen, Daten und Datenquellen bereit haben. Sie sind jetzt bereit, die Anbieterintegration entweder mit der AWS Entity Resolution Konsole oder zu testen APIs.

2. Testen Sie die Anbieterintegration entweder mit der AWS Entity Resolution APIs Oder-Konsole.

API

Um eine Anbieterintegration mit dem zu testen AWS Entity Resolution APIs

1. Erstellen Sie eine Schemazuordnung mithilfe der CreateSchemaMapping API. Eine vollständige Liste der unterstützten Programmiersprachen finden Sie im Abschnitt „Siehe auch“ der CreateSchemaMapping API.

   Schema-Mapping ist der Prozess, mit dem Sie festlegen, AWS Entity Resolution wie Ihre Daten für den Abgleich zu interpretieren sind. Sie definieren das Schema der Eingabedatentabelle, die AWS Entity Resolution in einen passenden Workflow einlesen soll.

   Bei der Erstellung einer Schemazuordnung muss jeder Zeile mit Eingabedaten, die AWS Entity Resolution liest, ein eindeutiger Bezeichner zugewiesen werden. Zum Beispiel: `Primary_key`, `Row_ID`, `Record_ID`.

   Example Erstellen einer Schemazuordnung für eine Datenquelle, die **`id`** und enthält **`email`**

   Im Folgenden finden Sie ein Beispiel für eine Schemazuordnung für eine Datenquelle, die `id` und enthält`email`:

```
[
  {
    "fieldName": "id",
    "type": "UNIQUE_ID"
  },
  {
    "fieldName": "email",
    "type": "EMAIL_ADDRESS"
  }
]
```

Example Erstellen einer Schemazuordnung für eine Datenquelle, die Java **`email`** SDK enthält **`id`** und verwendet

Im Folgenden finden Sie ein Beispiel für eine Schemazuordnung für eine Datenquelle, die das Java-SDK enthält `id` und `email` verwendet:

```
EntityResolutionClient.createSchemaMapping(
            CreateSchemaMappingRequest.builder()
                                      .schemaName(<schema-name>)
                                      .mappedInputFields([

 SchemaInputAttribute.builder().fieldName("id").type("UNIQUE_ID").build(),

 SchemaInputAttribute.builder().fieldName("email").type("EMAIL_ADDRESS").build()
                                       ])
                                      .build()

)
```

2. Erstellen Sie mithilfe der CreateMatchingWorkflow API einen passenden Workflow. Eine vollständige Liste der unterstützten Programmiersprachen finden Sie im Abschnitt „Siehe auch“ der CreateMatchingWorkflow API.

   Example Einen passenden Workflow mit dem Java SDK erstellen

   Im Folgenden finden Sie ein Beispiel für einen passenden Workflow unter Verwendung des Java-SDK:

```
EntityResolutionClient.createMatchingWorkflow(
            CreateMatchingWorkflowRequest.builder()
                                         .workflowName(<workflow-name>)
                                         .inputSourceConfig(

 InputSource.builder().inputSourceARN(<glue-inputsource-from-
step1>).schemaName(<schema-name-from-step2>).build()
                                         )

 .outputSourceConfig(OutputSource.builder().outputS3Path(<output-s3-
path>).output(<output-1>, <output-2>, <output-3>).build())

 .resolutionTechniques(ResolutionTechniques.builder()
```

```
   .resolutionType(PROVIDER)

   .providerProperties(ProviderProperties.builder()

                                          .providerServiceArn(<provider-arn>)

                                           .providerConfiguration(<configuration-
depending-on-service>)


 .intermediateSourceConfiguration(<intermedaite-s3-path>)

                                          .build())

   .build()
                                          .roleArn(<role-from-step1>)
                                          .build()

)
```

Nachdem der passende Workflow eingerichtet wurde, können Sie einen Workflow ausführen.

3. Führen Sie mithilfe der StartMatchingJob API einen passenden Workflow aus. Um einen passenden Workflow auszuführen, müssen Sie mithilfe des `CreateMatchingWorkflow` Endpunkts einen passenden Workflow erstellt haben.

   Eine vollständige Liste der unterstützten Programmiersprachen finden Sie im Abschnitt „Siehe auch“ der StartMatchingJob API.

   Example Einen passenden Workflow mit dem Java SDK ausführen

   Im Folgenden finden Sie ein Beispiel für einen laufenden Matching-Workflow mit dem Java-SDK:

   ```
   EntityResolutionClient.startMatchingJob(StartMatchingJobRequest.builder()
                   .workflowName(<name-of-workflow-from-step3)
                   .build()
   )
   ```

4. Überwachen Sie den Status eines Workflows mithilfe der GetMatchingJob API.

Diese API gibt den Status, die Metriken und Fehler (falls vorhanden) zurück, die mit einem Job verknüpft sind.

ExampleÜberwachung eines passenden Workflows mithilfe des Java SDK

Im Folgenden finden Sie ein Beispiel für die Überwachung eines passenden Workflow-Jobs mithilfe des Java-SDK:

```
EntityResolutionClient.getMatchingJob(GetMatchingJobRequest.builder()
                .workflowName(<name-of-workflow-from-step3)
                .jobId(jobId-from-startMatchingJob)
                .build()
)
```

Der end-to-end Test ist abgeschlossen, wenn der Workflow erfolgreich abgeschlossen wurde.

Console

Um eine Anbieterintegration mit der AWS Entity Resolution Konsole zu testen

1. Erstellen Sie eine Schemazuordnung, indem Sie die Schritte unter befolgenEine Schemazuordnung erstellen.

   Bei der Schemazuordnung legen Sie fest, AWS Entity Resolution wie Ihre Daten für den Abgleich zu interpretieren sind. Sie definieren das Schema der Eingabedatentabelle, die Sie in einen Abgleichs-Workflow einlesen möchten AWS Entity Resolution .

   Bei der Erstellung einer Schemazuordnung muss jeder Zeile mit Eingabedaten, die AWS Entity Resolution gelesen werden, ein eindeutiger Bezeichner zugewiesen werden. Zum Beispiel: `Primary_key`, `Row_ID`, `Record_ID`.

   Example Schemazuweisung für eine Datenquelle, die **`id`** und enthält **`email`**

   Im Folgenden finden Sie ein Beispiel für eine Schemazuordnung für eine Datenquelle, die `id` und enthält`email`:

   ```
   [
     {
       "fieldName": "id",
   ```

```
    "type": "UNIQUE_ID"
  },
  {
    "fieldName": "email",
    "type": "EMAIL_ADDRESS"
  }
]
```

2. Folgen Sie den Schritten unter, um einen passenden Workflow zu erstellen und auszuführenErstellen eines auf dem Provider-Service basierenden Matching-Workflows.

   Das Erstellen eines Abgleichsworkflows ist der Prozess, den Sie einrichten, um anzugeben, welche Eingabedaten miteinander abgeglichen werden sollen und wie der Abgleich durchgeführt werden soll. Im anbieterbasierten Workflow können Sie, wenn für ein Konto ein Abonnement bei einem Dienstanbieter AWS Data Exchange besteht, Ihre bekannten Kennungen Ihrem bevorzugten Anbieter zuordnen. Je nachdem, welchen Anbieter und welchen Dienst Sie für die Durchführung eines End-to-End-Tests verwenden, können Sie Ihren Matching-Workflow entsprechend konfigurieren.

   Die AWS Entity Resolution Konsole kombiniert die Aktionen „Erstellen“ und „Ausführen“ in einer einzigen Schaltfläche. Nachdem Sie Erstellen und ausführen ausgewählt haben, wird eine Meldung angezeigt, die darauf hinweist, dass der entsprechende Workflow erstellt und der Job gestartet wurde.

3. Überwachen Sie den Status des Workflows auf der Seite Passende Workflows.

   Der end-to-end Test ist abgeschlossen, wenn der Workflow erfolgreich abgeschlossen wurde (Jobstatus ist Abgeschlossen).

   Auf der Registerkarte „Metriken“ der entsprechenden Workflow-Detailseite können Sie unter „Letzte Job-Metriken“ Folgendes einsehen:

   - Die Job-ID.
   - Der Status des passenden Workflow-Jobs: In Warteschlange, In Bearbeitung, Abgeschlossen, Fehlgeschlagen
   - Die Zeit, in der der Workflow-Job abgeschlossen wurde.
   - Die Anzahl der verarbeiteten Datensätze.
   - Die Anzahl der nicht verarbeiteten Datensätze.
   - Das IDs generierte eindeutige Match.

- Die Anzahl der Eingabedatensätze.

Sie können auch die Job-Metriken für übereinstimmende Workflow-Jobs, die zuvor ausgeführt wurden, unter dem Jobverlauf anzeigen.

Sicherheit in AWS Entity Resolution

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS-Services in der läuft AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Entity Resolution, finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS-Service , was Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung anwenden können AWS Entity Resolution. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Entity Resolution , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere verwenden können AWS-Services , die Ihnen bei der Überwachung und Sicherung Ihrer AWS Entity Resolution Ressourcen helfen.

Topics

- Datenschutz in AWS Entity Resolution
- Identitäts- und Zugriffsmanagement für AWS Entity Resolution
- Konformitätsüberprüfung für AWS Entity Resolution
- Resilienz in AWS Entity Resolution

Datenschutz in AWS Entity Resolution

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in AWS Entity Resolution. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz . Informationen zum Datenschutz in Europa finden Sie im General Data Protection Regulation (GDPR) Center.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API AWS Entity Resolution oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung im Ruhezustand für AWS Entity Resolution

AWS Entity Resolution bietet standardmäßig Verschlüsselung zum Schutz vertraulicher Kundendaten im Speicher mithilfe AWS eigener Verschlüsselungsschlüssel.

AWS-eigene Schlüssel — AWS Entity Resolution verwendet diese Schlüssel standardmäßig, um persönlich identifizierbare Daten automatisch zu verschlüsseln. Sie können AWS -eigene Schlüssel weder anzeigen noch verwalten oder verwenden und auch nicht ihre Nutzung prüfen. Sie müssen jedoch keine Maßnahmen ergreifen, um die Schlüssel zu schützen, mit denen Ihre Daten verschlüsselt werden. Weitere Informationen finden Sie unter AWS-eigene Schlüssel im AWS Key Management Service Entwicklerhandbuch.

Die standardmäßige Verschlüsselung von Daten im Ruhezustand trägt dazu bei, den betrieblichen Aufwand und die Komplexität zu reduzieren, die mit dem Schutz vertraulicher Daten verbunden sind. Gleichzeitig können Sie damit sichere Anwendungen erstellen, die strenge Verschlüsselungsvorschriften und regulatorische Anforderungen erfüllen.

Alternativ können Sie auch einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung angeben, wenn Sie Ihre passende Workflow-Ressource erstellen.

Vom Kunden verwaltete Schlüssel — AWS Entity Resolution unterstützt die Verwendung eines symmetrischen, vom Kunden verwalteten KMS-Schlüssels, den Sie selbst erstellen, besitzen und verwalten, um die Verschlüsselung Ihrer vertraulichen Daten zu ermöglichen. Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie beispielsweise folgende Aufgaben ausführen:

- Festlegung und Pflege wichtiger Richtlinien
- Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
- Aktivieren und Deaktivieren wichtiger Richtlinien
- Kryptographisches Material mit rotierendem Schlüssel
- Hinzufügen von -Tags
- Erstellen von Schlüsselaliasen
- Schlüssel für das Löschen von Schlüsseln planen

Weitere Informationen finden Sie unter vom Kunden verwalteter Schlüssel im AWS Key Management Service Entwicklerhandbuch.

Weitere Informationen AWS KMS dazu finden Sie unter Was ist AWS Key Management Service?

Schlüsselverwaltung

Wie AWS Entity Resolution verwendet Zuschüsse in AWS KMS

AWS Entity Resolution erfordert einen Zuschuss, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können. Wenn Sie einen passenden Workflow erstellen, der mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, AWS Entity Resolution erstellt in Ihrem Namen einen Zuschuss, indem es eine CreateGrantAnfrage an sendet AWS KMS. Grants in AWS KMS werden verwendet, um AWS Entity Resolution Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren. AWS Entity Resolution setzt voraus, dass der Zuschuss Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwendet:

- Senden Sie GenerateDataKeyAnfragen AWS KMS zur Generierung von Datenschlüsseln, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt sind.
- Senden Sie Entschlüsselungsanfragen an AWS KMS , um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie zur Verschlüsselung Ihrer Daten verwendet werden können.

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn Sie dies tun, können Sie auf AWS Entity Resolution keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise den Dienstzugriff auf Ihren Schlüssel durch die Gewährung entfernen und versuchen, einen Job für einen passenden Workflow zu starten, der mit einem Kundenschlüssel verschlüsselt ist, würde der Vorgang einen `AccessDeniedException` Fehler zurückgeben.

Einen vom Kunden verwalteten Schlüssel erstellen

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel mithilfe der AWS-Managementkonsole AWS KMS APIs oder erstellen.

Einen symmetrischen kundenverwalteten Schlüssel erstellen

AWS Entity Resolution unterstützt die Verschlüsselung mit symmetrischen KMS-Schlüsseln. Folgen Sie den Schritten zum Erstellen eines symmetrischen kundenverwalteten Schlüssels im Entwicklerhandbuch zum AWS Key Management Service .

Wichtige Richtlinienerklärung

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren kundenseitig verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Verwaltung des Zugriffs auf vom Kunden verwaltete Schlüssel im AWS Key Management Service Entwicklerhandbuch.

Um Ihren vom Kunden verwalteten Schlüssel mit Ihren AWS Entity Resolution Ressourcen zu verwenden, müssen die folgenden API-Operationen in der Schlüsselrichtlinie zulässig sein:

- `kms:DescribeKey`— Stellt Informationen wie den Schlüssel-ARN, das Erstellungsdatum (und gegebenenfalls das Löschdatum), den Schlüsselstatus sowie das Herkunfts- und Ablaufdatum (falls vorhanden) des Schlüsselmaterials bereit. Es enthält Felder wie, die Ihnen helfen`KeySpec`, verschiedene Arten von KMS-Schlüsseln zu unterscheiden. Außerdem werden die Schlüsselverwendung (Verschlüsselung, Signierung oder Generierung und Überprüfung von MACs) und die Algorithmen angezeigt, die der KMS-Schlüssel unterstützt. AWS Entity Resolution bestätigt, dass das `KeySpec` ist und ist`SYMMETRIC_DEFAULT`. `KeyUsage` `ENCRYPT_DECRYPT`
- `kms:CreateGrant`: Fügt einem kundenverwalteten Schlüssel eine Erteilung hinzu. Gewährt Kontrollzugriff auf einen bestimmten KMS-Schlüssel, der den Zugriff für Grant-Operationen AWS Entity Resolution erfordert. Weitere Informationen zum Verwenden von Zuweisungen finden Sie im Entwicklerhandbuch für AWS Key Management Service .

Auf diese Weise können AWS Entity Resolution Sie Folgendes tun:

- `GenerateDataKey` aufrufen, um einen verschlüsselten Datenschlüssel zu generieren und zu speichern, da der Datenschlüssel nicht sofort zum Verschlüsseln verwendet wird.
- `Decrypt` aufrufen, um den gespeicherten verschlüsselten Datenschlüssel für den Zugriff auf verschlüsselte Daten zu verwenden.
- Einen Prinzipal für die Außerbetriebnahme einrichten, damit der Service in den Status `RetireGrant` wechseln kann.

Im Folgenden finden Sie Beispiele für Richtlinienerklärungen, die Sie hinzufügen können 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"
        }
      }
}
```

Berechtigungen für Benutzer

Wenn Sie einen KMS-Schlüssel als Standardschlüssel für die Verschlüsselung konfigurieren, ermöglicht die standardmäßige KMS-Schlüsselrichtlinie jedem Benutzer mit Zugriff auf die erforderlichen KMS-Aktionen, diesen KMS-Schlüssel zum Verschlüsseln oder Entschlüsseln von Ressourcen zu verwenden. Sie müssen Benutzern die Erlaubnis erteilen, die folgenden Aktionen aufzurufen, um die vom Kunden verwaltete KMS-Schlüsselverschlüsselung verwenden zu können:

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

Während einer `CreateMatchingWorkflow`Anfrage AWS Entity Resolution sendet ich in Ihrem Namen eine CreateGrantAnfrage DescribeKeyund eine Anfrage AWS KMS an. Dies setzt voraus, dass die IAM-Entität, die die `CreateMatchingWorkflow` Anfrage mit einem vom Kunden verwalteten KMS-Schlüssel stellt, über die `kms:DescribeKey` Berechtigungen für die KMS-Schlüsselrichtlinie verfügt.

Während einer `CreateIdMappingWorkflowStartIdMappingJob`AND-Anfrage AWS Entity Resolution sendet er in Ihrem Namen eine DescribeKeyund eine CreateGrantAnfrage AWS KMS an. Dies setzt voraus, dass die IAM-Entität, die die `CreateIdMappingWorkflow` und die `StartIdMappingJob` Anfrage mit einem vom Kunden verwalteten KMS-Schlüssel stellt, über die `kms:DescribeKey` Berechtigungen für die KMS-Schlüsselrichtlinie verfügt. Anbieter können auf den vom Kunden verwalteten Schlüssel zugreifen, um die Daten im AWS Entity Resolution Amazon S3 S3-Bucket zu entschlüsseln.

Im Folgenden finden Sie Beispiele für Richtlinienerklärungen, die Sie für Anbieter hinzufügen können, um die Daten im AWS Entity Resolution Amazon S3 S3-Bucket zu entschlüsseln:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::715724997226:root"
        },
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id",
        "Condition": {
            "StringEquals": {
            "kms:ViaService": "s3.us-east-1.amazonaws.com"
            }
        }
    }]
}
```

Ersetzen Sie jeden *<user input placeholder>* durch Ihre Informationen.

<KMSKeyARN>	AWS KMS Name der Amazon-Ressource.

Ebenso muss die IAM-Entität, die die `StartMatchingJob`API aufruft, über `kms:GenerateDataKey` Berechtigungen für den vom Kunden verwalteten KMS-Schlüssel verfügen`kms:Decrypt`, der im entsprechenden Workflow bereitgestellt wird.

Weitere Informationen zur Angabe von Berechtigungen in einer Richtlinie finden Sie im AWS Key Management Service Entwicklerhandbuch.

Weitere Informationen zur Problembehandlung beim Zugriff auf Schlüssel finden Sie im AWS Key Management Service Entwicklerhandbuch.

Angabe eines vom Kunden verwalteten Schlüssels für AWS Entity Resolution

Sie können einen vom Kunden verwalteten Schlüssel als zweite Verschlüsselungsebene für die folgenden Ressourcen festlegen:

Abgleichender Workflow — Wenn Sie eine passende Workflow-Ressource erstellen, können Sie den Datenschlüssel angeben, indem Sie einen KMSarn eingeben, der zur Verschlüsselung der von der Ressource gespeicherten identifizierbaren persönlichen Daten AWS Entity Resolution verwendet wird.

kmSARN — Geben Sie einen Schlüssel-ARN ein, der eine Schlüssel-ID für einen vom AWS KMS Kunden verwalteten Schlüssel ist.

Sie können einen vom Kunden verwalteten Schlüssel als zweite Verschlüsselungsebene für die folgenden Ressourcen angeben, wenn Sie einen ID-Zuordnungs-Workflow für zwei Ressourcen erstellen oder ausführen: AWS-Konten

ID-Zuordnungs-Workflow oder ID-Zuordnungs-Workflow starten — Wenn Sie eine Workflow-Ressource für die ID-Zuordnung erstellen oder einen Workflow-Job für die ID-Zuordnung starten, können Sie den Datenschlüssel angeben, indem Sie einen KMSarn eingeben, der zur Verschlüsselung der von der Ressource gespeicherten identifizierbaren personenbezogenen Daten AWS Entity Resolution verwendet wird.

kmSARN — Geben Sie einen Schlüssel-ARN ein, der eine Schlüssel-ID für einen vom AWS KMS Kunden verwalteten Schlüssel ist.

Überwachen Sie Ihre Verschlüsselungsschlüssel für AWS Entity Resolution Service

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel mit Ihren AWS Entity Resolution Serviceressourcen verwenden, können Sie AWS CloudTrail oder Amazon CloudWatch Logs verwenden, um Anfragen zu verfolgen, die AWS Entity Resolution an gesendet AWS KMS werden.

Die folgenden Beispiele sind AWS CloudTrail Ereignisse für`CreateGrant`,`GenerateDataKey`, und zur Überwachung von AWS KMS Vorgängen`Decrypt`, `DescribeKey` die aufgerufen werden, AWS Entity Resolution um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden:

Themen

- CreateGrant
- DescribeKey
- GenerateDataKey
- Decrypt

CreateGrant

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel verwenden, um Ihre passende Workflow-Ressource zu verschlüsseln, AWS Entity Resolution sendet in Ihrem Namen eine `CreateGrant` Anfrage für den Zugriff auf den KMS-Schlüssel in Ihrem AWS-Konto. Die gewährten Zuschüsse AWS Entity Resolution sind spezifisch für die Ressource, die dem vom AWS KMS Kunden verwalteten Schlüssel zugeordnet ist. AWS Entity Resolution Verwendet außerdem den `RetireGrant` Vorgang, um einen Zuschuss zu entfernen, wenn Sie eine Ressource löschen.

Das folgende Beispielereignis zeichnet den Vorgang `CreateGrant` auf:

```
{
    "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 verwendet den `DescribeKey` Vorgang, um zu überprüfen, ob der vom AWS KMS Kunden verwaltete Schlüssel, der Ihrer entsprechenden Ressource zugeordnet ist, im Konto und in der Region vorhanden ist.

Das folgende Beispielereignis zeichnet die `DescribeKey`-Operation auf:

```
{
    "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

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel für Ihre passende Workflow-Ressource aktivieren, AWS Entity Resolution sendet eine `GenerateDataKey` Anfrage über Amazon Simple Storage Service (Amazon S3) an AWS KMS , in der der vom AWS KMS Kunden verwaltete Schlüssel für die Ressource angegeben ist.

Das folgende Beispielereignis zeichnet die `GenerateDataKey`-Operation auf:

```
{
    "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

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel für Ihre passende Workflow-Ressource aktivieren, AWS Entity Resolution sendet eine `Decrypt` Anfrage über Amazon Simple Storage Service (Amazon S3) an AWS KMS , in der der vom AWS KMS Kunden verwaltete Schlüssel für die Ressource angegeben ist.

Das folgende Beispielereignis zeichnet die `Decrypt`-Operation auf:

```
{
    "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"
}
```


Überlegungen

AWS Entity Resolution unterstützt nicht die Aktualisierung eines passenden Workflows mit einem neuen kundenverwalteten KMS-Schlüssel. In solchen Fällen können Sie einen neuen Workflow mit dem vom Kunden verwalteten KMS-Schlüssel erstellen.

Weitere Informationen

Die folgenden Ressourcen enthalten weitere Informationen zur Datenverschlüsselung im Ruhezustand:

Weitere Informationen zu den Grundkonzepten von AWS Key Management Service finden Sie im AWS Key Management Service Developer Guide.

Weitere Informationen zu bewährten Sicherheitsmethoden für AWS Key Management Service finden Sie im AWS Key Management Service Developer Guide.

Zugriff AWS Entity Resolution über einen Schnittstellenendpunkt (AWS PrivateLink)

Sie können AWS PrivateLink damit eine private Verbindung zwischen Ihrer VPC und AWS Entity Resolution herstellen. Sie können darauf zugreifen, AWS Entity Resolution als ob es in Ihrer VPC wäre, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder Direct Connect eine Verbindung zu verwenden. Instances in Ihrer VPC benötigen für den Zugriff AWS Entity Resolution keine öffentlichen IP-Adressen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Hierbei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Eingangspunkt für den Datenverkehr dienen, der für AWS Entity Resolution bestimmt ist.

Weitere Informationen finden Sie AWS PrivateLink im AWS PrivateLink Leitfaden unter Zugriff AWS-Services durch.

Überlegungen zu AWS Entity Resolution

Bevor Sie einen Schnittstellen-Endpunkt für einrichten AWS Entity Resolution, lesen Sie die Überlegungen im AWS PrivateLink Handbuch.

AWS Entity Resolution unterstützt Aufrufe aller API-Aktionen über den Schnittstellenendpunkt.

VPC-Endpunktrichtlinien werden unterstützt für AWS Entity Resolution. Standardmäßig AWS Entity Resolution ist der vollständige Zugriff auf über den Schnittstellenendpunkt zulässig. Alternativ können Sie den Endpunkt-Netzwerkschnittstellen eine Sicherheitsgruppe zuordnen, um den Datenverkehr AWS Entity Resolution über den Schnittstellenendpunkt zu kontrollieren.

Erstellen Sie einen Schnittstellenendpunkt für AWS Entity Resolution

Sie können einen Schnittstellenendpunkt für die AWS Entity Resolution Verwendung entweder der Amazon VPC-Konsole oder der AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink - Leitfaden.

Erstellen Sie einen Schnittstellenendpunkt für die AWS Entity Resolution Verwendung des folgenden Servicenamens:

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

AWS Entity Resolution unterstützt auch einen FIPS-konformen Endpunkt (Federal Information Processing Standard). Verwenden Sie den folgenden Dienstnamen, um den FIPS-Endpunkt zu verwenden:

```
com.amazonaws.region.entityresolution-fips
```

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anfragen an die AWS Entity Resolution Verwendung des standardmäßigen regionalen DNS-Namens stellen. Beispiel, `entityresolution.us-east-1.amazonaws.com`.

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-Endpunkt anfügen können. Die standardmäßige Endpunktrichtlinie ermöglicht den vollen Zugriff AWS Entity Resolution über den Schnittstellenendpunkt. Um den Zugriff AWS Entity Resolution von Ihrer VPC aus zu kontrollieren, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen).
- Aktionen, die ausgeführt werden können
- Die Ressourcen, auf denen die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Beispiel: VPC-Endpunktrichtlinie für Aktionen AWS Entity Resolution

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellenendpunkt anhängen, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten AWS Entity Resolution Aktionen.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
```

```
            "Action": [
               "entityresolution:CreateMatchingWorkflow",
               "entityresolution:StartMatchingJob",
               "entityresolution:GetMatchingJob"
            ],
            "Resource":"*"
         }
      ]
}
```

Identitäts- und Zugriffsmanagement für AWS Entity Resolution

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Entity Resolution IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

> **Note**
>
> AWS Entity Resolution unterstützt kontoübergreifende Richtlinien. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie AWS Entity Resolution funktioniert mit IAM
- Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution
- AWS verwaltete Richtlinien für AWS Entity Resolution
- Problembehandlung bei AWS Entity Resolution Identität und Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Problembehandlung bei AWS Entity Resolution Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe Wie AWS Entity Resolution funktioniert mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen

aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.

- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

Wie AWS Entity Resolution funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren AWS Entity Resolution, mit welchen IAM-Funktionen Sie arbeiten können. AWS Entity Resolution

IAM-Funktionen, die Sie mit verwenden können AWS Entity Resolution

IAM-Feature	AWS Entity Resolution Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein

IAM-Feature	AWS Entity Resolution Unterstützung
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie AWS Entity Resolution und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für AWS Entity Resolution

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Beispiele für AWS Entity Resolution identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Ressourcenbasierte Richtlinien finden Sie in AWS Entity Resolution

Unterstützt ressourcenbasierte Richtlinien: Ja

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS Entity Resolution

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der AWS Entity Resolution Aktionen finden Sie unter Definierte Aktionen von AWS Entity Resolution in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Entity Resolution verwendet:

```
entityresolution
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
```

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

Beispiele für AWS Entity Resolution identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Politische Ressourcen für AWS Entity Resolution

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der AWS Entity Resolution Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Resources Defined by AWS Entity Resolution in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Entity Resolution definierte Aktionen.

Beispiele für AWS Entity Resolution identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Bedingungsschlüssel für Richtlinien für AWS Entity Resolution

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der AWS Entity Resolution Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Entity Resolution in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Definierte Aktionen von AWS Entity Resolution.

Beispiele für AWS Entity Resolution identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

ACLs in AWS Entity Resolution

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS Entity Resolution

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS Entity Resolution

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Zugriffssitzungen weiterleiten für AWS Entity Resolution

Unterstützt Forward Access Sessions (FAS): Ja

Forward-Access-Sitzungen (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Entity Resolution

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS Entity Resolution Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, AWS Entity Resolution wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für AWS Entity Resolution

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS Entity Resolution -Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden AWS Entity Resolution, einschließlich des Formats von ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Entity Resolution in der Referenz zur Serviceautorisierung.

Themen

- Best Practices für Richtlinien
- Verwenden der Konsole AWS Entity Resolution
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Best Practices für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Entity Resolution Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr

verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren

Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Konsole AWS Entity Resolution

Um auf die AWS Entity Resolution Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Entity Resolution Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS Entity Resolution Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS Entity Resolution *ConsoleAccess* oder die *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI AWS OR-API.

```
{
    "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 verwaltete Richtlinien für AWS Entity Resolution

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das

Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSEntityResolutionConsoleFullAccess

Sie können die `AWSEntityResolutionConsoleFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt vollen Zugriff auf AWS Entity Resolution Endgeräte und Ressourcen.

Diese Richtlinie ermöglicht auch bestimmten Lesezugriff auf verwandte Themen AWS-Services wie S3 AWS Glue, Tagging, Amazon AWS KMS EventBridge, AWS Data Exchange sodass die Konsole Auswahlmöglichkeiten anzeigen und die ausgewählten Optionen verwenden kann, um Aktionen zur Entitätsauflösung durchzuführen. Darüber hinaus gewährt diese Richtlinie Zugriff auf Connect-APIs für Kundenprofile, um die Integration für die automatische Verarbeitung von Spielergebnissen zu ermöglichen. Einige Ressourcen sind so eingegrenzt, dass sie den Dienstnamen `entityresolution` enthalten.

Da AWS Entity Resolution für die Ausführung von Aktionen mit verwandten AWS Ressourcen eine übergebene Rolle erforderlich ist, gewährt diese Richtlinie auch die Berechtigungen zum Auswählen und Weitergeben einer gewünschten Rolle.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `EntityResolutionAccess`— Ermöglicht Prinzipalen den vollen Zugriff auf AWS Entity Resolution Endpunkte und Ressourcen.
- `GlueSourcesConsoleDisplay`— Gewährt den Zugriff auf AWS Glue Listentabellen als Datenquellenoptionen und das Importtabellenschema einer Datenquelle aus Gründen der Benutzerfreundlichkeit.
- `S3BucketsConsoleDisplay`— Gewährt den Zugriff, um alle S3-Buckets als Datenquellenoptionen aufzulisten.
- `S3SourcesConsoleDisplay`— Gewährt den Zugriff zur Anzeige von S3-Buckets als Datenquellenoptionen.

- `TaggingConsoleDisplay`— Gewährt den Zugriff zum Lesen von Tagging-Schlüsseln und -Werten.
- `KMSConsoleDisplay`— Gewährt den Zugriff zur Beschreibung von Schlüsseln und zum Auflisten von Aliasnamen AWS Key Management Service zum Entschlüsseln und Verschlüsseln von Datenquellen.
- `ListRolesToPickForPassing`— Gewährt den Zugriff auf eine Liste aller Rollen, sodass der Benutzer die Rolle auswählen kann, der er übergeben werden soll.
- `PassRoleToEntityResolutionService`— Gewährt den Zugriff zur Weitergabe einer eingegrenzten Rolle an den AWS Entity Resolution Dienst.
- `ManageEventBridgeRules`— Gewährt den Zugriff zum Erstellen, Aktualisieren und Löschen der EventBridge Amazon-Regel für den Empfang von S3-Benachrichtigungen.
- `ADXReadAccess`— Gewährt den Zugriff, AWS Data Exchange um zu überprüfen, ob der Kunde über einen Anspruch oder ein Abonnement verfügt.
- `CustomerProfilesIntegrationAccess`— Gewährt Zugriff auf die APIs Amazon Connect Customer und Connect Customer Profiles, um die Integration zwischen Kundenprofilen AWS Entity Resolution und Connect-Kundenprofilen für die automatisierte Verarbeitung von Spielergebnissen zu ermöglichen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSEntityResolutionConsoleFullAccess in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEntityResolutionConsoleReadOnlyAccess

Sie können `AWSEntityResolutionConsoleReadOnlyAccess` an Ihre IAM-Entitäten anhängen.

Diese Richtlinie gewährt nur Lesezugriff auf AWS Entity Resolution Endpunkte und Ressourcen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `EntityResolutionRead`— Ermöglicht Prinzipalen den schreibgeschützten Zugriff auf Endpunkte und Ressourcen. AWS Entity Resolution

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSEntityResolutionConsoleReadOnlyAccess in der Referenz zu von AWS verwalteten Richtlinien.

AWS Entity Resolution Aktualisierungen für AWS Verwaltete Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien, die AWS Entity Resolution seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite AWS Entity Resolution Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderungen	Beschreibung	Date
`AWSEntityResolutionConsoleFullAccess` – Aktualisierung auf eine bestehende Richtlinie	Hinzugefügt `CustomerProfilesIntegrationAccess` , um die Integration mit Amazon Connect Connect-Kundenprofilen für die automatische Verarbeitung von Spielergebnissen zu ermöglichen.	15. Dezember 2025
`AWSEntityResolutionConsoleFullAccess` – Aktualisierung auf eine bestehende Richtlinie	Die Option Provider-Services wurde im passenden Workflow hinzugefügt `ADXReadAccess` und aktiviert. `ManageEventBridgeRules`	16. Oktober 2023
AWS Entity Resolution hat begonnen, Änderungen zu verfolgen	AWS Entity Resolution hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	18. August 2023

Problembehandlung bei AWS Entity Resolution Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Entity Resolution und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Entity Resolution

- Ich bin nicht berechtigt, iam durchzuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Entity Resolution Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Entity Resolution

Wenn Ihnen AWS-Managementkonsole mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort zur Verfügung gestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `entityresolution:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `entityresolution:`*`GetWidget`* zugreifen zu können.

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Entity Resolutionübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Entity Resolution auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Entity Resolution Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS Entity Resolution unterstützt werden, finden Sie unter. Wie AWS Entity Resolution funktioniert mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Konformitätsüberprüfung für AWS Entity Resolution

Unser neues AWS Anmeldeerlebnis ist nicht für regulierte Workloads konzipiert. Wenn Sie unser neues AWS Anmeldeerlebnis nutzen, es aber AWS für regulierte Workloads nutzen möchten, können Sie sich für erweiterte Funktionen für AWS Ihre Umgebung anmelden oder diese aktivieren. AWS

Um zu erfahren, ob AWS-Service ein Programm AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme, .

Sie können Auditberichte von Drittanbietern mit herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter Berichte AWS Artifact .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens sowie den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Compliance-Verantwortung bei der Verwendung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

AWS Entity Resolution Bewährte Verfahren zur Einhaltung

In diesem Abschnitt finden Sie bewährte Verfahren und Empfehlungen zur Einhaltung der Vorschriften bei der Verwendung AWS Entity Resolution.

Payment Card Industry Data Security Standards (PCI DSS)

AWS Entity Resolution unterstützt die Verarbeitung, Speicherung und Übertragung von Kreditkartendaten durch einen Händler oder Dienstleister und wurde als konform mit dem Payment Card Industry (PCI) Data Security Standard (DSS) validiert. Weitere Informationen zu PCI DSS, einschließlich der Frage, wie Sie eine Kopie des AWS PCI Compliance Package anfordern können, finden Sie unter PCI DSS Level 1.

System and Organization Controls (SOC)

AWS Entity Resolution entspricht den SOC-Maßnahmen (System and Organization Controls), einschließlich SOC 1, SOC 2 und SOC 3. SOC-Berichte sind unabhängige Prüfungsberichte von Drittanbietern, aus denen hervorgeht, wie wichtige Compliance-Kontrollen und -Ziele AWS erreicht werden. Diese Audits stellen sicher, dass geeignete Sicherheitsmaßnahmen und Verfahren zum Schutz vor Beeinträchtigungen von Sicherheit, Vertraulichkeit und Verfügbarkeit von Kunden- und Unternehmensdaten vorhanden sind. Die Ergebnisse dieser Prüfungen durch Dritte sind auf der AWS SOC-Compliance-Website verfügbar. Dort können Sie die veröffentlichten Berichte einsehen, um weitere Informationen zu den Kontrollen zu erhalten, die den AWS Betrieb und die Einhaltung der Vorschriften unterstützen.

Resilienz in AWS Entity Resolution

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur AWS Entity Resolution bietet es mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

Überwachung AWS Entity Resolution

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Entity Resolution anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, mit denen Sie beobachten AWS Entity Resolution, melden können, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen ergreifen können:

- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, anhand der Quell-IP ermitteln, von wem die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolle von Amazon EC2 EC2-Instances und anderen Quellen überprüfen CloudTrail, speichern und darauf zugreifen. CloudWatch Logs kann Informationen in den Protokolldateien überprüfen und Ihnen mitteilen, wann bestimmte Schwellenwerte erreicht sind. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

Themen

- Protokollieren von AWS Entity Resolution API-Aufrufen mit AWS CloudTrail
- Workflows mithilfe von Amazon Logs überwachen und CloudWatch protokollieren

Protokollieren von AWS Entity Resolution API-Aufrufen mit AWS CloudTrail

AWS Entity Resolution ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden AWS Entity Resolution. CloudTrail erfasst alle API-Aufrufe AWS Entity Resolution als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Entity Resolution Konsole und Codeaufrufen für die AWS Entity Resolution API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Entity Resolution. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen.

Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde AWS Entity Resolution, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

AWS Entity Resolution Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet AWS Entity Resolution, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen im Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse im CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich der Ereignisse für AWS Entity Resolution, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle AWS Entity Resolution Aktionen werden von der AWS Entity Resolution API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

AWS Entity Resolution Logdateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Workflows mithilfe von Amazon Logs überwachen und CloudWatch protokollieren

AWS Entity Resolution bietet umfassende Protokollierungsfunktionen, mit denen Sie Ihre Workflows für den Abgleich und die Zuordnung von IDs überprüfen und analysieren können. Durch die Integration mit Amazon CloudWatch Logs können Sie detaillierte Informationen zur Workflow-Ausführung erfassen, darunter Ereignistypen, Zeitstempel, Verarbeitungsstatistiken und Fehlerzahlen. Sie können wählen, ob Sie diese CloudWatch Protokolle an Logs-, Amazon S3- oder Amazon Data Firehose-Ziele liefern möchten. Durch die Analyse dieser Protokolle können Sie die Serviceleistung bewerten, Probleme beheben, Einblicke in Ihren Kundenstamm gewinnen und Ihre AWS Entity Resolution Nutzung und Abrechnung besser verstehen. Die Protokollierung ist zwar standardmäßig deaktiviert, Sie können sie jedoch über die Konsole oder API sowohl für neue als auch für bestehende Workflows aktivieren.

Wenn Sie die Protokollierung für AWS Entity Resolution Workflows aktivieren, fallen die üblichen CloudWatch Verkaufsgebühren von Amazon an, einschließlich der Kosten für die Aufnahme, Speicherung und Analyse von Protokollen. Detaillierte Preisinformationen finden Sie auf der CloudWatch Preisseite. .

Themen

- Einrichten der Protokollbereitstellung
- Protokollierung deaktivieren (Konsole)

- Die Protokolle lesen

Einrichten der Protokollbereitstellung

In diesem Abschnitt werden die erforderlichen Berechtigungen für die Verwendung der AWS Entity Resolution Protokollierung sowie die Aktivierung der Protokollzustellung über die Konsole und erläutert APIs.

Themen

- Berechtigungen
- Aktivieren der Protokollierung für einen neuen Workflow (Konsole)
- Aktivieren der Protokollierung für einen neuen Workflow (API)
- Aktivieren der Protokollierung für einen vorhandenen Workflow (Konsole)

Berechtigungen

AWS Entity Resolution verwendet CloudWatch bereitgestellte Protokolle, um die Workflow-Protokollierung bereitzustellen. Für die Übermittlung von Workflow-Protokollen benötigen Sie Berechtigungen für das von Ihnen angegebene Protokollierungsziel.

Um die erforderlichen Berechtigungen für jedes Protokollierungsziel zu sehen, wählen Sie im Amazon CloudWatch Logs-Benutzerhandbuch einen der folgenden AWS Dienste aus.

- CloudWatch Amazon-Protokolle
- Amazon Simple Storage Service (Amazon-S3)
- Amazon Data Firehose

Um die Protokollierungskonfiguration zu erstellen, anzuzeigen oder zu ändern AWS Entity Resolution, benötigen Sie die erforderlichen Berechtigungen. Ihre IAM-Rolle muss die folgenden Mindestberechtigungen für die Verwaltung der Workflow-Protokollierung in der AWS Entity Resolution Konsole enthalten.

JSON

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

```
    "Statement": [
        {
            "Sid": "AllowLogDeliveryActionsConsoleCWL",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:log-group:*"
            ]
        },
        {
            "Sid": "AllowLogDeliveryActionsConsoleS3",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowLogDeliveryActionsConsoleFH",
            "Effect": "Allow",
            "Action": [
                "firehose:ListDeliveryStreams",
                "firehose:DescribeDeliveryStream"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Weitere Informationen zu Berechtigungen zur Verwaltung der Workflow-Protokollierung finden Sie unter Aktivieren der Protokollierung von AWS Diensten im Amazon CloudWatch Logs-Benutzerhandbuch.

Aktivieren der Protokollierung für einen neuen Workflow (Konsole)

Nachdem Sie die Berechtigungen für das Protokollierungsziel eingerichtet haben, können Sie die Protokollierung für einen neuen Workflow AWS Entity Resolution mithilfe der Konsole aktivieren.

So aktivieren Sie die Protokollierung für einen neuen Workflow (Konsole)

1. Öffnen Sie die AWS Entity Resolution Konsole zu https://console.aws.amazon.com/entityresolution/Hause.
2. Wählen Sie unter Workflows entweder Passende Workflows oder Workflows für ID-Mapping aus.
3. Folgen Sie den Schritten, um einen der folgenden Workflows zu erstellen:
   - Regelbasierter Abgleichs-Workflow
   - Auf maschinellem Lernen basierender Matching-Workflow
   - Auf Diensten basierender Abgleichs-Workflow für Anbieter
   - Workflow zur ID-Zuordnung für ein Konto
   - Workflow zur ID-Zuordnung für zwei Konten
4. Wählen Sie für Schritt 1 Passende Workflow-Details angeben und für Protokolllieferungen — EntityResolution Workflow-Protokolle die Option Hinzufügen aus.
   - Wählen Sie eines der folgenden Ziele für die Protokollierung aus.
     - Zu Amazon CloudWatch Logs
     - Zu Amazon S3
     - Zu Amazon Data Firehose

> **Tip**
>
> Wenn Sie sich für Amazon S3 oder Firehose entscheiden, können Sie Ihre Protokolle an ein Cross-Konto oder ein Girokonto senden.
> Um die kontoübergreifende Lieferung zu ermöglichen, AWS-Konten müssen beide über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie im Beispiel für kontoübergreifende Lieferungen im Amazon CloudWatch Logs-Benutzerhandbuch.

5. Für die Ziel-Protokollgruppe werden die Protokollgruppen, denen das Präfix '/aws/vendedlogs/' vorangestellt ist, automatisch erstellt. Wenn Sie andere Protokollgruppen verwenden, erstellen Sie diese, bevor Sie eine Protokollzustellung einrichten. Weitere Informationen finden Sie unter Arbeiten mit Protokollgruppen und Protokollstreams im Amazon CloudWatch Logs-Benutzerhandbuch.
6. Für weitere Einstellungen — optional — wählen Sie Folgendes:
   a. Wählen Sie unter Feldauswahl die Protokollfelder aus, die in jeden Protokolldatensatz aufgenommen werden sollen.
   b. (CloudWatch Protokolle) Wählen Sie unter Ausgabeformat das Ausgabeformat für das Protokoll aus.
   c. Wählen Sie unter Feldtrennzeichen aus, wie die einzelnen Protokollfelder getrennt werden sollen.
   d. (Amazon S3) Geben Sie für Suffix den Suffixpfad an, um Ihre Daten zu partitionieren.
   e. (Amazon S3) Wählen Sie für HIVE-kompatibel die Option Aktivieren aus, wenn Sie Hive-kompatible S3-Pfade verwenden möchten.
7. Um ein weiteres Protokollziel zu erstellen, wählen Sie Hinzufügen und wiederholen Sie die Schritte 4 bis 6.
8. Führen Sie die verbleibenden Schritte aus, um den Workflow einzurichten und auszuführen.
9. Nachdem die Workflow-Jobs abgeschlossen sind, überprüfen Sie die Workflow-Protokolle in dem von Ihnen angegebenen Ziel für die Protokollzustellung.

Aktivieren der Protokollierung für einen neuen Workflow (API)

Nachdem Sie die Berechtigungen für das Protokollierungsziel eingerichtet haben, können Sie die Protokollierung für einen neuen Workflow AWS Entity Resolution mithilfe von Amazon CloudWatch Logs aktivieren APIs.

Um die Protokollierung für einen neuen Workflow (API) zu aktivieren

1. Nachdem Sie einen Workflow in der AWS Entity Resolution Konsole erstellt haben, rufen Sie den Amazon-Ressourcennamen (ARN) des Workflows ab.

   Sie finden den ARN auf der Workflow-Seite in der AWS Entity Resolution Konsole oder Sie rufen die Operation `GetMatchingWorkflow` oder die `GetIdMappingWorkflow` API auf.

Ein Workflow-ARN folgt diesem Format:

```
arn:(aws|aws-us-gov|aws-cn):entityresolution:[a-z]{2}-[a-z]{1,10}-
[0-9]:[0-9]{12}:(matchingworkflow/[a-zA-Z_0-9-]{1,255})
```

Ein ID-Mapping-ARN folgt diesem Format:

```
arn:(aws|aws-us-gov|aws-cn):entityresolution:[a-z]{2}-[a-z]{1,10}-
[0-9]:[0-9]{12}:(idmappingworkflow/[a-zA-Z_0-9-]{1,255})
```

Weitere Informationen finden Sie unter GetMatchingWorkflow oder GetIdMappingWorkflow in der AWS Entity Resolution API-Referenz.

2. Verwenden Sie den CloudWatch `PutDeliverySource` Logs-API-Vorgang, um eine Übermittlungsquelle für die Workflow-Protokolle zu erstellen.

   Weitere Informationen finden Sie PutDeliverySourcein der Amazon CloudWatch Logs API-Referenz.

   a. Übergeben Sie das`resourceArn`.

   b. Denn `logType` es werden folgende Arten von Protokollen gesammelt`WORKFLOW_LOGS`:

   Example

   Beispiel für einen `PutDeliverySource` API-Vorgang

   ```
   {
       "logType": "WORKFLOW_LOGS",
       "name": "my-delivery-source",
       "resourceArn": "arn:aws:entityresolution:region:accoungId:matchingworkflow/
   XXXWorkflow"
   }
   ```

3. Verwenden Sie den `PutDeliveryDestination` API-Vorgang, um zu konfigurieren, wo Ihre Protokolle gespeichert werden sollen.

   Sie können entweder CloudWatch Logs, Amazon S3 oder Firehose als Ziel wählen. Sie müssen den ARN einer der Zieloptionen angeben, wo Ihre Protokolle gespeichert werden sollen.

Weitere Informationen finden Sie PutDeliveryDestinationin der Amazon CloudWatch Logs API-Referenz.

Example

Beispiel für einen `PutDeliveryDestination` API-Vorgang

```
{
   "delivery-destination-configuration": {
      "destinationResourceArn": "arn:aws:logs:region:accountId:log-group:my-log-
group"
   },
   "name": "my-delivery-destination",
   "outputFormat": "json",
   }
}
```

> **Note**
>
> Wenn Sie Protokolle kontoübergreifend bereitstellen, müssen Sie die PutDeliveryDestinationPolicyAPI verwenden, um dem Zielkonto eine AWS Identity and Access Management (IAM-) Richtlinie zuzuweisen. Die IAM-Richtlinie ermöglicht die Bereitstellung von einem Konto in einem anderen Konto.

4. Verwenden Sie den `CreateDelivery` API-Vorgang, um die Lieferquelle mit dem Ziel zu verknüpfen, das Sie in den vorherigen Schritten erstellt haben. Diese API-Operation verknüpft die Bereitstellungsquelle mit dem Endziel.

   Weitere Informationen finden Sie PutDeliveryDestinationin der Amazon CloudWatch Logs API-Referenz.

   Example

   Beispiel für einen `CreateDelivery` API-Vorgang

   ```
   {
      "delivery-destination-arn": "arn:aws:logs:region:accountId:log-group:my-log-
   group",
      "delivery-source-name": "my-delivery-source",
      "tags": {
   ```

```
      "string" : "string"
   }
}
```

5. Führen Sie den Workflow aus.
6. Nachdem die Workflow-Jobs abgeschlossen sind, überprüfen Sie die Workflow-Protokolle in dem von Ihnen angegebenen Ziel für die Protokollzustellung.

Aktivieren der Protokollierung für einen vorhandenen Workflow (Konsole)

Nachdem Sie die Berechtigungen für das Protokollierungsziel eingerichtet haben, können Sie die Protokollierung für einen vorhandenen Workflow AWS Entity Resolution mithilfe der Registerkarte Protokolllieferungen in der Konsole aktivieren.

Um die Protokollierung für einen vorhandenen Workflow mithilfe der Registerkarte Lieferungen protokollieren (Konsole) zu aktivieren

1. Öffnen Sie die AWS Entity Resolution Konsole zu https://console.aws.amazon.com/entityresolution/Hause.
2. Wählen Sie unter Workflows entweder Passende Workflows oder Workflows für ID-Mapping aus und wählen Sie dann Ihren vorhandenen Workflow aus.
3. Wählen Sie auf der Registerkarte Protokollzustellungen unter Protokollzustellung die Option Hinzufügen aus, und wählen Sie dann eines der folgenden Protokollierungsziele aus.
   - Zu Amazon CloudWatch Logs
   - Zu Amazon S3
     - Kontoübergreifend
     - Im aktuellen Konto
   - Zu Amazon Data Firehose
     - Kontoübergreifend
     - Im aktuellen Konto

> **Tip**
>
> Wenn Sie sich für Amazon S3 oder Firehose entscheiden, können Sie Ihre Protokolle an ein Cross-Konto oder ein Girokonto senden.

Um die kontoübergreifende Lieferung zu ermöglichen, AWS-Konten müssen beide über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie im Beispiel für kontoübergreifende Lieferungen im Amazon CloudWatch Logs-Benutzerhandbuch.

4. Gehen Sie im Modal je nach Art der Protokollzustellung, die Sie ausgewählt haben, wie folgt vor.

   a. Zeigen Sie den Protokolltyp an: WORKFLOW_LOGS.

      Der Protokolltyp kann nicht geändert werden.

   b. (CloudWatch Protokolle) Für die Zielprotokollgruppe werden die Protokollgruppen, denen das Präfix '/aws/vendedlogs/' vorangestellt ist, automatisch erstellt. Wenn Sie andere Protokollgruppen verwenden, erstellen Sie diese, bevor Sie eine Protokollzustellung einrichten. Weitere Informationen finden Sie unter Arbeiten mit Protokollgruppen und Protokollstreams im Amazon CloudWatch Logs-Benutzerhandbuch.

      (Amazon S3 im Girokonto) Wählen Sie für Destination S3-Bucket einen Bucket aus oder geben Sie einen ARN ein.

      (Kontenübergreifendes Amazon S3) Geben Sie für den Lieferziel-ARN einen Lieferziel-ARN ein.

      (Firehose im Girokonto) Geben Sie für Destination Delivery Stream den ARN der Lieferzielressource ein, die in einem anderen Konto erstellt wurde.

      (Firehose Cross-Konto) Geben Sie für Lieferziel-ARN einen Lieferziel-ARN ein.

5. Wählen Sie für weitere Einstellungen — optional — Folgendes aus:

   a. Wählen Sie unter Feldauswahl die Protokollfelder aus, die in jeden Protokolldatensatz aufgenommen werden sollen.

   b. (CloudWatch Protokolle) Wählen Sie unter Ausgabeformat das Ausgabeformat für das Protokoll aus.

   c. Wählen Sie unter Feldtrennzeichen aus, wie die einzelnen Protokollfelder getrennt werden sollen.

   d. (Amazon S3) Geben Sie für Suffix den Suffixpfad an, um Ihre Daten zu partitionieren.

   e. (Amazon S3) Wählen Sie für HIVE-kompatibel die Option Aktivieren aus, wenn Sie Hive-kompatible S3-Pfade verwenden möchten.

6. Wählen Sie Hinzufügen aus.

7. Wählen Sie auf der Workflow-Seite die Option Ausführen aus.
8. Nachdem die Workflow-Jobs abgeschlossen sind, überprüfen Sie die Workflow-Protokolle in dem von Ihnen angegebenen Ziel für die Protokollzustellung.

Protokollierung deaktivieren (Konsole)

Sie können die Protokollierung für Ihren AWS Entity Resolution Workflow jederzeit in der Konsole deaktivieren.

Um die Workflow-Protokollierung zu deaktivieren (Konsole)

1. Öffnen Sie die AWS Entity Resolution Konsole zu https://console.aws.amazon.com/entityresolution/Hause.
2. Wählen Sie unter Workflows entweder Matching Workflows oder ID Mapping Workflows und wählen Sie dann Ihren Workflow aus.
3. Wählen Sie auf der Registerkarte Protokollzustellungen unter Protokollzustellung das Ziel aus, und wählen Sie dann Löschen aus.
4. Überprüfen Sie Ihre Änderungen und fahren Sie dann mit dem nächsten Schritt fort, um Ihre Änderungen zu speichern.

Die Protokolle lesen

Das Lesen von Amazon CloudWatch Logs hilft Ihnen dabei, effiziente AWS Entity Resolution Arbeitsabläufe aufrechtzuerhalten. Protokolle bieten einen detaillierten Einblick in die Ausführung Ihres Workflows, einschließlich wichtiger Kennzahlen wie der Anzahl der verarbeiteten Datensätze und aller aufgetretenen Fehler, sodass Sie sicherstellen können, dass Ihre Datenverarbeitung reibungslos abläuft. Darüber hinaus bieten die Protokolle eine Echtzeitverfolgung des Workflow-Fortschritts anhand von Zeitstempeln und Ereignistypen, sodass Sie Engpässe oder Probleme in Ihrer Datenverarbeitungspipeline schnell erkennen können. Die umfassenden Informationen zur Fehlerverfolgung und zur Anzahl der Datensätze helfen Ihnen dabei, die Qualität und Vollständigkeit der Daten aufrechtzuerhalten, da genau angezeigt wird, wie viele Datensätze erfolgreich verarbeitet wurden und ob welche unbearbeitet geblieben sind.

Wenn Sie CloudWatch Logs als Ziel verwenden, können Sie CloudWatch Logs Insights verwenden, um die Workflow-Protokolle zu lesen. Es fallen typische Gebühren für CloudWatch Logs an. Weitere

Informationen finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im Amazon CloudWatch Logs-Benutzerhandbuch.

> **Note**
>
> Es kann einige Minuten dauern, bis Workflow-Protokolle an Ihrem Zielort angezeigt werden. Wenn Sie die Protokolle nicht sehen, warten Sie ein paar Minuten und aktualisieren Sie die Seite.

Die Workflow-Protokolle bestehen aus einer Folge formatierter Protokolldatensätze, wobei jeder Protokolldatensatz einen Workflow darstellt. Die Reihenfolge der Felder innerhalb des Protokolls kann variieren.

```
{
  "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-ingress-point/inp-
xxxxx",
  "event_type": "JOB_START",
  "event_timestamp": 1728562395042,
  "job_id": "b01eea4678d4423a4b43eeada003f6",
  "workflow_name": "TestWorkflow",
  "workflow_start_time": "2025-03-11 10:19:56",
  "data_procesing_progression": "Matching Job Starts ...",
  "total_records_processed": 1500,
  "total_records_unprocessed": 0,
  "incremental_records_processed": 0,
  "error_message": "sample error that caused workflow failure"
}
```

In der folgenden Liste werden die Protokolldatensatzfelder der Reihe nach beschrieben:

`resource_arn`

Der Amazon-Ressourcenname (ARN), der die im Workflow verwendete AWS Ressource eindeutig identifiziert.

`event_type`

Die Art des Ereignisses, das während der Workflow-Ausführung aufgetreten ist. AWS Entity Resolution unterstützt derzeit:

`JOB_START`

DATA_PROCESSING_STEP_START

DATA_PROCESSING_STEP_END

JOB_SUCCESS

JOB_FAILURE

`event_timestamp`

Der Unix-Zeitstempel, der angibt, wann das Ereignis während des Workflows eingetreten ist.

`job_id`

Eine eindeutige Kennung, die der spezifischen Workflow-Jobausführung zugewiesen wurde.

`workflow_name`

Der Name, der dem ausgeführten Workflow gegeben wurde.

`workflow_start_time`

Datum und Uhrzeit des Beginns der Workflow-Ausführung.

`data_procesing_progression`

Eine Beschreibung der aktuellen Phase im Datenverarbeitungs-Workflow. Beispiele: `"Matching Job Starts"`, `"Loading Step Starts"`, `"ID_Mapping Job Ends Successfully"`.

`total_records_processed`

Die Gesamtzahl der Datensätze, die während des Workflows erfolgreich verarbeitet wurden.

`total_records_unprocessed`

Die Anzahl der Datensätze, die während der Workflow-Ausführung nicht verarbeitet wurden.

`incremental_records_processed`

Die Anzahl der neuen Datensätze, die in einer inkrementellen Workflow-Aktualisierung verarbeitet wurden.

`error_message`

Die Hauptursache für Workflow-Fehler.

Erstellen Sie AWS Entity Resolution-Ressourcen mit AWS CloudFormation

AWS Entity Resolution ist in einen Service integriert AWS CloudFormation, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt (z. B. AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace und AWS::EntityResolution::PolicyStatement) und diese Ressourcen für Sie CloudFormation bereitstellt und konfiguriert.

Wenn Sie sie verwenden CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre AWS Entity Resolution-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren AWS-Konten Regionen bereit.

AWS-Entitätsauflösung und CloudFormation Vorlagen

Um Ressourcen für AWS Entity Resolution und verwandte Services bereitzustellen und zu konfigurieren, müssen Sie CloudFormation Vorlagen verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie CloudFormation Designer verwenden, um Ihnen die ersten Schritte mit Vorlagen zu erleichtern. CloudFormation Weitere Informationen finden Sie unter Was ist CloudFormation - Designer? im AWS CloudFormation -Benutzerhandbuch.

AWS Entity Resolution unterstützt das Erstellen AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace und AWS::EntityResolution::PolicyStatement Eingeben CloudFormation. Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace und AWS::EntityResolution::PolicyStatement, finden Sie in der AWS-Referenz zum Ressourcentyp „AWS Entity Resolution“ im AWS CloudFormation Benutzerhandbuch.

Die folgenden Vorlagen sind verfügbar:

- Passender Arbeitsablauf

  Erstellen Sie ein `MatchingWorkflow` Objekt, das die Konfiguration des auszuführenden Datenverarbeitungsjobs speichert.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::EntityResolution::MatchingWorkflow im CloudFormation -Benutzerhandbuch

  CreateMatchingWorkflow in der AWS Entity Resolution -API-Referenz

- Schemazuordnung

  Erstellen Sie eine Schemazuordnung, die das Schema der Eingabetabelle mit Kundendatensätzen definiert.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::EntityResolution::SchemaMapping im CloudFormation -Benutzerhandbuch

  CreateSchemaMapping in der AWS Entity Resolution -API-Referenz

- Arbeitsablauf für die ID-Zuordnung

  Erstellen Sie ein `IdMappingWorkflow` Objekt, das die Konfiguration des auszuführenden Datenverarbeitungsauftrags speichert.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::EntityResolution::IdMappingWorkflow im CloudFormation -Benutzerhandbuch

  CreateIdMappingWorkflow in der AWS Entity Resolution -API-Referenz

- ID-Namespace

  Erstellen Sie ein `IdNamespace` Objekt, das die Metadaten speichert, in denen der Datensatz und seine Verwendung erklärt werden.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::EntityResolution::IdNamespace im CloudFormation -Benutzerhandbuch

  CreateIdNamespace in der AWS Entity Resolution -API-Referenz

- PolicyStatement

Erstellen Sie ein `PolicyStatement`-Objekt.

Weitere Informationen finden Sie unter den folgenden Themen:

AWS::EntityResolution::PolicyStatement im CloudFormation -Benutzerhandbuch

AddPolicyStatement in der AWS Entity Resolution -API-Referenz

Erfahren Sie mehr über CloudFormation

Weitere Informationen CloudFormation dazu finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- CloudFormation API Referenz
- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Kontingente für AWS Entity Resolution

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jedes Kontingent AWS-Service. Sofern nicht anders angegeben, gilt für jedes Kontingent Region-specific. Sie können für einige Kontingente eine Erhöhung beantragen, andere Kontingente können jedoch nicht erhöht werden.

Um die Kontingente für anzuzeigen AWS Entity Resolution, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS-Services aus und wählen Sie AWS Entity Resolution.

Informationen zum Beantragen einer Kontingenterhöhung finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch. Wenn das Kontingent noch nicht unter Servicekontingente verfügbar ist, verwenden Sie das Formular zur Erhöhung des Limits.

Ihr AWS-Konto hat die folgenden Kontingente im Zusammenhang mit AWS Entity Resolution.

Name	Standard	Anpas	Description
Gleichzeitige Jobs zur ID-Zuordnung	Jede unterstützte Region: 1	Nein	Die maximale Anzahl von Workflows zur ID-Zuordnung, die in der aktuellen AWS Region gleichzeitig verarbeitet werden können.
Gleichzeitige übereinstimmende Jobs	Jede unterstützte Region: 1	Nein	Die maximale Anzahl von passenden Workflows, die in der aktuellen AWS Region gleichzeitig verarbeitet werden können.
Workflows zur ID-Zuordnung	Jede unterstützte Region: 10	Yes (Ja)	Die maximale Anzahl von Workflows zur ID-Zuordnung, die Sie in diesem Konto in der aktuellen AWS Region erstellen können.

Name	Standard	Anpas	Description
ID-Namespaces	Jede unterstützte Region: 10	Yes (Ja)	Die maximale Anzahl von ID-Namespaces, die Sie in diesem Konto in der aktuellen Region erstellen können. AWS
Passende Workflows	Jede unterstützte Region: 10	Yes (Ja)	Die maximale Anzahl übereinstimmender Workflows, die Sie in diesem Konto in der aktuellen AWS Region erstellen können.
Rate der GenerateMatchId API-Anfragen	Jede unterstützte Region: 10	Yes (Ja)	Die maximale Anzahl von GenerateMatchId API-Anfragen pro Sekunde
Rate der GetMatchId API-Anfragen	Jede unterstützte Region: 50	Ja	Die maximale Anzahl von GetMatchId API-Anfragen pro Sekunde.
Datensätze pro auf maschinellem Lernen basierendem Matching-Workflow	Jede unterstützte Region: 150.000.000	Ja	Die maximale Anzahl von Datensätzen, die von einem auf maschinellem Lernen basierenden Matching-Workflow in diesem Konto in den AWS Regionen af-south-1, ap-northeast-2, eu-west-2 verarbeitet werden können.

Name	Standard	Anpas	Description
Datensätze pro auf maschinellem Lernen basierendem Matching-Workflow	Jede unterstützte Region: 600.000.000	Ja	Die maximale Anzahl von Datensätzen, die von einem auf maschinellem Lernen basierenden Abgleichsworkflow in diesem Konto in den AWS Regionen ap-northeast-1, ap-southeast-1, ap-southeast-2, ca-central-1, eu-central-1, eu-west-1, us-east-1, us-east-2, us-west-2 verarbeitet werden können.
Workflow für die Zuordnung von Datensätzen pro Anbieter-ID	Jede unterstützte Region: 150.000.000	Ja	Die maximale Anzahl von Datensätzen, die für die Anbieter-ID-Zuordnung in diesem Konto in den AWS Regionen af-south-1, ap-northeast-2, eu-west-2 verarbeitet werden können.
Workflow für die Zuordnung von Datensätzen pro Anbieter-ID	Jede unterstützte Region: 250.000.000	Ja	Die maximale Anzahl von Datensätzen, die für die Anbieter-ID-Zuordnung in diesem Konto in den AWS Regionen ap-northeast-1, ap-southeast-1, ap-southeast-2, ca-central-1, eu-central-1, eu-west-1, us-east-1, us-east-2, us-west-2 verarbeitet werden können.

Name	Standard	Anpas	Description
Dienstbasierter Abgleichs-Workflow für Datensätze pro Anbieter	Jede unterstützte Region: 100 000 000	Ja	Die maximale Anzahl von Datensätzen, die von einem auf Anbieterdiensten basierenden Abgleichsworkflow in diesem Konto in der aktuellen AWS Region verarbeitet werden können.
Datensätze pro regelbasiertem ID-Zuordnungs-Workflow	Jede unterstützte Region: 150.000.000	Ja	Die maximale Anzahl von Datensätzen, die für die regelbasierte ID-Zuordnung in diesem Konto in den AWS Regionen af-south-1, ap-northeast-2, eu-west-2 verarbeitet werden können.
Datensätze pro regelbasiertem ID-Zuordnungs-Workflow	Jede unterstützte Region: 1.000.000.000	Ja	Die maximale Anzahl von Datensätzen, die für die regelbasierte ID-Zuordnung in diesem Konto in den AWS Regionen ap-northeast-1, ap-southeast-1, ap-southeast-2, ca-central-1, eu-central-1, eu-west-1, us-east-1, us-east-2, us-west-2 verarbeitet werden können.

Name	Standard	Anpas	Description
Datensätze pro regelbasiertem Abgleichs-Workflow	Jede unterstützte Region: 100 000 000	Ja	Die maximale Anzahl von Datensätzen, die von einem regelbasierten Abgleichsworkflow in diesem Konto in der aktuellen Region verarbeitet werden können. AWS
Schemazuordnungen	Jede unterstützte Region: 50	Ja	Die maximale Anzahl von Schemazuordnungen, die Sie in diesem Konto in der aktuellen Region erstellen können. AWS

API-Drosselungskontingente

Ressource	Ratenlimit	Description
Rate der Anfragen `CreateMatchingWorkflow`	5 TPS	Maximale Anzahl von `CreateMatchingWorkflow` API-Aufrufen pro Sekunde.
Rate der `DeleteMatchingWorkflow` Anfragen	5 TPS	Maximale Anzahl von `DeleteMatchingWorkflow` API-Aufrufen pro Sekunde.
Rate der `GetMatchingWorkflow` Anfragen	5 TPS	Maximale Anzahl von `GetMatchingWorkflow` API-Aufrufen pro Sekunde.
Rate der `ListMatchingWorkflows` Anfragen	5 TPS	Maximale Anzahl von `ListMatchingWorkfl`

Ressource	Ratenlimit	Description
		ows API-Aufrufen pro Sekunde.
Rate der UpdateMatchingWorkflow Anfragen	5 TPS	Maximale Anzahl von UpdateMatchingWorkflow API-Aufrufen pro Sekunde.
Rate der CreateSchemaMapping Anfragen	5 TPS	Maximale Anzahl von CreateSchemaMapping API-Aufrufen pro Sekunde.
Rate der DeleteSchemaMapping Anfragen	5 TPS	Maximale Anzahl von DeleteSchemaMapping API-Aufrufen pro Sekunde.
Rate der GetSchemaMapping Anfragen	5 TPS	Maximale Anzahl von GetSchemaMapping API-Aufrufen pro Sekunde.
Rate der ListSchemaMappings Anfragen	5 TPS	Maximale Anzahl von ListSchemaMappings API-Aufrufen pro Sekunde.
Rate der UpdateSchemaMapping Anfragen	5 TPS	Maximale Anzahl von UpdateSchemaMapping API-Aufrufen pro Sekunde.
Rate der GetPartnerComponent Anfragen	5 TPS	Maximale Anzahl von GetPartnerComponent API-Aufrufen pro Sekunde.
Rate der ListPartnerComponents Anfragen	5 TPS	Maximale Anzahl von ListPartnerComponents API-Aufrufen pro Sekunde.

Ressource	Ratenlimit	Description
Rate der `TagResource` Anfragen	5 TPS	Maximale Anzahl von `TagResource` API-Aufrufen pro Sekunde.
Rate der `UntagResource` Anfragen	5 TPS	Maximale Anzahl von `UntagResource` API-Aufrufen pro Sekunde.
Rate der `ListTagsForResource` Anfragen	5 TPS	Maximale Anzahl von `ListTagsForResource` API-Aufrufen pro Sekunde.
Rate der `CreateIdMappingWorkflow` Anfragen	5 TPS	Maximale Anzahl von `CreateIdMappingWorkflow` API-Aufrufen pro Sekunde.
Rate der `DeleteIdMappingWorkflow` Anfragen	5 TPS	Maximale Anzahl von `DeleteIdMappingWorkflow` API-Aufrufen pro Sekunde.
Rate der `GetIdMappingWorkflow` Anfragen	5 TPS	Maximale Anzahl von `GetIdMappingWorkflow` API-Aufrufen pro Sekunde.
Rate der `ListIdMappingWorkflow` Anfragen	5 TPS	Maximale Anzahl von `ListIdMappingWorkflow` API-Aufrufen pro Sekunde.
Rate der `UpdateIdMappingWorkflow` Anfragen	5 TPS	Maximale Anzahl von `UpdateIdMappingWorkflow` API-Aufrufen pro Sekunde.

Ressource	Ratenlimit	Description
Rate der `ListProviderServices` Anfragen	5 TPS	Maximale Anzahl von `ListProviderServices` API-Aufrufen pro Sekunde.
Rate der `GetProviderService` Anfragen	5 TPS	Maximale Anzahl von `GetProviderService` API-Aufrufen pro Sekunde.
Rate der `CreateIdNamespace` Anfragen	5 TPS	Maximale Anzahl von `CreateIdNamespace` API-Aufrufen pro Sekunde.
Rate der `DeleteIdNamespace` Anfragen	5 TPS	Maximale Anzahl von `DeleteIdNamespace` API-Aufrufen pro Sekunde.
Rate der `GetIdNamespace` Anfragen	5 TPS	Maximale Anzahl von `GetIdNamespace` API-Aufrufen pro Sekunde.
Rate der `ListIdNamespaces` Anfragen	5 TPS	Maximale Anzahl von `ListIdNamespaces` API-Aufrufen pro Sekunde.
Rate der `UpdateIdNamespace` Anfragen	5 TPS	Maximale Anzahl von `UpdateIdNamespace` API-Aufrufen pro Sekunde.
Rate der `AddPolicyStatement` Anfragen	5 TPS	Maximale Anzahl von `AddPolicyStatement` API-Aufrufen pro Sekunde.
Rate der `DeletePolicyStatement` Anfragen	5 TPS	Maximale Anzahl von `DeletePolicyStatement` API-Aufrufen pro Sekunde.

Ressource	Ratenlimit	Description
Rate der `GetPolicy` Anfragen	5 TPS	Maximale Anzahl von `GetPolicy` API-Aufrufen pro Sekunde.
Rate der `PutPolicy` Anfragen	5 TPS	Maximale Anzahl von `PutPolicy` API-Aufrufen pro Sekunde.
Rate der `GetMatchingJob` Anfragen	10 TPS	Maximale Anzahl von `GetMatchingJob` API-Aufrufen pro Sekunde.
Rate der `ListMatchingJobs` Anfragen	5 TPS	Maximale Anzahl von `ListMatchingJobs` API-Aufrufen pro Sekunde.
Rate der `StartMatchingJob` Anfragen	5 TPS	Maximale Anzahl von `StartMatchingJob` API-Aufrufen pro Sekunde.
Rate der `GetMatchId` Anfragen	50 TPS	Maximale Anzahl von `GetMatchId` API-Aufrufen pro Sekunde.
Rate der `GetIdMappingJob` Anfragen	10 TPS	Maximale Anzahl von `GetIdMappingJob` API-Aufrufen pro Sekunde.
Rate der `ListIdMappingJobs` Anfragen	5 TPS	Maximale Anzahl von `ListIdMappingJobs` API-Aufrufen pro Sekunde.
Rate der `StartIdMappingJob` Anfragen	5 TPS	Maximale Anzahl von `StartIdMappingJob` API-Aufrufen pro Sekunde.

Ressource	Ratenlimit	Description
Rate der `BatchDeleteUniqueId` Anfragen	5 TPS	Maximale Anzahl von `BatchDeleteUniqueId` API-Aufrufen pro Sekunde.

Dokumentenhistorie für AWS Entity Resolution Benutzer-Leitfaden

In der folgenden Tabelle werden die Dokumentationsversionen für beschrieben AWS Entity Resolution.

Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie den RSS-Feed abonnieren. Um RSS-Updates zu abonnieren, müssen Sie ein RSS-Plugin für den von Ihnen verwendeten Browser aktiviert haben.

Änderung	Beschreibung	Datum
Support für transitives Matching	AWS Entity Resolution unterstützt jetzt den transitiven Abgleich für regelbasierte Abgleichs-Workflows, die den Regeltyp Advanced verwenden. Beim transitiven Abgleich werden Datensätze auf allen Regelebenen verarbeitet, sodass abgeglichene Datensätze als Links fungieren können, die Datensätze ohne Zuordnung mit vorhandenen Abgleichsgruppen verbinden.	27. April 2026
Aktualisierung auf eine bestehende Richtlinie	Die folgende neue Berechtigung wurde der `AWSEntityResolutionConsoleFullAccess` verwalteten Richtlinie hinzugefügt:`CustomerProfilesIntegrationAccess` .	15. Dezember 2025

Support für Connect-Kundenprofile	Es wurde die Möglichkeit hinzugefügt, deduplizierte Kundendatensätze direkt in Connect-Kundenprofile zu exportieren, wenn regelbasierte oder auf maschinellem Lernen basierende Matching-Workflows verwendet werden.	15. Dezember 2025
Support für FIPS	AWS Entity Resolution unterstützt jetzt Endgeräte, die dem Federal Information Processing Standard (FIPS) 140-2 entsprechen. AWS PrivateLink	21. Oktober 2025
Arbeitsablauf bei der ID-Zuordnung — Aktualisierung	Kunden können jetzt die inkrementelle Verarbeitung in einem regelbasierten ID-Mapping-Workflow verwenden, um große Datensätze effizienter zu verarbeiten. Kunden können auch Datensätze aus einem ID-Mapping-Workflow löschen, um die Einhaltung der Datenverwaltungsvorschriften zu gewährleisten.	22. September 2025
Support für Cross-Regions	Kunden können jetzt Daten in einem anderen AWS-Region als Eingabe für einen ID-Namespace, einen Zuordnungs-Workflow oder einen ID-Zuordnungs-Workflow verwenden.	8. September 2025

Support für erweiterte Regelbedingungen und inkrementelles Löschen	Kunden können jetzt Regelbedingungen mit booleschen Operatore n und neuen Abgleichs funktionen verwenden ExactManyToMany, die genauere Abgleichskriterien mit Kombinationen aus exaktem und unscharfem Abgleich ermöglichen. Darüber hinaus können Kunden Datensätze in erweiterten Abgleichs-Workflows mithilfe einer Amazon S3 S3-Datei inkrementell löschen.	30. Juli 2025
Klarstellung bei der Verarbeit ung der Match-ID	Es wurde klargestellt, dass für die Optionen „Match-ID ändern oder generieren“ und „Match-ID nachschlagen“ ein automatischer Verarbeit ungsrhythmus in Abgleichs-Workflows erforderlich ist.	17. Juli 2025
Generieren Sie eine neue Match-ID	Kunden können jetzt eine bestehende Match-ID nachschlagen und ändern oder eine neue Match-ID generieren, wenn sie einen regelbasierten Matching-Workflow verwenden.	2. Juni 2025

Workflow für den Abgleich auf Anbieterdiensten — Update	Kunden können jetzt digitale Identifikatoren wie IPV4, IPV6 und MAID verwenden, wenn sie den TransUnion dienstbasierten Matching-Workflow für Anbieter verwenden.	21. April 2025
CloudWatch Amazon-Protokolle	AWS Entity Resolution unterstützt jetzt die CloudWatch Logs-Integration, sodass Sie eine detaillierte Workflow-Protokollierung aktivieren können, in der Metriken, Timing und Verarbeitungsstatistiken zur Auftragsausführung erfasst werden, die an CloudWatch Logs-, Amazon S3- oder Amazon Data Firehose-Ziele gesendet werden können.	14. April 2025
Arbeitsablauf bei der ID-Zuordnung — Aktualisierung	Kunden können jetzt die AWS Glue Partitionierung einrichten, wenn sie einen ID-Mapping-Workflow verwenden.	25. März 2025

Kontingente — Aktualisierung	Documentation-only aktualisieren. Rule-based Matching-Workflows können bis zu 100 Millionen Datensätze verarbeiten, während auf maschinellem Lernen basierende Matching-Workflows bis zu 250 Millionen Datensätze verarbeiten können. Kunden, die höhere Limits benötigen, werden angewiesen, sich an das Serviceteam zu wenden.	7. Februar 2025
Schemazuordnung — Aktualisierung	Documentation-only Aktualisierung, um klarzustellen, dass die Normalisierung für die Attributtypen Vollständiger Name, Vollständige Adresse und Vollständige Telefonnummer unterstützt wird.	17. Januar 2025
Anbieterintegration	Documentation-only aktualisieren. Kunden können lernen, wie sie sich als Dienstanbieter integrieren können AWS Entity Resolution.	8. August 2024
Arbeitsablauf bei der ID-Zuordnung — Aktualisierung	Kunden können jetzt Abgleichsregeln verwenden, um First-Party-Daten in einem ID-Mapping-Workflow zu übersetzen.	23. Juli 2024

Abgleichender Arbeitsablauf — Update	Kunden können die Datensätze jetzt entweder aus einem regelbasierten oder einem ML-based passenden Workflow löschen, um die Einhaltung der Datenverwaltungsvorschriften zu gewährleisten.	8. April 2024
Workflow zur ID-Zuordnung — Aktualisierung	Kunden können jetzt einen ID-Mapping-Workflow für mehrere verwenden AWS-Konten.	2. April 2024
CloudFormation Ressourcen — Neue und aktualisierte Ressourcen	AWS Entity Resolution hat die folgenden Ressourcen hinzugefügt: `AWS::EntityResolution::IdNamespace` und `AWS::EntityResolution::PolicyStatement` und die folgende Ressource aktualisiert:`AWS::EntityResolution::IdMappingWorkflow` .	2. April 2024
Finde die Match-ID	Kunden können jetzt die entsprechende Match-ID und die zugehörige Regel für einen verarbeiteten regelbasierten Workflow finden.	25. März 2024
Abgleichender Arbeitsablauf — Update	AWS Entity Resolution unterstützt jetzt die PII-based RAMPID-Zuweisung im auf LiveRamp Anbieterdiensten basierenden Matching-Workflow.	12. Februar 2024

AWS PrivateLink	AWS Entity Resolution unterstützt jetzt zusätzliche Datensicherheit AWS PrivateLink , sodass Kunden privat auf Dienste zugreifen können, auf denen gehostet wird. AWS	20. Oktober 2023
CloudFormation Ressourcen — Neue und aktualisierte Ressourcen	AWS Entity Resolution hat die folgende Ressource hinzugefügt: `AWS::EntityResolution:IdMappingWorkflow` und die folgenden Ressourcen aktualisiert: `AWS::EntityResolution::MatchingWorkflow` und`AWS::EntityResolution::Schemamapping` .	19. Oktober 2023
Aktualisierung auf eine bestehende Richtlinie	Die folgenden neuen Berechtigungen wurden der `AWSEntityResolutionConsoleFullAccess` verwalteten Richtlinie hinzugefügt: `ADXReadAccess` und`ManageEventBridgeRules` .	16. Oktober 2023
Schemazuordnung — Aktualisierung	Kunden haben jetzt die Möglichkeit, ein vorhandenes Datenschema zu bearbeiten und zu aktualisieren.	16. Oktober 2023

Passender Arbeitsablauf — Aktualisierung	Kunden können jetzt einen bevorzugten Datenanbieter-Service auswählen, um ihre Daten abzugleichen und zu verknüpfen.	16. Oktober 2023
Arbeitsablauf bei der ID-Zuordnung	Kunden können diesen neuen Workflow verwenden, um Details zur ID-Zuordnung anzugeben, die gewünschte ID-Zuordnungsmethode auszuwählen und Dateneingabe- und Ausgabefelder festzulegen.	16. Oktober 2023
CloudFormation Integration	AWS Entity Resolution integriert sich jetzt mit CloudFormation.	24. August 2023
AWS verwaltetes Richtlinienupdate — Neue Richtlinien	AWS Entity Resolution zwei neue verwaltete Richtlinien hinzugefügt.	18. August 2023
Erstversion	Erste Version des AWS Entity Resolution Benutzerhandbuchs	26. Juli 2023

AWS Entity Resolution Glossar

Amazon-Ressourcenname (ARN)

Ein eindeutiger Bezeichner für AWS Ressourcen. ARNs sind erforderlich, wenn Sie eine Ressource in allen Bereichen eindeutig angeben müssen AWS Entity Resolution, z. B. in AWS Entity Resolution Richtlinien, Amazon Relational Database Service (Amazon RDS) -Tags und API-Aufrufen.

Attribut Typ

Der Typ des Attributs für das Eingabefeld. Wenn Sie eine Schemazuordnung erstellen, wählen Sie den Attributtyp aus einer vorkonfigurierten Werteliste wie Name , Adresse, Telefonnummer oder E-Mail-Adresse aus. Der Attributtyp gibt an, AWS Entity Resolution welche Art von Daten Sie präsentieren, sodass sie ordnungsgemäß klassifiziert und normalisiert werden können.

Automatische Verarbeitung

Eine Option für den Verarbeitungsrhythmus für einen passenden Workflow-Job, die es ermöglicht, ihn automatisch auszuführen, wenn sich Ihre Dateneingabe ändert.

Diese Option ist nur für den regelbasierten Abgleich verfügbar.

Standardmäßig ist der Verarbeitungsrhythmus für einen passenden Workflow-Job auf Manuell festgelegt , sodass er bei Bedarf ausgeführt werden kann. Sie können die automatische Verarbeitung so einrichten, dass Ihr passender Workflow-Job automatisch ausgeführt wird, wenn sich Ihre Dateneingabe ändert. Dadurch bleibt Ihre passende Workflow-Ausgabe auf dem neuesten Stand.

AWS KMS key ARN

Dies ist Ihr AWS KMS Amazon-Ressourcenname (ARN) für die Verschlüsselung im Ruhezustand. Falls nicht angegeben, verwendet das System einen AWS Entity Resolution verwalteten KMS-Schlüssel.

Batch-Arbeitsablauf

Ein Prozess, der in geplanten Intervallen ausgeführt wird, um Daten aus einem gesamten Datensatz abzugleichen und zu lösen. Batch-Workflows in AWS Entity Resolution eignen sich am besten für die Ersteinrichtung, regelmäßige vollständige Aktualisierungen und Szenarien mit erheblichen Änderungen sowohl der Quell- als auch der Zieldatensätze.

Klartext

Daten, die nicht kryptografisch geschützt sind.

Konfidenzniveau () ConfidenceLevel

Für den ML-Abgleich ist dies das Konfidenzniveau, das angewendet wird AWS Entity Resolution , wenn ML einen übereinstimmenden Datensatz identifiziert. Dies ist Teil der passenden Workflow-Metadaten, die in die Ausgabe aufgenommen werden.

Konfidenzniveau aufzeichnen (RecordConfidenceLevel)

Für den inkrementellen ML-Abgleich ist dies das Konfidenzniveau pro Datensatz, das angewendet wird, AWS Entity Resolution wenn ML eine übereinstimmende Datensatzgruppe identifiziert. Dies ist Teil der passenden Workflow-Metadaten, die in die Ausgabe aufgenommen werden.

Entschlüsselung

Der Prozess der Rücktransformation verschlüsselter Daten in ihre ursprüngliche Form. Die Entschlüsselung kann nur durchgeführt werden, wenn Sie Zugriff auf den geheimen Schlüssel haben.

Verschlüsselung

Der Vorgang, bei dem Daten mithilfe eines geheimen Werts, der als Schlüssel bezeichnet wird, in eine zufällig erscheinende Form codiert werden. Ohne Zugriff auf den Schlüssel ist es unmöglich, den ursprünglichen Klartext zu ermitteln.

Gruppenname

Der Gruppenname verweist auf die gesamte Gruppe von Eingabefeldern und kann Ihnen helfen, analysierte Daten zu Vergleichszwecken zu gruppieren.

Wenn es beispielsweise drei Eingabefelder gibt:**`first_name`**, und**`middle_name`**, können Sie sie gruppieren**`last_name`**, indem Sie den Gruppennamen wie **`full_name`** für den Abgleich und die Ausgabe eingeben.

Hash

Hashing bedeutet, dass ein kryptografischer Algorithmus angewendet wird, der eine irreversible und eindeutige Zeichenfolge mit einer festen Größe erzeugt — einen sogenannten Hash. AWS Entity Resolution verwendet das Secure Hash Algorithm 256-Bit-Hash-Protokoll (SHA256) und gibt eine 32-Byte-Zeichenfolge aus. In können Sie wählen AWS Entity Resolution, ob Datenwerte in Ihrer Ausgabe gehasht werden sollen.

Hash-Protokoll (HashingProtocol)

AWS Entity Resolution verwendet das Secure Hash Algorithm 256-Bit-Hash-Protokoll (SHA256) und gibt eine 32-Byte-Zeichenfolge aus. Dies ist Teil der passenden Workflow-Metadaten, die in die Ausgabe aufgenommen werden.

Methode der ID-Zuordnung

Wie die ID-Zuordnung durchgeführt werden soll.

Es gibt zwei Methoden zur ID-Zuordnung:

- Rule-based — Die Methode, mit der Sie Vergleichsregeln verwenden, um Erstanbieterdaten in einem ID-Mapping-Workflow von einer Quelle in ein Ziel zu übersetzen.
- Provider-Dienste — Die Methode, mit der Sie einen Provider-Service verwenden, um in einem ID-Mapping-Workflow von Drittanbietern kodierte Daten von einer Quelle in ein Ziel zu übersetzen.

  AWS Entity Resolution unterstützt derzeit LiveRamp als Provider-Dienste die ID-Zuordnungsmethode. Sie müssen über ein Abonnement für LiveRamp Through verfügen, um diese

AWS Data Exchange Methode verwenden zu können. Weitere Informationen finden Sie unter Schritt 1: Abonnieren Sie einen Anbieterdienst unter AWS Data Exchange.

Arbeitsablauf für die ID-Zuordnung

Ein Datenverarbeitungsauftrag, der Daten aus einer Eingabedatenquelle einem Eingabedatenziel auf der Grundlage der angegebenen ID-Zuordnungsmethode zuordnet. Es erstellt eine ID-Zuordnungstabelle. Für diesen Workflow müssen Sie die ID-Zuordnungsmethode und die Eingabedaten angeben, die Sie von einer Quelle in ein Ziel übersetzen möchten.

Sie können einen ID-Zuordnungs-Workflow einrichten, der in Ihrem eigenen AWS-Konto oder in zwei Arbeitsabläufen ausgeführt wird AWS-Konten.

ID-Namespace

Eine Ressource AWS Entity Resolution , die Metadaten enthält, in denen Datensätze aus mehreren Quellen erklärt werden AWS-Konten und wie diese Datensätze in einem ID-Mapping-Workflow verwendet werden.

Es gibt zwei Arten von ID-Namespaces: und. `SOURCE` `TARGET` Der `SOURCE` enthält Konfigurationen für die Quelldaten, die in einem ID-Zuordnungs-Workflow verarbeitet werden. Das `TARGET` enthält eine Konfiguration der Zieldaten, in die alle Quellen aufgelöst werden. Um die Eingabedaten zu definieren, die Sie in zwei Gruppen auflösen möchten AWS-Konten, erstellen Sie eine ID-Namespace-Quelle und ein ID-Namespace-Ziel, um Ihre Daten von einem Set (`SOURCE`) in ein anderes () zu übersetzen. `TARGET`

Nachdem Sie und ein anderes Mitglied ID-Namespaces erstellt und einen ID-Zuordnungs-Workflow ausgeführt haben, können Sie einer Kollaboration beitreten, AWS Clean Rooms um eine Verknüpfung mehrerer Tabellen in der ID-Zuordnungstabelle auszuführen und die Daten zu analysieren.

Weitere Informationen finden Sie im AWS Clean Rooms -Benutzerhandbuch.

Inkrementeller Arbeitsablauf

Ein Prozess, der nur neue oder aktualisierte Datensätze seit dem letzten Lauf abgleicht und auflöst, anstatt den gesamten Datensatz zu verarbeiten. Inkrementelle Workflows in AWS Entity Resolution

eignen sich am besten für häufige Aktualisierungen, um die Aktualität der Daten aufrechtzuerhalten, wenn sich nur ein kleiner Teil des Datensatzes geändert hat.

Eingabefeld

Ein Eingabefeld entspricht einem Spaltennamen aus Ihrer AWS Glue Eingabedatentabelle.

Eingabequelle ARN (InputSourceARN)

Der Amazon-Ressourcenname (ARN), der für eine AWS Glue Tabelleneingabe generiert wurde. Dies ist Teil der passenden Workflow-Metadaten, die in die Ausgabe aufgenommen werden.

Abgleich auf Grundlage von Machine Learning

Beim maschinellen Lernen (ML-Matching) werden Übereinstimmungen in Ihren Daten gefunden, die möglicherweise unvollständig sind oder nicht exakt gleich aussehen. Beim ML-Abgleich handelt es sich um einen voreingestellten Prozess, bei dem versucht wird, Datensätze aus allen von Ihnen eingegebenen Daten abzugleichen. Beim ML-Abgleich werden eine Übereinstimmungs-ID und ein Konfidenzniveau für jeden übereinstimmenden Datensatz zurückgegeben.

Manuelle Verarbeitung

Eine Option für den Verarbeitungsrhythmus für einen passenden Workflow-Job, mit der dieser bei Bedarf ausgeführt werden kann.

Diese Option ist standardmäßig festgelegt und sowohl für den regelbasierten Abgleich als auch für den auf maschinellem Lernen basierenden Abgleich verfügbar.

Many-to-Many übereinstimmend

Many-to-many Matching vergleicht mehrere Instanzen ähnlicher Daten. Werte in Eingabefeldern, denen derselbe Vergleichsschlüssel zugewiesen wurde, werden miteinander verglichen, unabhängig davon, ob sie sich im selben Eingabefeld oder in unterschiedlichen Eingabefeldern befinden.

Beispielsweise könnten Sie mehrere Eingabefelder für Telefonnummern wie `mobile_phone` und `home_phone` mit demselben Vergleichsschlüssel „Telefon“ haben. Verwenden Sie den Viele-zu-

Viele-Abgleich, um Daten im `mobile_phone` Eingabefeld mit Daten im `mobile_phone` Eingabefeld und Daten im `home_phone` Eingabefeld zu vergleichen.

Vergleichsregeln werten Daten in mehreren Eingabefeldern mit demselben Vergleichsschlüssel mithilfe einer (ODER) -Operation aus, und beim Eins-zu-Viele-Vergleich werden Werte in mehreren Eingabefeldern verglichen. Das bedeutet, dass, wenn eine Kombination aus `mobile_phone` oder zwischen zwei Datensätzen `home_phone` übereinstimmt, der Vergleichsschlüssel „Telefon“ einen Treffer zurückgibt. Für die Vergleichstaste „Telefon“, um eine Übereinstimmung zu finden, `Record One mobile_phone = Record Two mobile_phone` ODER `Record One mobile_phone = Record Two home_phone` ODER `Record One home_phone = Record Two home_phone` ODER`Record One home_phone = Record Two mobile_phone`.

Spiel-ID (MatchID)

Bei regelbasiertem Abgleich und ML-Abgleich ist dies die ID, die von jedem übereinstimmenden Datensatz generiert AWS Entity Resolution und auf ihn angewendet wird. Dies ist Teil der passenden Workflow-Metadaten, die in die Ausgabe aufgenommen werden.

Schlüssel abgleichen (MatchKey)

Der Abgleichschlüssel gibt an AWS Entity Resolution , welche Eingabefelder als ähnliche Daten und welche als unterschiedliche Daten betrachtet werden sollen. Dies hilft dabei, AWS Entity Resolution automatisch regelbasierte Abgleichsregeln zu konfigurieren und ähnliche Daten zu vergleichen, die in verschiedenen Eingabefeldern gespeichert sind.

Wenn Ihre Daten mehrere Arten von Telefonnummerninformationen wie ein `mobile_phone` Eingabefeld und ein `home_phone` Eingabefeld enthalten, die Sie miteinander vergleichen möchten, können Sie beiden den Vergleichsschlüssel „Telefon“ geben. Dann kann der regelbasierte Abgleich so konfiguriert werden, dass Daten mithilfe von „oder“ -Anweisungen in allen Eingabefeldern mit dem One-to-One Abgleichschlüssel „Telefon“ verglichen werden (siehe Abgleichen und Abgleichen von Definitionen im Abschnitt Many-to-Many Abgleichen von Arbeitsabläufen).

Wenn Sie möchten, dass beim regelbasierten Abgleich verschiedene Arten von Telefonnummerninformationen völlig getrennt betrachtet werden, können Sie spezifischere Vergleichsschlüssel wie „Mobile_Phone“ und „“ erstellen. Home_Phone Wenn Sie dann einen Abgleichsworkflow einrichten, können Sie angeben, wie die einzelnen Telefonabgleichsschlüssel beim regelbasierten Abgleich verwendet werden sollen.

Wenn für ein bestimmtes Eingabefeld „Nein“ angegeben MatchKey ist, kann es nicht für den Abgleich verwendet werden. Es kann jedoch den passenden Workflow-Prozess durchlaufen und bei Bedarf ausgegeben werden.

Name des Abgleichsschlüssels

Der Name, der einem Match-Schlüssel zugewiesen ist.

Regel abgleichen (MatchRule)

Bei regelbasiertem Abgleich ist dies die angewendete Regelnummer, die eine übereinstimmende Datensatzgruppe generiert hat. Dies ist Teil der passenden Workflow-Metadaten, die in die Ausgabe aufgenommen werden.

Übereinstimmung

Der Prozess, bei dem Daten aus verschiedenen Eingabefeldern, Tabellen oder Datenbanken kombiniert und verglichen werden und anhand der Erfüllung bestimmter Abgleichskriterien (z. B. durch Vergleichsregeln oder Modelle) bestimmt wird, welche davon ähnlich sind — oder „übereinstimmen“.

Passender Arbeitsablauf

Der Prozess, den Sie eingerichtet haben, um die Eingabedaten anzugeben, die miteinander verglichen werden sollen, und die Art und Weise, wie der Abgleich durchgeführt werden soll.

Passende Workflow-Beschreibung

Eine optionale Beschreibung des passenden Workflows, den Sie eingeben können. Beschreibungen helfen Ihnen dabei, zwischen passenden Workflows zu unterscheiden, wenn Sie mehr als einen erstellen.

Passender Workflow-Name

Der Name für den passenden Workflow, den Sie angeben.

> **Note**
>
> Passende Workflow-Namen müssen eindeutig sein. Sie dürfen nicht denselben Namen haben, da sonst ein Fehler zurückgegeben wird.

Passende Workflow-Metadaten

Informationen, die AWS Entity Resolution während eines passenden Workflow-Jobs generiert und ausgegeben wurden. Diese Information ist bei der Ausgabe erforderlich.

Normalisierung () ApplyNormalization

Wählen Sie, ob die Eingabedaten wie im Schema definiert normalisiert werden sollen. Bei der Normalisierung werden Daten standardisiert, indem zusätzliche Leerzeichen und Sonderzeichen entfernt und das Format auf Kleinbuchstaben standardisiert wird.

Wenn ein Eingabefeld beispielsweise den Attributtyp Vollständige Telefonnummer hat und die Werte in der Eingabetabelle als formatiert sind`(123) 456-7890`, AWS Entity Resolution werden die Werte auf normalisiert. `1234567890`

> **Note**
>
> Die Normalisierung wird nur für den Gruppentyp für Name, Adresse , Telefon und E-Mail unterstützt.

In den folgenden Abschnitten werden unsere Standardregeln für die Normalisierung beschrieben.

Informationen zum speziellen ML-based Abgleich finden Sie unterNormalisierung () — nur ApplyNormalization ML-based.

Themen

- Name
- Email
- Phone
- Adresse
- Gehasht

- Source_ID

Name

> **Note**
>
> Die Normalisierung wird nur für den Gruppentyp Name unterstützt.
> Der Gruppentyp Name wird in der Konsole und wie in der API als `NAME` Vollständiger Name angezeigt.
> Wenn Sie die Untertypen des Gruppentyps Name normalisieren möchten, gehen Sie wie folgt vor:
>
> - Weisen Sie in der Konsole der Gruppe „Vollständiger Name“ die folgenden Untertypen zu: Vorname, Zweiter Vorname und Nachname.
> - Weisen Sie der `NAME` GroupName in der CreateSchemaMapping API die folgenden Typen zu: `NAME_FIRSTNAME_MIDDLE`, und. `NAME_LAST`

- TRIM = Schneidet führende und nachfolgende Leerzeichen ab
- LOWERCASE = Alle Alphazeichen werden in Kleinbuchstaben geschrieben
- CONVERT_ACCENT = Wandelt Buchstaben mit Akzent in normale Buchstaben um
- REMOVE_ALL_NON_ALPHA = Entfernt alle Nicht-Alpha-Zeichen [a-z] A-Z

Email

> **Note**
>
> Die Normalisierung wird für den Gruppentyp E-Mail unterstützt.
> Der Gruppentyp E-Mail wird in der Konsole als E-Mail-Adresse und `EMAIL_ADDRESS` in der API angezeigt.

- TRIM = Schneidet führende und nachfolgende Leerzeichen ab
- LOWERCASE = Alle Alphazeichen werden in Kleinbuchstaben geschrieben
- CONVERT_ACCENT = Wandelt Buchstaben mit Akzent in normale Buchstaben um

- EMAIL_ADDRESS_UTIL_NORM = Entfernt alle Punkte (.) aus dem Nutzernamen, entfernt alles, was nach einem Pluszeichen (+) im Nutzernamen steht, und standardisiert gängige Domainvarianten
- REMOVE_ALL_NON_EMAIL_CHARS = Entfernt alle nicht-alphanumerischen Zeichen [a-z] und [.@ -] A-Z0-9

Phone

> **Note**
>
> Die Normalisierung wird nur für den Gruppentyp Telefon unterstützt.
> Der Gruppentyp Telefon wird in der Konsole und wie **`PHONE`** in der API als Vollständige Telefonnummer angezeigt.
> Wenn Sie die Untertypen des Gruppentyps Telefon normalisieren möchten, gehen Sie wie folgt vor:
>
> - Weisen Sie in der Konsole der vollständigen Telefongruppe die folgenden Untertypen zu: Telefonnummer und Telefonvorwahl.
> - Weisen Sie in der CreateSchemaMapping API dem `PHONE` GroupName die folgenden Typen zu: `PHONE_NUMBER` und. `PHONE_COUNTRYCODE`

- TRIM = Schneidet führende und nachfolgende Leerzeichen ab
- REMOVE_ALL_NON_NUMERIC = Entfernt alle nicht numerischen Zeichen [0-9]
- REMOVE_ALL_LEADING_ZEROES = Entfernt alle führenden Nullen
- ENSURE_PREFIX_WITH_MAP, „phone" = Überprüft jede Telefonnummer und versucht, sie mit den Mustern im Telefon abzugleichen. PrefixMap PrefixMap Wenn eine Übereinstimmung gefunden wird, fügt die Regel das Präfix der Telefonnummer hinzu oder ändert es, um sicherzustellen, dass es dem in der Karte angegebenen standardisierten Format entspricht.

Adresse

> **Note**
>
> Die Normalisierung wird nur für den Gruppentyp „Adresse“ unterstützt.

Der Adressgruppentyp wird in der Konsole und wie **`ADDRESS`** in der API als Vollständige Adresse angezeigt.
Gehen Sie wie folgt vor, wenn Sie die Untertypen des Adressgruppentyps normalisieren möchten:

- Weisen Sie in der Konsole der vollständigen Adressgruppe die folgenden Untertypen zu: Straße 1, Straße 2: Straße 3, Name der Stadt, Bundesland , Land und Postleitzahl t
- Weisen Sie dem `ADDRESS` GroupName in der CreateSchemaMapping API die folgenden Typen zu:`ADDRESS_STREET1`,`ADDRESS_STREET2`,`ADDRESS_STREET3`, `ADDRESS_CITY` `ADDRESS_STATE``ADDRESS_COUNTRY`, und. `ADDRESS_POSTALCODE`

- TRIM = Schneidet führende und nachfolgende Leerzeichen ab
- LOWERCASE = Alle Alphazeichen werden in Kleinbuchstaben geschrieben
- CONVERT_ACCENT = Wandelt Buchstaben mit Akzent in normale Buchstaben um
- REMOVE_ALL_NON_ALPHA = Entfernt alle Nicht-Alpha-Zeichen [a-z] A-Z
- RAME_WORDS mit ADDRESS_RAME_WORD_MAP = ersetzt Wörter in der Adresszeichenfolge durch Wörter aus ADDRESS_RAME_WORD_MAP ???
- RAME_DELIMITERS mit ADDRESS_RAME_DELIMITER_MAP = Ersetze die Trennzeichen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_RAME_DELIMITER_MAP
- RAME_DIRECTIONS mit ADDRESS_RAME_DIRECTION_MAP = Ersetze die Trennzeichen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_RAME_DIRECTION_MAP ???
- RAME_NUMBERS mit ADDRESS_RAME_NUMBER_MAP = ersetzt Zahlen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_RAME_NUMBER_MAP
- RAME_SPECIAL_CHARS mit ADDRESS_RAME_SPECIAL_CHAR_MAP = Ersetze Sonderzeichen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_RAME_SPECIAL_CHAR_MAP

ADDRESS_RENAME_WORD_MAP

Dies sind die Wörter, die bei der Normalisierung der Adresszeichenfolge umbenannt werden.

```
"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"
```

ADDRESS_RENAME_DELIMITER_MAP

Dies sind die Trennzeichen, die bei der Normalisierung der Adresszeichenfolge umbenannt werden.

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

ADDRESS_RENAME_DIRECTION_MAP

Dies sind die Richtungskennungen, die bei der Normalisierung der Adresszeichenfolge umbenannt werden.

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

ADDRESS_RENAME_NUMBER_MAP

Dies sind die Zahlenzeichenfolgen, die bei der Normalisierung der Adresszeichenfolge umbenannt werden.

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

ADDRESS_RENAME_SPECIAL_CHAR_MAP

Dies ist die Zeichenfolge mit Sonderzeichen, die bei der Normalisierung der Adresszeichenfolge umbenannt wird.

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

Gehasht

- TRIM = Schneidet führende und nachfolgende Leerzeichen ab

Source_ID

- TRIM = Schneidet Leerzeichen am Anfang und am Ende ab

Normalisierung () — nur ApplyNormalization ML-based

Wählen Sie, ob die Eingabedaten wie im Schema definiert normalisiert werden sollen. Bei der Normalisierung werden Daten standardisiert, indem zusätzliche Leerzeichen und Sonderzeichen entfernt und das Format auf Kleinbuchstaben standardisiert wird.

Wenn ein Eingabefeld beispielsweise den Attributtyp hat und die Werte in der `NAME` Eingabetabelle als formatiert sind`Johns  Smith`, AWS Entity Resolution werden die Werte auf normalisiert. `john smith`

In den folgenden Abschnitten werden die Normalisierungsregeln für Matching-Workflows beschrieben, die auf maschinellem Lernen basieren.

Themen

- Name
- Email
- Phone

Name

- TRIM = Schneidet führende und nachfolgende Leerzeichen ab
- LOWERCASE = Alle Alphazeichen werden in Kleinbuchstaben geschrieben

Email

- LOWERCASE = Alle Alphazeichen werden in Kleinbuchstaben geschrieben
- Ersetzt nur (at) (Groß- und Kleinschreibung beachten) durch ein @-Symbol
- Entfernt alle Leerzeichen an einer beliebigen Stelle im Wert
- Entfernt alles, was sich außerhalb des ersten befindet, `"< >"` falls es existiert

Phone

- TRIM = Schneidet führende und nachfolgende Leerzeichen ab
- REMOVE_ALL_NON_NUMERIC = Entfernt alle nicht numerischen Zeichen [0-9]
- REMOVE_ALL_LEADING_ZEROES = Entfernt alle führenden Nullen

- ENSURE_PREFIX_WITH_MAP, „phone" = Überprüft jede Telefonnummer und versucht, sie mit den Mustern im Telefon abzugleichen. PrefixMap PrefixMap Wenn eine Übereinstimmung gefunden wird, fügt die Regel das Präfix der Telefonnummer hinzu oder ändert es, um sicherzustellen, dass es dem in der Karte angegebenen standardisierten Format entspricht.

One-to-One übereinstimmend

One-to-one Matching vergleicht einzelne Instanzen ähnlicher Daten. Eingabefelder mit demselben Vergleichsschlüssel und Werten in demselben Eingabefeld werden miteinander verglichen.

Beispielsweise könnten Sie mehrere Eingabefelder für Telefonnummern wie `mobile_phone` und `home_phone` haben denselben Vergleichsschlüssel „Telefon“. Verwenden Sie den Eins-zu-Eins-Abgleich, um Daten im `mobile_phone` Eingabefeld mit Daten im `mobile_phone` Eingabefeld zu vergleichen und um Daten im `home_phone` Eingabefeld mit Daten im `home_phone` Eingabefeld zu vergleichen. Die Daten im `mobile_phone` Eingabefeld werden nicht mit den Daten im `home_phone` Eingabefeld verglichen.

Vergleichsregeln werten Daten in mehreren Eingabefeldern mit demselben Vergleichsschlüssel mithilfe einer (ODER) -Operation aus, und beim Eins-zu-Viele-Abgleich werden Werte in einem einzelnen Eingabefeld verglichen. Das heißt, wenn `mobile_phone` oder zwischen zwei Datensätzen `home_phone` übereinstimmt, gibt der Vergleichsschlüssel „Telefon“ einen Treffer zurück. Für die Suchtaste „Telefon“, um eine Übereinstimmung zu finden, `Record One mobile_phone = Record Two mobile_phone` ODER`Record One home_phone = Record Two home_phone`.

Vergleichsregeln werten Daten in Eingabefeldern mit unterschiedlichen Vergleichstasten mit einer (und) -Operation aus. Wenn Sie möchten, dass beim regelbasierten Abgleich verschiedene Arten von Telefonnummerninformationen völlig getrennt betrachtet werden, können Sie spezifischere Vergleichsschlüssel wie „mobile_phone“ und „home_phone“ erstellen. Wenn Sie beide Vergleichstasten in einer Regel verwenden möchten, um Übereinstimmungen zu finden, UND. `Record One mobile_phone = Record Two mobile_phone` `Record One home_phone = Record Two home_phone`

Ausgabe

Eine Liste von OutputAttribute Objekten, von denen jedes die Felder Name und Hashed hat. Jedes dieser Objekte steht für eine Spalte, die in die AWS Glue Ausgabetabelle aufgenommen werden soll, und gibt an, ob die Werte in der Spalte gehasht werden sollen.

Gibt S3Path aus

Das S3-Ziel, in das die AWS Entity Resolution Ausgabetabelle geschrieben wird.

OutputSourceConfig

Eine Liste von OutputSource Objekten, von denen jedes die Felder Outputs3Path und Output enthält. ApplyNormalization

Abgleich auf Basis des Provider-Dienstes

Beim Anbieterservice-basierten Abgleich werden Ihre Datensätze mit bevorzugten Datendienstanbietern und lizenzierten Datensätzen abgeglichen, verknüpft und erweitert. Sie müssen über ein Abonnement beim Anbieterdienst AWS Data Exchange verfügen, um diese Matching-Technik verwenden zu können.

AWS Entity Resolution ist derzeit in die folgenden Datendienstanbieter integriert:

- LiveRamp
- TransUnion
- UID 2.0

Rule-based übereinstimmend

Rule-based Matching ist ein Prozess, der entwickelt wurde, um genaue Übereinstimmungen zu finden. Rule-based Beim Abgleichen handelt es sich um einen hierarchischen Satz von Regeln für den Wasserfallvergleich, der von Ihnen vorgeschlagen wird AWS Entity Resolution, auf der Grundlage der von Ihnen eingegebenen Daten und vollständig von Ihnen konfigurierbar ist. Alle in den Regelkriterien angegebenen Vergleichsschlüssel müssen exakt übereinstimmen, damit verglichene Daten als Treffer deklariert und die zugehörigen Metadaten ausgegeben werden können. Rule-based matching gibt eine Match-ID und eine Regelnummer für jeden übereinstimmenden Datensatz zurück.

Wir empfehlen, Regeln zu definieren, mit denen eine Entität eindeutig identifiziert werden kann. Ordnen Sie Ihre Regeln so an, dass Sie zuerst genauere Treffer finden.

Nehmen wir zum Beispiel an, Sie haben zwei Regeln, Regel 1 und Regel 2.

Diese Regeln haben die folgenden Vergleichsschlüssel:

- Regel 1 beinhaltet den vollständigen Namen und die Adresse
- Regel 2 beinhaltet den vollständigen Namen, die Adresse und die Telefonnummer

Da Regel 1 zuerst ausgeführt wird, werden nach Regel 2 keine Treffer gefunden, da nach Regel 1 alle Treffer gefunden worden wären.

Ordnen Sie die Regeln wie folgt neu an, um Übereinstimmungen zu finden, die nach Telefonnummer unterschieden werden:

- Regel 2 beinhaltet den vollständigen Namen, die Adresse und die Telefonnummer
- Regel 1 beinhaltet den vollständigen Namen und die Adresse

Transitiver Abgleich

Transitiver Abgleich ist eine optionale Funktion für regelbasierte Matching-Workflows, die den Regeltyp „Erweitert“ verwenden. AWS Entity Resolution Verwendet standardmäßig einen Wasserfallabgleich, bei dem Datensätze, die auf einer höheren Regelebene übereinstimmen, von nachfolgenden Regeln ausgeschlossen werden. Wenn der transitive Abgleich aktiviert ist, werden alle Datensätze auf allen Regelebenen verarbeitet. Die Übereinstimmungs-ID eines Datensatzes wird bei seinem ersten Treffer festgelegt, aber der Datensatz fungiert weiterhin als Link, um Datensätze, die nicht übereinstimmen, aus späteren Regeln mit Übereinstimmungsgruppen aus früheren Regeln zu verbinden.

Weitere Informationen finden Sie unter Verwendung von transitivem Matching.

Schema

Der Begriff, der für eine Struktur oder ein Layout verwendet wird, das definiert, wie ein Datensatz organisiert und verknüpft ist.

Beschreibung des Schemas

Eine optionale Beschreibung des Schemas, die Sie eingeben können. Beschreibungen helfen Ihnen dabei, zwischen Schemazuordnungen zu unterscheiden, wenn Sie mehrere erstellen.

Name des Schemas

Der Name des Schemas.

> **Note**
>
> Schemanamen müssen eindeutig sein. Sie dürfen nicht denselben Namen haben, da sonst ein Fehler zurückgegeben wird.

Schema-Zuordnung

Schema-Mapping AWS Entity Resolution ist der Prozess, bei dem Sie angeben, AWS Entity Resolution wie Ihre Daten für den Abgleich zu interpretieren sind. Sie definieren das Schema der Eingabedatentabelle, das Sie in einen passenden Workflow einlesen möchten AWS Entity Resolution .

ARN für Schemazuordnung

Der Amazon-Ressourcenname (ARN), der für die Schemazuordnung generiert wurde.

Eindeutige ID

Eine eindeutige Kennung, die Sie angeben und die jeder Zeile mit Eingabedaten zugewiesen werden muss, die AWS Entity Resolution gelesen wird.

Example

Beispiel: **`Primary_key`**, **`Row_ID`** oder **`Record_ID`**.

Die Spalte Eindeutige ID ist erforderlich.

Die eindeutige ID muss ein eindeutiger Bezeichner innerhalb einer einzelnen Tabelle sein.

Die eindeutige ID muss diesem Muster entsprechen: `[a-zA-Z0-9_-]`

In verschiedenen Tabellen kann die eindeutige ID doppelte Werte enthalten.

Die maximale Länge der eindeutigen ID beträgt 38 für einen passenden Workflow

Die maximale Länge einer eindeutigen ID beträgt 257 Zeichen für eine Arbeitsablauf für die ID-Zuordnung

Wenn der Matching-Workflow ausgeführt wird, wird der Datensatz abgelehnt, wenn die eindeutige ID:

- ist nicht angegeben
- ist innerhalb derselben Tabelle nicht eindeutig
- überschneidet sich in Bezug auf den Attributnamen zwischen den Quellen
- überschreitet 38 Zeichen (nur regelbasierte Matching-Workflows)

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.