User Guide

AWS Entity Resolution

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

AWS Entity Resolution: User Guide

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

Die Handelsmarken und 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?

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 Abgleichstechniken wie regelbasierten Abgleich, auf maschinellem Lernen basierenden Abgleich (ML-Matching) und von Datendienstanbietern gesteuerter Abgleich. 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 verwenden (z. B.UPC)SKU, in Ihren Geschäften besser nachverfolgen. Sie können AWS Entity Resolution damit die Genauigkeit der Zuordnung kontrollieren, die Datensicherheit besser schützen und gleichzeitig die Datenbewegung minimieren.

Themen

Sind Sie ein Erstanwender? AWS Entity Resolution

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

- 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 Zuordnungsverarbeitung zu verbessern, z. B. durch 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.

  - R eady-to-use regelbasierter Abgleich

    Diese Vergleichstechnik beinhaltet eine Reihe von ready-to-use Regeln im AWS Management Console 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 zurücksetzen, um sie auf ihre ursprüngliche Konfiguration zurückzusetzen. Die in Ihrem Amazon Simple Storage Service (Amazon S3) -Bucket ausgegebenen Daten enthalten Übereinstimmungsgruppen, die mithilfe der regelbasierten Abgleichstechnik 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, auf maschinellem Lernen basierender Abgleich (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.

- Abgleich von Datensätzen mit Datendienstanbietern

  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 von API und AWS Management Console oder können Sie bei Bedarf eine manuelle Massenverarbeitung auf der Grundlage Ihrer vorhandenen Datenpipeline zum Extrahieren, Transformieren und Laden (ETL) ausführen, die alle Daten für neue Treffer und Aktualisierungen vorhandener Treffer erneut verarbeitet. AWS CLI 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 während des AWS Entity Resolution GetMatchId APIVorgangs nach beliebigen Entitätsfeldern suchen, können Sie eine vorhandene Match-ID synchron abrufen. Sie können AWS Entity Resolution mit Attributen für persönlich identifizierbare Informationen (PII) anrufen, die über verschiedene Quellen und Kanäle erfasst wurden. AWS Entity Resolution verwendet aus Datenschutzgründen einen Hashwert für diese Attribute 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 in Ihrem S3-Bucket gespeicherten übereinstimmenden Ergebnissen 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 importieren, AWS Entity Resolution in Amazon S3.

  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.

- AWS CloudFormation

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

  Weitere Informationen finden Sie unter Ressourcen zur AWS Entitätsauflösung erstellen 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 Developer Guide:
    - 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

Bevor du es verwendest AWS Entity Resolution melden Sie sich zum ersten Mal an für AWS und erstellen Sie einen Administratorbenutzer, um Rollen zu erstellen.

Melden Sie sich an für AWS

Wenn Sie bereits eine haben AWS-Konto, überspringe diesen Schritt.

Wenn Sie keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um einen zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, ein Root-Benutzer des AWS-Kontoswird erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen im Konto. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Einen Administratorbenutzer erstellen

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
Im IAM Identity Center (Empfohlen)	Verwenden Sie kurzfristige Zugangsdaten für den Zugriff AWS. Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch.	Folgen Sie den Anweisungen unter Erste Schritte im AWS IAM Identity Center Benutzerleitfaden.	Konfigurieren Sie den programmatischen Zugriff, indem Sie AWS CLI zu verwenden AWS IAM Identity Center in der AWS Command Line Interface Benutzerleitfaden.
In IAM (Nicht empfohlen)	Verwenden Sie langfristige Anmeldeinformationen für den Zugriff AWS.	Folgen Sie den Anweisungen unter Erstellen Ihres ersten IAM Admin-Benutzers und Ihrer ersten Administrator-Benutzergruppe im IAMBenutzerhandbuch.	Konfigurieren Sie den programmatischen Zugriff, indem Sie im Benutzerhandbuch die Zugriffsschlüssel für IAM IAM Benutzer verwalten.

Eine IAM Rolle für einen Konsolenbenutzer erstellen

Führen Sie das folgende Verfahren aus, wenn Sie das verwenden AWS Entity Resolution console.

So erstellen Sie eine IAM-Rolle

1. Melden Sie sich mit Ihrem Administratorkonto an 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.
4. Wählen Sie im Assistenten zum Erstellen von Rollen unter Vertrauenswürdiger Entitätstyp 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 JSONRegisterkarte 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: Stichwörter aus, fügen Sie Stichwörter 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 Create Policy (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 AWS-Konto für die Person oder Personen, 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.

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.
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.

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

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "entityresolution.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

6. Wählen Sie Weiter.
7. Wählen Sie unter 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 AWS Glue. Je nachdem, wie Sie Ihre Datenquellen eingerichtet haben, müssen Sie diese Richtlinie jedoch möglicherweise ändern.
> Ihre AWS Glue Ressourcen und zugrunde liegende Amazon S3 S3-Ressourcen müssen sich im selben Verzeichnis befinden AWS-Region als AWS Entity Resolution.
> Du musst nicht gewähren AWS KMS Berechtigungen, wenn Ihre Datenquellen nicht ver- oder entschlüsselt sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
```

```
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{input-buckets}}",
                "arn:aws:s3:::{{input-buckets}}/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "{{accountId}}"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{output-bucket}}",
                "arn:aws:s3:::{{output-bucket}}/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "{{accountId}}"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:GetSchema",
                "glue:GetSchemaVersion",
                "glue:BatchGetPartition"
            ],
```

```
            "Resource": [
                "arn:aws:glue:{{aws-region}}:{{accountId}}:database/{{input-
databases}}",
                "arn:aws:glue:{{aws-region}}:{{accountId}}:table/{{input-
database}}/{{input-tables}}",
                "arn:aws:glue:{{aws-region}}:{{accountId}}:catalog"
            ]
        }
    ]
}
```

Ersetze jedes *{{user input placeholder}}* mit Ihren eigenen Informationen.

aws-region	AWS-Region Ihrer Ressourcen. Ihre AWS Glue Ressourcen, zugrunde liegende Amazon S3 S3-Ressourcen und AWS KMS Ressourcen müssen sich im selben Verzeichnis befinden AWS-Region alsAWS Entity Resolution .
accountId	Ihre AWS-Konto ID.
input-buckets	Amazon S3 S3-Buckets, die die zugrunde liegenden Datenobjekte von enthalten AWS Glue von wo aus gelesen AWS Entity Resolution wird.
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 Kundenschlüssel verschlüsselt ist, fügen Sie Folgendes hinzu:

```
        {
            "Effect": "Allow",
```

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

Ersetzen Sie jeden *{{user input placeholder}}* mit Ihren eigenen Informationen.

aws-region	AWS-Region Ihrer Ressourcen. Ihre AWS Glue Ressourcen, zugrunde liegende Amazon S3 S3-Ressourcen und AWS KMS Ressourcen müssen sich im selben Verzeichnis befinden AWS-Region alsAWS Entity Resolution .
accountId	Ihre AWS-Konto ID.
inputKeys	Verwaltete Schlüssel in 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}}:{{accountId}}:key/{{outputKeys}}"
            ]
        }
```

Ersetzen Sie jeden *{{user input placeholder}}* mit Ihren eigenen Informationen.

aws-region	AWS-Region Ihrer Ressourcen. Ihre AWS Glue Ressourcen, zugrunde liegende Amazon S3 S3-Ressourcen und AWS KMS Ressourcen müssen sich im selben Verzeichnis befinden AWS-Region alsAWS Entity Resolution .
accountId	Ihre AWS-Konto ID.
outputKeys	Verwaltete Schlüssel in 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 ein Abonnement bei einem Dienstanbieter abgeschlossen haben AWS Data Exchange, und Sie möchten eine bestehende Rolle für einen auf Providerdiensten basierenden Workflow verwenden, 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 jedes *{{user input placeholder}}* mit Ihren eigenen Informationen.

aws-region	Das Tool AWS-Region wo die Provider-Ressource gewährt wird. Sie finden diesen Wert im Asset ARN auf der AWS Data Exchange console. Zum Beispiel: `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
datasetId	Die ID des Datensatzes, gefunden auf AWS Data Exchange console.
revisionId	Die Revision des Datensatzes, gefunden auf AWS Data Exchange console.
assetId	Die ID des Assets, gefunden auf AWS Data Exchange console.

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.

Die Workflow-Jobrolle für AWS Entity Resolution wurde erstellt.

Eingabedatentabellen vorbereiten

In AWS Entity Resolution, jede Ihrer Eingabedatentabellen enthält 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 verfügbar AWS Glue von Amazon S3 unterstützte Tabelle. 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 eine AWS Glue Crawler zum Erstellen einer Datentabelle in AWS Glue Data Catalog. Sie können die Datentabelle dann als Eingabe verwenden für 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

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: 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.

Zur Verwendung 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 2: 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**
>
> Die Eingabedaten müssen in Amazon Simple Storage Service (Amazon S3) im selben AWS-Konto and AWS-Region in dem Sie den passenden Workflow ausführen möchten.

So laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch

1. Melden Sie sich bei der an AWS Management Console 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 3: Erstellen Sie ein AWS Glue Tabelle

Die Eingabedaten in Amazon S3 müssen katalogisiert sein AWS Glue und dargestellt als AWS Glue Tabelle. Für weitere Informationen zum Erstellen einer AWS Glue Tabelle mit Amazon S3 als Eingabe, siehe Arbeiten mit Crawlern auf der AWS Glue Konsole in der AWS Glue Entwicklerhandbuch.

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

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

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

Um ein zu erstellen AWS Glue Tabelle

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Glue Konsole bei 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 „IAMRolle auswählen“ die Option Vorhandene IAM Rolle auswählen aus und klicken Sie dann auf Weiter.

   Sie können auch „IAMRolle erstellen“ wählen oder die IAM Rolle bei Bedarf von Ihrem Administrator erstellen lassen.
7. Behalten Sie für „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 Folgendes ein AWS Glue Datenbank und wählen Sie dann Weiter.
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 nicht mehr ausgeführt wurde, klicken Sie auf AWS Glue Wählen Sie in der 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.

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

c. Notieren Sie sich die AWS Glue Datenbankname und AWS Glue Tabellenname.

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

Eingabedaten von Drittanbietern werden vorbereitet

Datendienste von Drittanbietern stellen Kennungen bereit, die Ihren bekannten Kennungen zugeordnet werden können.

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

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 Einzelperson und Haushalt IDs
Einheitliche ID 2.0	USA Ost (Nord-Virginia) (us-east-1), USA Ost (Ohio) (us-east-2) und USA West (Oregon) (US-West-2)	Auslosung 2 UID

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

Wenn Sie ein Abonnement bei einem Anbieterdienst haben über AWS Data Exchange, können Sie einen Abgleichsworkflow mit einem der folgenden Anbieterdienste ausführen, um Ihre bekannten Kennungen Ihrem bevorzugten Anbieter zuzuordnen. 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 an unter AWS Data Exchange. Die folgenden Anbieterlisten sind verfügbar:

   - LiveRamp
     - LiveRampAuflösung der Identität
     - LiveRampTranscodierung
   - TransUnion
     - TransUnion TruAudience Identitätsauflösung und -anreicherung ohne Übertragung
     - TransUnion TruAudience Identitätslösung ohne Übertragung
   - 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 in der AWS Data Exchange Benutzeranleitung zur Annahme eines privaten Angebots am AWS Data Exchange.
   - Bringen Sie Ihr eigenes Abonnement mit — Wenn Sie bereits ein Datenabonnement bei einem Anbieter haben, folgen Sie den Anweisungen für Angebote zum Mitbringen Ihres eigenen Abonnements (BYOS) in der AWS Data Exchange Benutzeranleitung zur Annahme eines BYOS Angebots für AWS Data Exchange.

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

Weitere Informationen zum Zugriff auf ein Anbieterprodukt, das Folgendes enthältAPIs, finden Sie unter Zugreifen auf ein API Produkt im AWS Data Exchange Benutzerleitfaden.

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 zur Formatierung von Eingabedateien für den Abgleichs-Workflow finden Sie ADX in der LiveRamp Dokumentation unter Perform Identity Resolution Through. Weitere Informationen zu den Richtlinien zur Formatierung von Eingabedateien für den Workflow zur ID-Zuordnung finden Sie ADX in der LiveRamp Dokumentation unter Durchführen der Transcodierung durch.

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen

TransUnion	Ja	Stellen Sie Folgendes sicher:
		• Für die TransUnion Datenanreicherung ist eine eindeutige ID vorhanden.
		Note
		Weitergabeattribute dürfen bei der Eingabe und Ausgabe an beibehalten werden. TransUnion Haushalts-E-Schlüssel und HHID sind spezifisch für den Client-Na mespace.
		• **`Phone number`** sollte aus 10 Ziffern bestehen, ohne Sonderzeichen wie Leerzeichen oder Bindestriche.
		• **`Addresses`** sollte aufgeteilt werden in
		  • eine einzelne Adresszeile (kombinie ren Sie die Adresszeilen 1 und 2, falls vorhanden)
		  • city
		  • zip (oder zip plus4), ohne Sonderzeichen wie Leerzeichen oder Bindestriche
		  • Bundesland, angegeben als 2-Buchsta ben-Code 3
		• **`Email addresses`** sollte im Klartext sein.
		• **`First Name`**kann in Klein- oder Großbuchstaben geschrieben werden, Spitznamen werden unterstützt, Titel und Suffixe sollten jedoch ausgeschlossen werden.

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen
		• **`Last Name`**können Klein- oder Großbuchstaben sein, mittlere Initialen sollen ausgeschlossen werden.

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen
Vereinheitlichte ID 2.0	Ja	Stellen Sie Folgendes sicher: • Die eindeutige ID darf kein Hash sein. • UID2unterstützt sowohl E-Mail als auch Telefonnummer für die UID2 Generieru ng. 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 Telefonnu mmer. Wenn Ihre Daten eine Mischung aus E-Mails und Telefonnummern enthalten und Sie diese doppelte Anzahl von Datensätz en in der Ausgabe vermeiden möchten, ist es am besten, für jeden einen eigenen Workflow mit separaten Schemazuo rdnungen zu erstellen. Führen Sie in diesem Szenario die Schritte zweimal durch: Erstellen Sie einen Workflow für E-Mails und einen separaten für Telefonnu mmern. **Note** Eine bestimmte E-Mail oder Telefonnu mmer zu einem bestimmten Zeitpunkt führt zu demselben UID2 Rohwert, unabhängig davon, wer die Anfrage gestellt hat. Rohsalze UID2s werden durch Zugabe von Salzen aus Salzkübel n gewonnen, die etwa einmal pro

Service für Anbieter	Eindeutige ID erforderlich?	Aktionen
		Jahr rotiert werden, sodass auch der Rohstoff UID2 mitgerissen wird. Die Salzkübel wechseln im Laufe des Jahres zu unterschiedlichen Zeiten. AWS Entity Resolution verfolgt derzeit nicht den Wechsel zwischen Salzkübeln und Rohsalz. Es wird daher empfohlenUID2s, den Rohsalz täglich zu regenerieren. UID2s Weitere Informationen finden Sie unter Wie oft sollte bei UID2s inkrementellen Updates aktualisiert werden? in der UID 2.0-Dokumentation.

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.

Zur Verwendung 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 CSV nur 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**
>
> Die Eingabedaten müssen in Amazon Simple Storage Service (Amazon S3) im selben AWS-Konto and AWS-Region in dem Sie den passenden Workflow ausführen möchten.

So laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch

1. Melden Sie sich bei der an AWS Management Console 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 sein AWS Glue und dargestellt als AWS Glue Tabelle. Für weitere Informationen zum Erstellen einer AWS Glue Tabelle mit Amazon S3 als Eingabe, siehe Arbeiten mit Crawlern auf der AWS Glue Konsole in der AWS Glue Entwicklerhandbuch.

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

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

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

Um ein zu erstellen AWS Glue Tabelle

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Glue Konsole bei 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 „IAMRolle auswählen“ die Option Vorhandene IAM Rolle auswählen aus und klicken Sie dann auf Weiter.

   Sie können auch „IAMRolle erstellen“ wählen oder die IAM Rolle bei Bedarf von Ihrem Administrator erstellen lassen.
7. Behalten Sie für „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 Folgendes ein AWS Glue Datenbank und wählen Sie dann Weiter.
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 nicht mehr ausgeführt wurde, klicken Sie auf AWS Glue Wählen Sie in der 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.

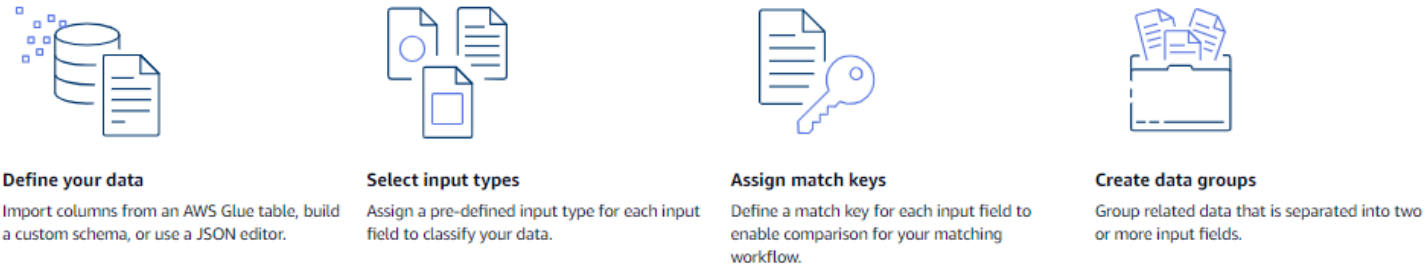
    b. Um das Schema einer Tabelle anzuzeigen, wählen Sie eine bestimmte Tabelle aus.

    c. Notieren Sie sich die AWS Glue Datenbankname und AWS Glue Tabellenname.

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 (Eingabetypen) und welche Spalten zugeordnet werden sollen.

Wenn Sie ein Schema-Mapping erstellen, definieren Sie zuerst Ihre Eingabefelder und Eingabetypen 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 es zunächst einrichten AWS Entity Resolution und bereiten Sie Ihre Datentabellen vor. Weitere Informationen erhalten Sie unter Einrichten AWS Entity Resolution und Eingabedatentabellen vorbereiten.

Nachdem Sie ein Schema-Mapping 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 einen ID-Mapping-Workflow innerhalb desselben AWS-KontoVerwenden Sie Ihr Schema-Mapping als Quelle.

Themen

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

Eine Schema-Mapping erstellen

Dieses Verfahren beschreibt den Prozess der Erstellung eines Schema-Mappings mithilfe von AWS Entity Resolution Konsole.

Es gibt drei Möglichkeiten, ein Schema-Mapping zu erstellen:

- Importieren Sie vorhandene Eingabedaten mit dem Befehl Import von AWS GlueOption — Verwenden Sie diese Erstellungsmethode, um Eingabefelder zu definieren, die mit vorausgefüllten Spalten aus einem beginnen AWS Glue Tabelle unter Verwendung eines geführten Ablaufs.
- Manuelles Definieren von Eingabedaten mit der Option Benutzerdefiniertes Schema erstellen — Verwenden Sie diese Erstellungsmethode, um die Eingabefelder mithilfe eines geführten Schemas manuell zu definieren.
- Manuell mit der Option „JSONEditor 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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
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 aus AWS Glue.

c. Wählen Sie das Symbol AWS Glue Datenbank aus der Dropdownliste und wählen Sie dann AWS Glue Tabelle aus der Dropdownliste.

   Um eine neue Tabelle zu erstellen, gehen Sie zu AWS Glue Konsole https://console.aws.amazon.com/glue/. Weitere Informationen finden Sie unter AWS Glue Tabellen in der AWS Glue Benutzerleitfaden.

d. 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 Quellen überschneidet, dann AWS Entity Resolution lehnt den Datensatz ab, wenn der entsprechende Workflow ausgeführt wird. Wenn Sie diese Schemazuordnung in einem regelbasierten Abgleichsworkflow verwenden, darf die eindeutige ID 38 Zeichen nicht überschreiten.

e. 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.

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

g. Wählen Sie Weiter.

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

   a. Geben Sie für Eingabefelder für den Abgleich für jedes Eingabefeld den Eingabetyp, den Abgleichsschlüssel und den Hashing-Status an.

      Der Eingabetyp hilft Ihnen bei der Klassifizierung der Daten. Die Zuordnungstaste ermöglicht den Vergleich der Eingabefelder mit Ihrem Abgleichs-Workflow. Der Hashing-Status gibt an, ob es sich bei dem Spaltenwert für dieses Eingabefeld um einen Hashwert oder einen Klartext handelt.

      > **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 Eingabetyp als LiveRampID an.
      > - Geben Sie das Namensfeld entweder in mehreren Feldern (z. B.**`first_name`**,**`last_name`**) oder in einem Feld an.
      > - Geben Sie das Feld für die Straßenadresse entweder in mehreren Feldern (z. B.**`address1`**,**`address2`**) oder in einem Feld an.
      >
      >   Bei einem Abgleich mit einer Adresse ist eine Postleitzahl erforderlich.
      > - Geben Sie E-Mail oder Telefonnummer mit dem Namen an, und diese Felder können mit der Straßenadresse übereinstimmen.

      > **Note**
      >
      > Wenn Sie ein Schema-Mapping zur Verwendung mit dem auf maschinellem Lernen basierenden Matching-Workflow erstellen, muss Ihr Datensatz mindestens eines der folgenden Attribute enthalten:**`phonenumber`**,, **`emailaddressfullname`**, **`addresses`** oder. **`birthdate`**

Geben Sie den Eingabetyp 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 es sich bei dem Spaltenwert für dieses Eingabefeld um einen Hashwert oder einen Klartext handelt.

c. Wählen Sie Weiter.

6. Gehen Sie für Schritt 3: Daten gruppieren wie folgt vor:

   a. Wählen Sie die entsprechenden Namensfelder aus und geben Sie dann den Gruppennamen und den Zuordnungsschlüssel ein.

      Example

      Wählen Sie beispielsweise die Eingabefelder **`First nameMiddle name`**, und aus**`Last name`**. Geben Sie dann einen Gruppennamen mit dem Namen „**`Full name`**“ und einen Abgleichsschlüssel mit dem Namen „**`Full name`**“ ein, um den Vergleich zu aktivieren.

   b. Wählen Sie die entsprechenden Adressfelder aus und geben Sie dann den Gruppennamen und den Zuordnungsschlüssel ein.

      Example

      Wählen Sie beispielsweise die Eingabefelder **`Home street address 1Home street address 2`**, und aus**`Home city`**. Geben Sie dann einen Gruppennamen mit dem Namen „**`Shipping address`**“ und einen Abgleichsschlüssel mit dem Namen „**`Shipping address`**“ ein, um den Vergleich zu aktivieren.

   c. Wählen Sie die entsprechenden Telefonnummernfelder aus und geben Sie dann den Gruppennamen und den Zuordnungsschlüssel ein.

      Example

      Wählen Sie beispielsweise die Eingabefelder **`Home phone 1Home phone 2`**, und aus**`Cell phone`**. Geben Sie dann einen Gruppennamen mit dem Namen „**`Shipping phone number`**“ und einen Abgleichsschlüssel mit dem Namen „**`Shipping phone number`**“ ein, um den Vergleich zu aktivieren.

Wenn Sie über mehr als einen Datentyp verfügen, können Sie weitere Gruppen hinzufügen.

d. Wählen Sie Weiter.

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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
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 Quellen überschneidet, dann AWS Entity Resolution lehnt den Datensatz ab, 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.

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. Fügen Sie für Eingabefelder für den Abgleich ein Eingabefeld und den entsprechenden Eingabetyp, den Abgleichsschlüssel und den Hashing-Status hinzu.

      Sie können insgesamt maximal 24 Eingabefelder für den Abgleich hinzufügen.

      Der Eingabetyp hilft Ihnen bei der Klassifizierung der Daten. Die Zuordnungstaste ermöglicht den Vergleich der Eingabefelder mit Ihrem Abgleichs-Workflow. Der Hashing-Status gibt an, ob es sich bei dem Spaltenwert für dieses Eingabefeld um einen Hashwert oder einen Klartext handelt.

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

> **Note**
>
> Wenn Sie ein Schema-Mapping zur Verwendung mit dem auf maschinellem Lernen basierenden Matching-Workflow erstellen, muss Ihr Datensatz mindestens eines der folgenden Attribute enthalten:**`phonenumber`**,, **`emailaddressfullname`**, **`addresses`** oder. **`birthdate`**
> Geben Sie den Eingabetyp 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.

c. Wählen Sie Weiter.

6. Für Schritt 3: Daten gruppieren:

   a. Wählen Sie die entsprechenden Namensfelder aus und geben Sie dann den Gruppennamen und den Zuordnungsschlüssel ein.

      Example

      Wählen Sie beispielsweise die Eingabefelder **`First nameMiddle name`**, und aus**`Last name`**. Geben Sie dann einen Gruppennamen mit dem Namen „**`Full name`**“ und einen Abgleichsschlüssel mit dem Namen „**`Full name`**“ ein, um den Vergleich zu aktivieren.

   b. Wählen Sie die entsprechenden Adressfelder aus und geben Sie dann den Gruppennamen und den Zuordnungsschlüssel ein.

Example

Wählen Sie beispielsweise die Eingabefelder **`Home street address 1Home street address 2`**, und aus**`Home city`**. Geben Sie dann einen Gruppennamen mit dem Namen „**`Shipping address`**“ und einen Abgleichsschlüssel mit dem Namen „**`Shipping address`**“ ein, um den Vergleich zu aktivieren.

c. Wählen Sie die entsprechenden Telefonnummernfelder aus und geben Sie dann den Gruppennamen und den Zuordnungsschlüssel ein.

Example

Wählen Sie beispielsweise die Eingabefelder **`Home phone 1Home phone 2`**, und aus**`Cell phone`**. Geben Sie dann einen Gruppennamen mit dem Namen „**`Shipping phone number`**“ und einen Abgleichsschlüssel mit dem Namen „**`Shipping phone number`**“ ein, um den Vergleich zu aktivieren.

Wenn Sie über mehr als einen Datentyp verfügen, können Sie weitere Gruppen hinzufügen.

d. Wählen Sie Weiter.

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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
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 unter Erstellungsmethode die Option JSONEditor 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.
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:

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

   b. Wählen Sie Weiter.
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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
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 aus.

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 eine Schemazuordnung zu bearbeiten:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie die Schemazuordnung aus.
4. Wählen Sie Edit (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 aus.
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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie die Schemazuordnung aus.
4. Wählen Sie Löschen.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Definieren Sie Eingabedaten mithilfe eines ID-Namespaces

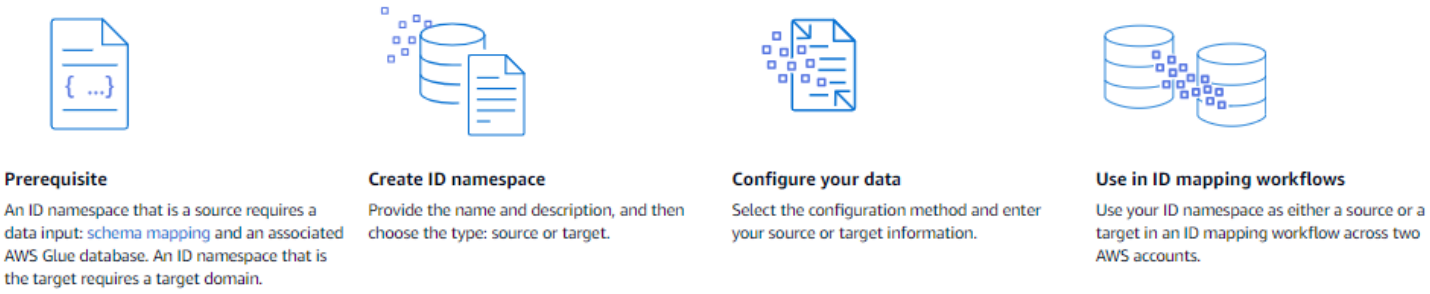
Ein ID-Namespace ist ein Wrapper, der Ihre Eingabedatentabelle umschließt. Sie verwenden einen ID-Namespace, um Metadaten bereitzustellen, in denen Ihre Eingabedaten und Abgleichstechniken sowie deren Verwendung in einem ID-Mapping-Workflow erläutert werden.

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

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

Sie können die Eingabedaten definieren, die Sie anhand von zwei Daten auflösen möchten AWS-Konten in einem ID-Zuordnungs-Workflow. 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.

Themen

- 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 Schema-Mapping erstellen und Zuordnen von Eingabedaten mithilfe eines Abgleichs-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 Zuordnen von Eingabedaten mithilfe eines ID-Mapping-Workflows.

Es gibt zwei Möglichkeiten, eine ID-Namespace-Quelle im AWS Entity Resolution Konsole: 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.

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

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.

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 Dateneingabe den gewünschten Eingabetyp aus, und ergreifen Sie dann die empfohlenen Maßnahmen.

Anbieter-Service	Empfohlene Aktionen
Eine bestehende Schemazuordnung	1. Wählen Sie die Schema-Mapping aus. 2. Wählen Sie das Symbol AWS Glue Datenbank, die AWS Glue Tabelle und das Schema-Mapping aus der Drop-down -Liste. Sie können bis zu 20 Dateneingaben hinzufügen.
Ein vorhandener Matching-Workflow	1. Wählen Sie den Matching-Workflow aus. 2. Wählen Sie das Konto aus, das dem ID-Namespace zugeordnet ist: entweder Ihr AWS-Kontooder Ein anderer AWS-Konto. 3. Wählen Sie je nach Kontotyp den Namen des Matching-Workflows aus oder geben Sie den Matching-Workflow einARN.

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 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.
Workflow für den Abgleich	Wählen Sie entweder Regeln aus dem Abgleichs-Workflow verwenden oder Neue Regeln bereitstellen, um Ihre Abgleichsregeln 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
Finden Sie eine beliebige 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 Datensatzabgleichs typ so, dass für jeden übereinstimmenden Datensatz im Ziel nur ein übereinst immender Datensatz in der Quelle gespeichert wird, wenn Sie den ID-Mappin g-Workflow erstellen.	Eingeschränkter Datensatzabgleich and Eine Quelle für ein Ziel

Ihr Ziel	Empfohlene Option
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 and 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 Zuordnung verfügen AWS Glue Datenbank.

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

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
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 derzeit den LiveRamp Provider-Dienst 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, die AWS Glue Tabelle und das Schema-Mapping aus der Drop-down-Liste.

   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 Richtlini e für diese Tabelle.

Option	Empfohlene Aktion
	• 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 ein AWS KMS Schlüssel, der zur Entschlüsselung 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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen 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-Mapping-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 Zuordnen von Eingabedaten mithilfe eines Abgleichs-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 Zuordnen von Eingabedaten mithilfe eines ID-Mapping-Workflows.

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

Themen

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

Ein ID-Namespace-Ziel erstellen (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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.

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 AWS-Kontooder Ein anderer AWS-Konto.

   b. Wählen Sie je nach Kontotyp den Namen des Matching-Workflows aus oder geben Sie den Matching-Workflow einARN.
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 Regeln auf das Ziel beschränkt, der Ziel-ID-Namespace die Regeln jedoch auf die Quelle beschränkt, führt dies zu einem Fehler.

b. Für Abgleichsregeln AWS Entity Resolution fügt 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
Finden Sie eine beliebige 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 Datensatzabgleichs typ so, dass für jeden übereinstimmenden Datensatz im Ziel nur ein übereinst	Eingeschränkter Datensatzabgleich and

Ihr Ziel	Empfohlene Option
immender Datensatz in der Quelle gespeichert wird, wenn Sie den ID-Mappin g-Workflow erstellen.	Eine Quelle für ein Ziel
Beschränken Sie den Datensatzabgleichs typ auf das Speichern aller übereinst immenden Datensätze in der Quelle für jeden übereinstimmenden Datensatz im Ziel, wenn Sie den ID-Mapping-Workflow erstellen.	Eingeschränkter Datensatzabgleich and 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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
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 derzeit den LiveRamp Provider-Dienst 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-Domänen-ID 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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option ID-Namespaces aus.
3. Wählen Sie den ID-Namespace aus.
4. Wählen Sie Edit (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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option ID-Namespaces aus.
3. Wählen Sie den ID-Namespace aus.
4. Wählen Sie Löschen.
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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
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.

Zuordnen von Eingabedaten mithilfe eines Abgleichs-Workflows

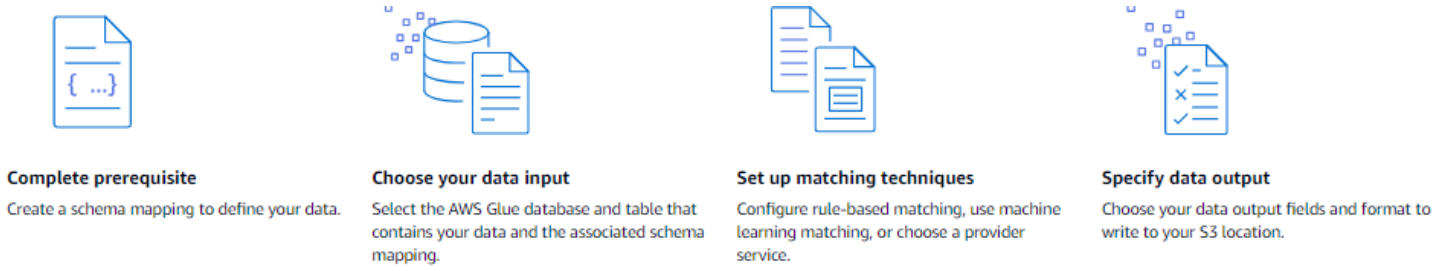
Ein Abgleichs-Workflow ist ein Datenverarbeitungsjob, der Daten aus verschiedenen Eingabequellen kombiniert und vergleicht und anhand verschiedener Abgleichstechniken bestimmt, welche davon übereinstimmen. Es erzeugt eine Datenausgabetabelle.

Wenn Sie einen Abgleichs-Workflow erstellen, geben Sie zunächst Ihre Dateneingaben und Normalisierungsschritte an und wählen dann die gewünschten Abgleichstechniken und die Datenausgabe aus. AWS Entity Resolution liest Ihre Daten von Ihrem oder Ihren angegebenen Standorten aus und findet eine Übereinstimmung zwischen zwei oder mehr Datensätzen in Ihren Daten. Anschließend wird den Datensätzen im abgeglichenen Datensatz eine Match-ID zugewiesen. AWS Entity Resolution schreibt dann Datenausgabedateien an einen von Ihnen ausgewählten Speicherort. Sie können Folgendes verwenden … AWS Entity Resolution um die Ausgabedaten auf Wunsch zu hashen, sodass Sie die Kontrolle über Ihre Daten behalten.

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

Die Datenausgabe enthält sowohl eine Datei für erfolgreiche Übereinstimmungen als auch eine Datei für Fehler. Die Datenausgabe kann mehrere Felder enthalten. Die erfolgreichen Ergebnisse werden in einen `success` Ordner geschrieben, der mehrere Dateien enthält, und jede Datei enthält eine Teilmenge der erfolgreichen Datensätze. In ähnlicher Weise werden Fehler in einen `error` Ordner mit mehreren Feldern geschrieben, wobei jedes Feld eine Teilmenge der Fehlerdatensätze enthält. Weitere Informationen zur Behebung von Fehlern finden Sie unterFehlerbehebung bei passenden Workflows.

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



Bevor Sie einen passenden Workflow erstellen, müssen Sie zunächst eine Schemazuordnung erstellen. Weitere Informationen finden Sie unter Eine Schema-Mapping erstellen.

Es gibt drei Möglichkeiten, einen Abgleichsworkflow auf der Grundlage von Abgleichstechniken zu erstellen: regelbasiert, aufmaschinellem Lernen oder auf Anbieterdiensten.

Nachdem Sie einen passenden Workflow erstellt und ausgeführt haben, können Sie wie folgt vorgehen:

- Zeigen Sie die Ergebnisse an dem von Ihnen angegebenen S3-Speicherort an. Passende Workflows werden generiert, IDs nachdem die Daten indexiert wurden.
- Verwenden Sie die Ergebnisse des regelbasierten Abgleichs oder des maschinellen Lernens (ML) als Eingabe für den Abgleich auf Anbieterdiensten oder umgekehrt, um Ihre Geschäftsanforderungen zu erfüllen.

Um beispielsweise Abonnementkosten für Anbieter zu sparen, können Sie zunächst einen regelbasierten Abgleich durchführen, um Übereinstimmungen in Ihren Daten zu finden. Anschließend können Sie eine Teilmenge nicht übereinstimmender Datensätze an den dienstbasierten Abgleich des Anbieters senden.

Themen

- Einen regelbasierten Abgleichsworkflow erstellen
- Einen auf maschinellem Lernen basierenden Abgleichs-Workflow erstellen
- Einen auf Provider-Services basierenden Abgleichs-Workflow erstellen
- Einen passenden Workflow bearbeiten
- Einen passenden Workflow löschen
- Suche nach einer Match-ID für einen regelbasierten Abgleichs-Workflow
- Löschen von Datensätzen aus einem regelbasierten oder ML-basierten Abgleichs-Workflow
- Fehlerbehebung bei passenden Workflows

Einen regelbasierten Abgleichsworkflow erstellen

Der regelbasierte Abgleich ist ein hierarchischer Satz von Wasserfall-Abgleichsregeln, vorgeschlagen von AWS Entity Resolution, basiert auf den von Ihnen eingegebenen Daten und ist vollständig von Ihnen konfigurierbar. Der regelbasierte Abgleichs-Workflow ermöglicht es Ihnen, Klartext- oder Hash-Daten zu vergleichen, um anhand von von Ihnen angepassten Kriterien exakte Übereinstimmungen zu finden.

Wann AWS Entity Resolution findet eine Übereinstimmung zwischen zwei oder mehr Datensätzen in Ihren Daten und weist Folgendes zu:

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

Um einen regelbasierten Abgleichs-Workflow zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Abgleichende 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 Dateneingabe eine AWS Glue Wählen Sie in der Dropdownliste die Datenbank AWS Glue Tabelle und dann das entsprechende Schema-Mapping.

      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.

   d. 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 Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautet `entityresolution-matching-workflow-<timestamp>` .

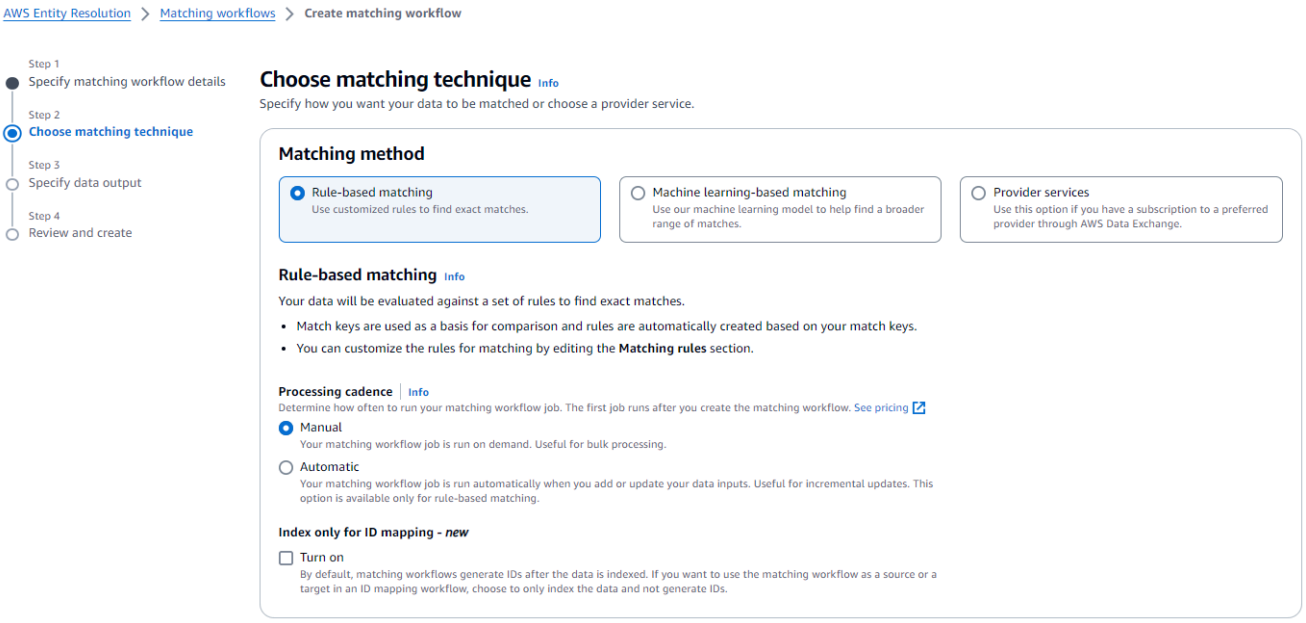
Option	Empfohlene Aktion
	• Sie müssen über die erforderlichen Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüs selt sind, wählen Sie die Option Diese Daten werden mit einem KMS Schlüssel verschlüsselt. Geben Sie dann ein AWS KMS Schlüssel, der zur Entschlüsselung Ihrer Dateneingabe verwendet wird.
Verwenden Sie eine vorhandene Servicero lle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownl iste 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 Servicero llen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht nicht, die bestehende Rollenric htlinie zu aktualisieren, um die erforderl ichen Berechtigungen hinzuzufügen.

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

f. Wählen Sie Weiter.

5. Für Schritt 2: Passende Technik wählen:

a. Wählen Sie unter Abgleichmethode die Option Regelbasierter Abgleich aus.



b. Wählen Sie für die Schrittfrequenz je nach Ziel eine der folgenden Optionen aus.

Ihr Ziel	Empfohlene Option
Führen Sie bei Bedarf einen Workflow für ein Massenupdate aus	Manuell
Führen Sie einen Workflow aus, sobald sich neue Daten in Ihrem S3-Bucket befinden	Automatisch

> **Note**
>
> Wenn Sie Automatisch wählen, stellen Sie sicher, dass Sie EventBridge Amazon-Benachrichtigungen für Ihren S3-Bucket aktiviert haben. Anweisungen zur

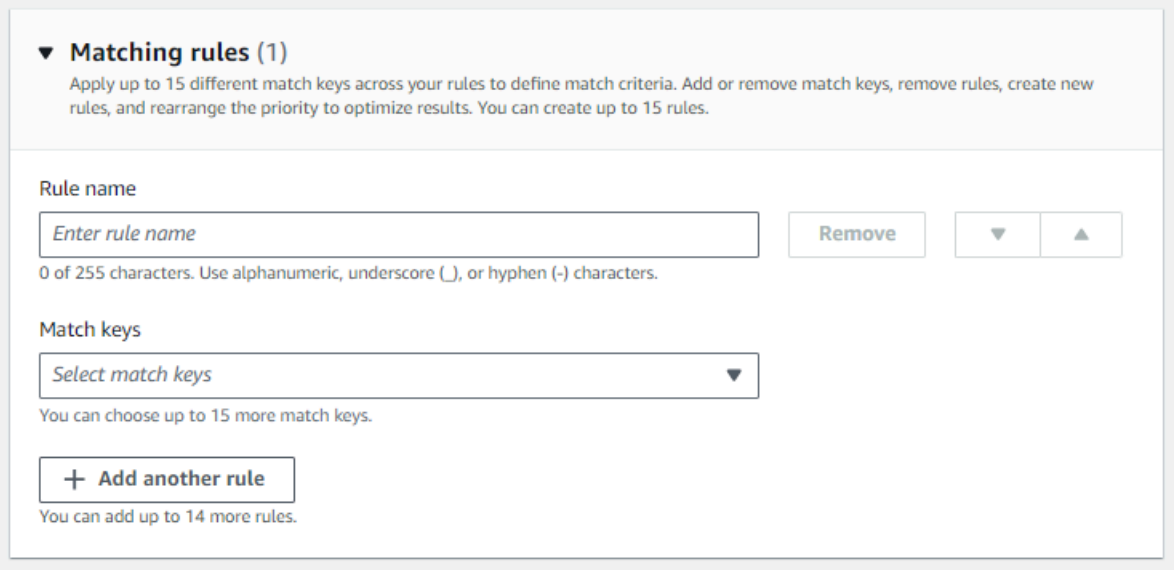
Aktivierung EventBridge von Amazon mithilfe der S3-Konsole finden Sie unter Enabling Amazon EventBridge im Amazon S3 S3-Benutzerhandbuch.

c. (Optional) Für den Index nur für die ID-Zuordnung können Sie wählen, ob Sie die Möglichkeit aktivieren möchten, die Daten nur zu indizieren und nicht zu generierenIDs.

   Standardmäßig werden passende Workflows generiert, IDs nachdem die Daten indexiert wurden.

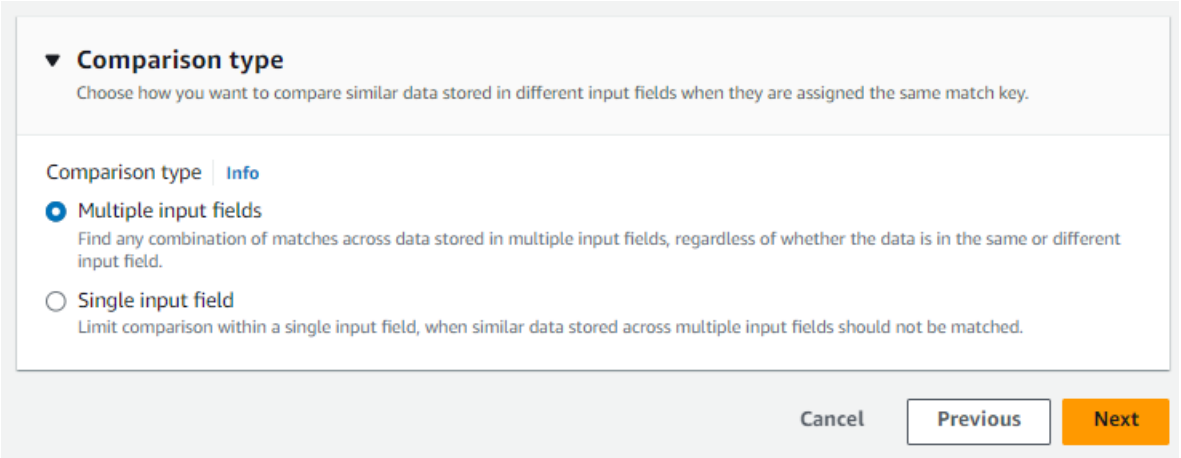
d. Geben Sie für Abgleichsregeln einen Regelnamen ein und wählen Sie dann die Option Abgleichsschlüssel für diese Regel aus.

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



e. Wählen Sie als 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 einzelnes Eingabefeld	Einzelnes Eingabefeld



f. Wählen Sie Weiter.

6. Für Schritt 3: Datenausgabe und Format angeben:

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

   b. Wenn Sie für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie AWS KMS Schlüssel ARN.

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

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

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

e. Wählen Sie Weiter.

7. Für Schritt 4: Überprüfen und erstellen:

   a. Überprüfen Sie die Auswahlen, 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 passende Workflow erstellt und der Job gestartet wurde.

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.
   - 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 IDsgenerierte eindeutige Match.
   - Die Anzahl der Eingabedatensätze.

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

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

10. (Nur manueller Verarbeitungstyp) Wenn Sie einen regelbasierten Abgleichs-Workflow mit dem Verarbeitungstyp Manuell erstellt haben, können Sie den Abgleichs-Workflow jederzeit ausführen, indem Sie auf der Seite mit den entsprechenden Workflow-Details die Option Workflow ausführen wählen.

Einen auf maschinellem Lernen basierenden Abgleichs-Workflow erstellen

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 Modells für maschinelles Lernen eine Vielzahl von Übereinstimmungen zu finden.

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

Wann AWS Entity Resolution findet eine Übereinstimmung zwischen zwei oder mehr Datensätzen in Ihren Daten und weist Folgendes zu:

- Eine Match-ID für die Datensätze im übereinstimmenden Datensatz
- Der Prozentsatz des Übereinstimmungskonfidenzniveaus.

Sie können die Ausgabe eines ML-basierten Abgleichs-Workflows als Eingabe für den Datendienstanbieterabgleich verwenden oder umgekehrt, um Ihre spezifischen Ziele zu erreichen. Sie können beispielsweise einen ML-basierten Abgleich ausführen, um zunächst in Ihren eigenen Datensätzen nach Übereinstimmungen in Ihren Datenquellen zu suchen. Wenn für eine Teilmenge kein Abgleich gefunden wurde, können Sie anschließend einen Abgleich auf Anbieterbasis ausführen, um weitere Treffer zu finden.

So erstellen Sie einen ML-basierten Abgleichsworkflow:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Abgleichende 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 Dateneingabe eine AWS Glue Wählen Sie in der Dropdownliste die Datenbank AWS Glue Tabelle und dann das entsprechende Schema-Mapping.

   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.

d. 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 Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautet `entityresolution-matching-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 ein AWS KMS Schlüssel, der zur Entschlüsselung Ihrer Dateneingabe verwendet wird.

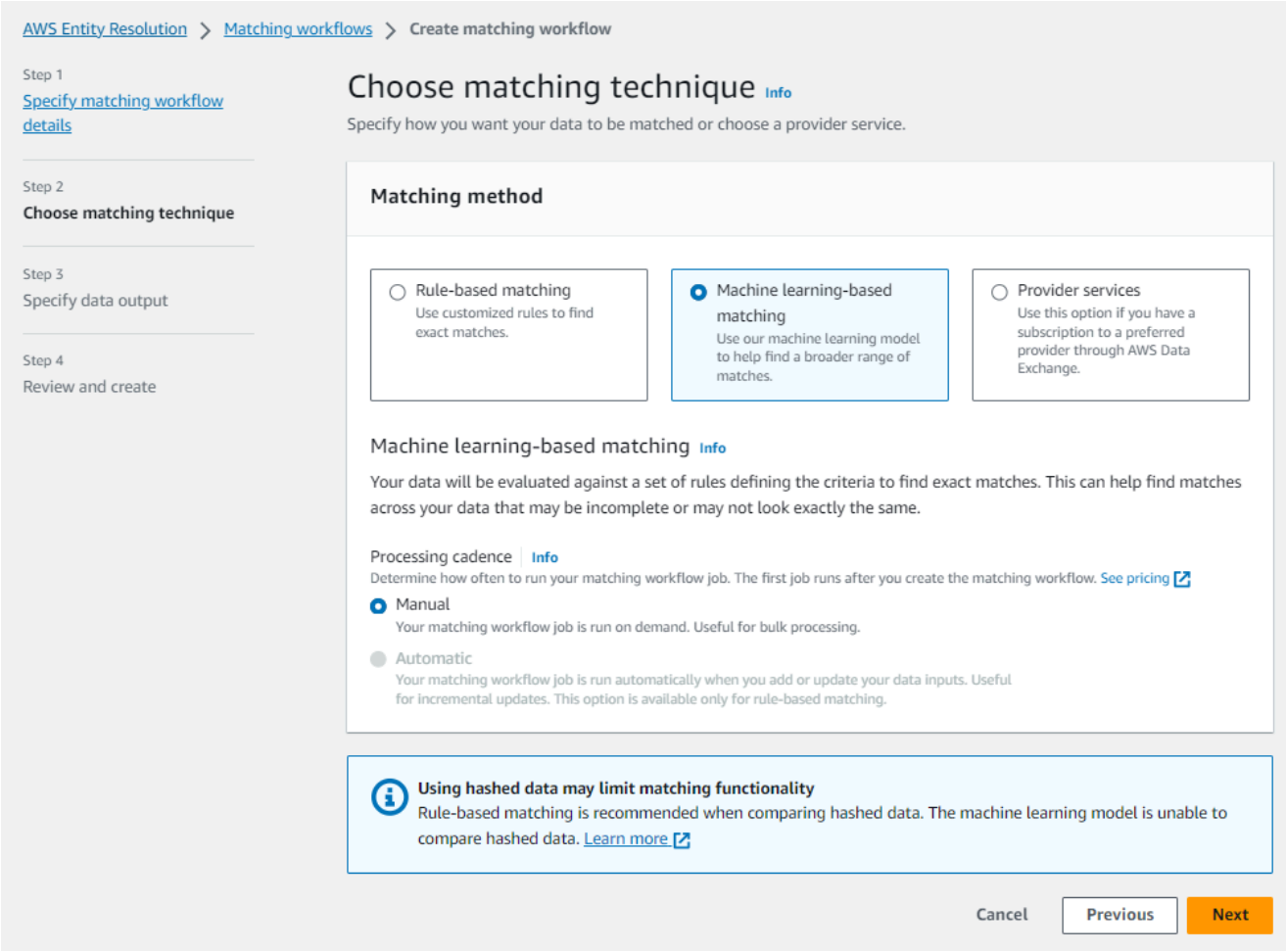
Option	Empfohlene Aktion
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht 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 - und Wertepaar ein.

f. Wählen Sie Weiter.

5. Für Schritt 2: Passende Technik wählen:

a. Wählen Sie als Matching-Methode die Option Matching auf Basis von maschinellem Lernen aus.



b. Für die Schrittfrequenz ist die Option Manuell ausgewählt.

   Mit dieser Option können Sie bei Bedarf einen Workflow für ein Massenupdate ausführen.

c. Wählen Sie Weiter.

6. Für Schritt 3: Datenausgabe und Format angeben:

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

   b. Wenn Sie für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie AWS KMS Schlüssel ARN.

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

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

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

e. Wählen Sie Weiter.

7. Für Schritt 4: Überprüfen und erstellen:

   a. Überprüfen Sie die Auswahlen, 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 passende Workflow erstellt und der Job gestartet wurde.

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.
   - 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 IDsgenerierte eindeutige Match.
   - Die Anzahl der Eingabedatensätze.

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

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

Einen auf Provider-Services basierenden Abgleichs-Workflow erstellen

Mit dem dienstbasierten Abgleich auf Anbieterbasis können Sie Ihre bekannten Kennungen Ihrem bevorzugten Datendienstanbieter zuordnen.

AWS Entity Resolution unterstützt derzeit die folgenden Datenanbieterdienste:

- LiveRamp
- TransUnion
- Vereinheitlichte ID 2.0

Weitere Informationen zu den unterstützten Anbieterdiensten finden Sie unterEingabedaten von Drittanbietern werden vorbereitet.

Sie können ein öffentliches Abonnement für diese Anbieter verwenden unter AWS Data Exchange oder handeln Sie ein privates Angebot direkt mit dem Datenanbieter aus. Weitere Informationen zum Erstellen eines neuen Abonnements oder zur Wiederverwendung eines vorhandenen 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.

Themen

- Einen passenden Workflow erstellen mit LiveRamp
- Einen passenden Workflow erstellen mit TransUnion
- Einen passenden Workflow mit UID 2.0 erstellen

Einen passenden Workflow erstellen mit LiveRamp

Wenn Sie ein Abonnement für den LiveRamp Dienst haben, können Sie einen passenden Workflow für den LiveRamp Dienst erstellen, um die Identitätsauflösung durchzuführen.

Der LiveRamp Dienst stellt eine Kennung namens RampID bereit. Die RampID ist eine der am häufigsten auf Demand-Side-Plattformen verwendeten IDs Plattformen, um ein Publikum für eine Werbekampagne zu gewinnen. Mithilfe eines passenden Workflows mit LiveRamp können Sie Hash-E-Mail-Adressen in auflösen. RAMPIDs

> **Note**
>
> AWS Entity Resolution unterstützt die PII basierte RampID-Zuweisung.

Für diesen Workflow ist ein Amazon S3 S3-Daten-Staging-Bucket erforderlich, in den die entsprechende Workflow-Ausgabe vorübergehend geschrieben werden soll. Bevor Sie einen ID-Mapping-Workflow mit erstellen LiveRamp, fügen Sie dem Daten-Staging-Bucket die folgenden Berechtigungen hinzu.

```
{
    "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 jede *<user input placeholder>* mit Ihren eigenen Informationen.

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

Um einen passenden Workflow zu erstellen mit LiveRamp:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Abgleichende 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 Dateneingabe eine AWS Glue Wählen Sie in der Dropdownliste die Datenbank AWS Glue Tabelle, und wählen Sie dann das entsprechende Schema-Mapping 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 den reinen E-Mail-Auflösungsprozess 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 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-matching-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 ein AWS KMS Schlüssel, der zur Entschlüsselung 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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht 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 - und Wertepaar ein.

f. Wählen Sie Weiter.

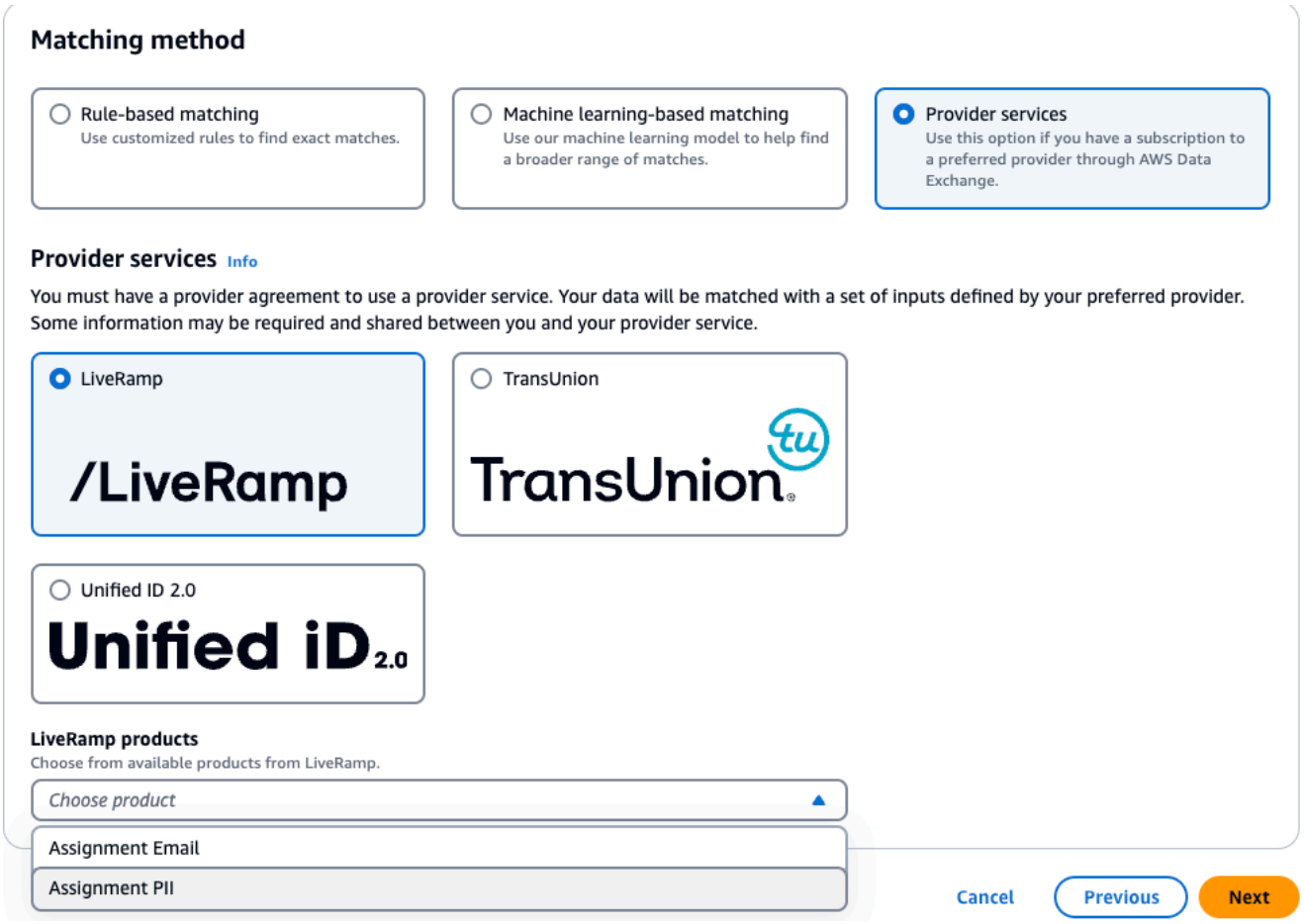
5. Für Schritt 2: Passende Technik wählen:

a. Wählen Sie als Abgleichmethode die Option Provider-Services aus.

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

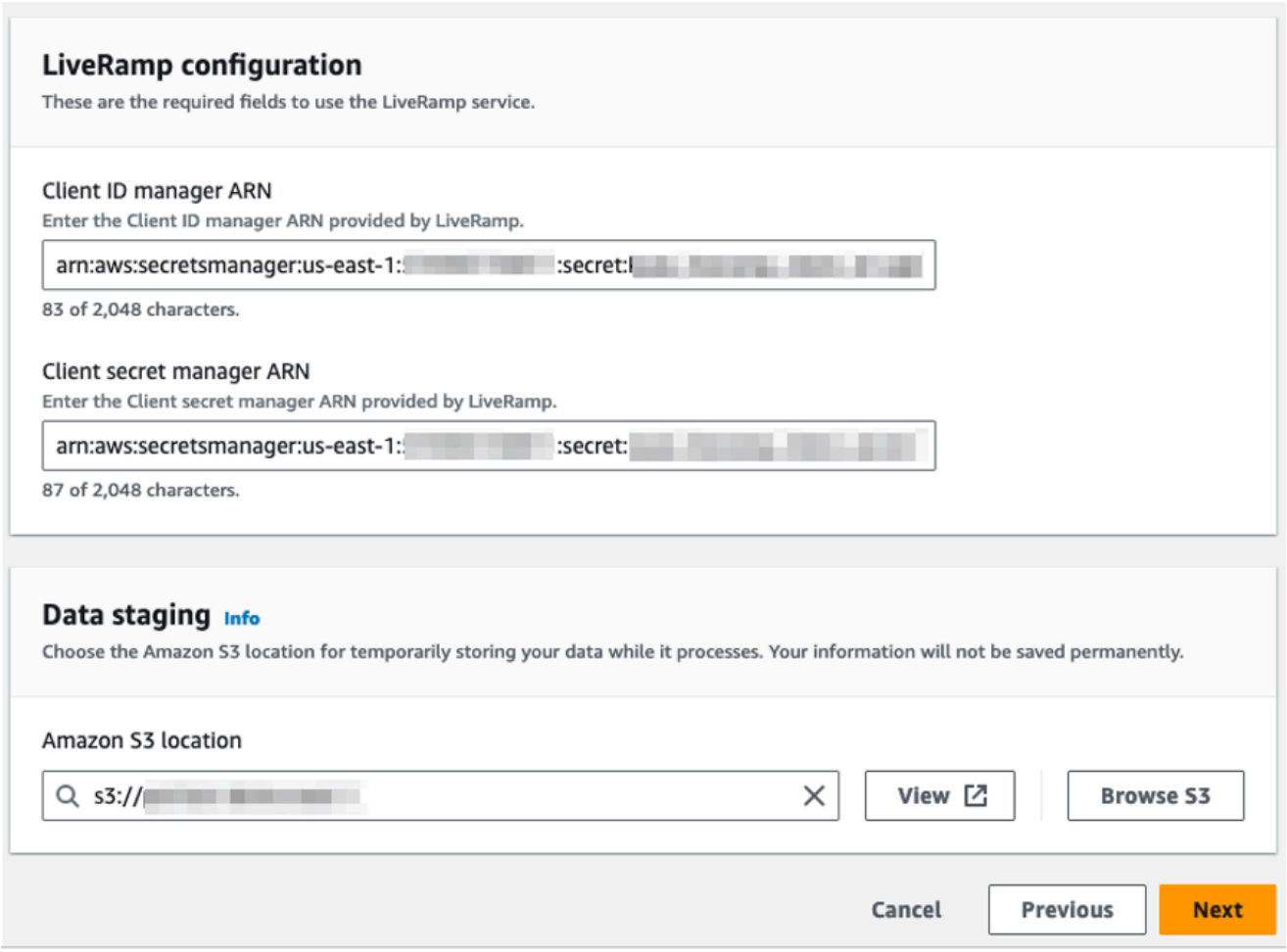
> **Note**
>
> Stellen Sie sicher, dass das Format und die Normalisierung Ihrer Dateneingabedatei den Richtlinien des Dienstanbieters entsprechen.
> Weitere Informationen zu den Richtlinien zur Formatierung von Eingabedateien für den Abgleichs-Workflow finden Sie ADX in der LiveRamp Dokumentation unter Perform Identity Resolution Through.

c. Wählen Sie für LiveRamp Produkte ein Produkt aus der Drop-down-Liste aus.



> **Note**
>
> Wenn Sie Zuweisung wählenPII, müssen Sie bei der Entitätsauflösung mindestens eine Spalte angeben, in der es sich nicht um eine Identifikationsspalte handelt. Zum Beispiel. GENDER

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



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

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

f. Wählen Sie Weiter.

6. Für Schritt 3: Datenausgabe angeben:

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

   b. Wenn Sie für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie AWS KMS Schlüssel ARN.

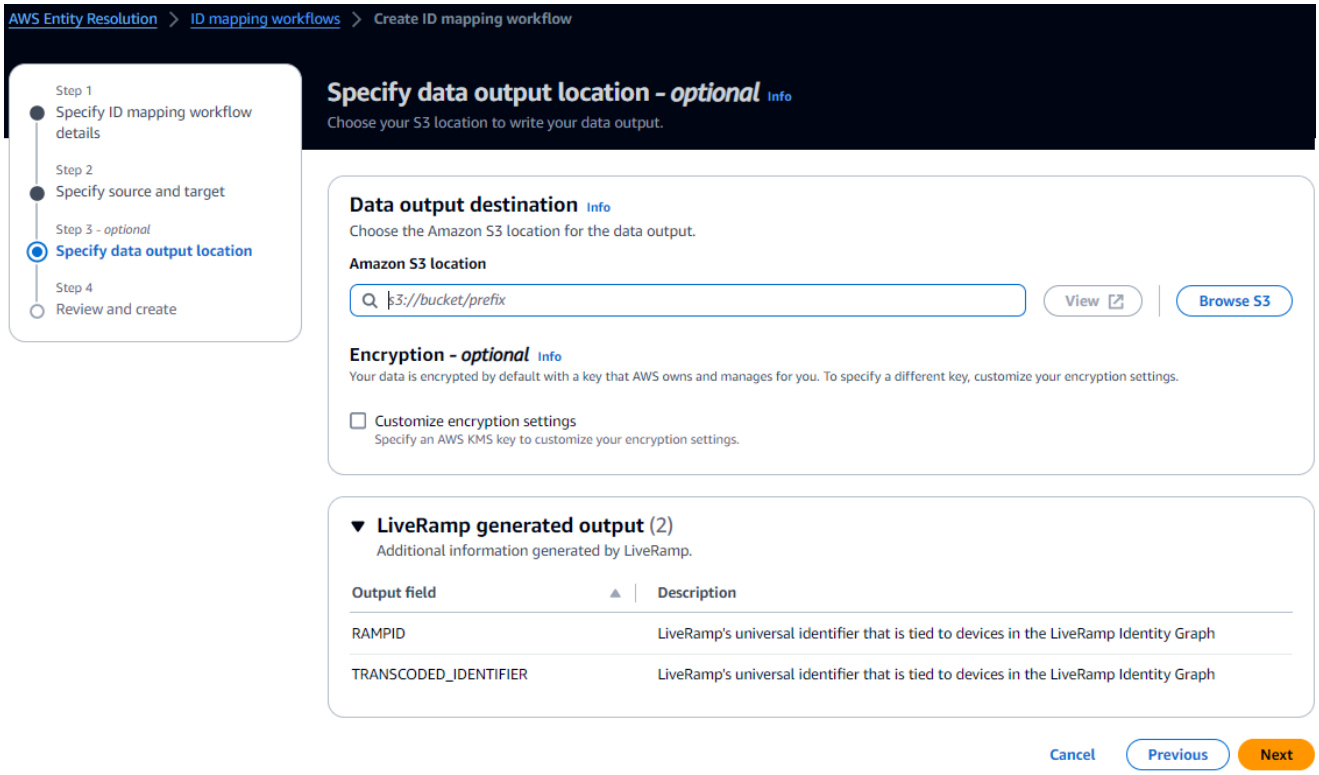
c. Sehen Sie sich die LiveRamp generierte Ausgabe an.

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

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

> **Note**
>
> Wenn Sie sich dafür entschieden haben LiveRamp, wird aufgrund von LiveRamp Datenschutzfiltern, die personenbezogene Daten (PII) entfernen, in einigen Feldern der Ausgabestatus Nicht verfügbar angezeigt.

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



e. Wählen Sie Weiter.

7. Für Schritt 4: Überprüfen und erstellen:

   a. Überprüfen Sie die Auswahlen, 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 passende Workflow erstellt und der Job gestartet wurde.

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.
   - 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 IDsgenerierte eindeutige Match.
- Die Anzahl der Eingabedatensätze.

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

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

Einen passenden Workflow erstellen 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 TransUnion Personen- und Haushalts-E-Schlüsseln und über 200 Datenattributen verknüpfen, abgleichen und erweitern.

Der TransUnion Service stellt Identifikatoren bereit, die als TransUnion Einzelperson und Haushalt bezeichnet werden. IDs TransUnion ermöglicht die ID-Zuweisung (auch als Kodierung bezeichnet) bekannter Identifikatoren wie Name, Adresse, Telefonnummer und E-Mail-Adresse.

Für diesen Workflow ist ein Amazon S3 S3-Daten-Staging-Bucket erforderlich, in den die entsprechende Workflow-Ausgabe vorübergehend geschrieben werden soll. Bevor Sie einen passenden Workflow mit erstellen TransUnion, fügen Sie dem Daten-Staging-Bucket die folgenden Berechtigungen hinzu.

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

            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:DeleteObject"
```

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

Ersetzen Sie jede *<user input placeholder>* mit Ihren eigenen Informationen.

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

Um einen passenden Workflow zu erstellen mit TransUnion:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Abgleichende 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 Dateneingabe eine AWS Glue Wählen Sie in der Dropdownliste die Datenbank AWS Glue Tabelle, und wählen Sie dann das entsprechende Schema-Mapping 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.

   d. 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 Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautet `entityresolution-matching-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 ein AWS KMS Schlüssel, der zur Entschlüsselung 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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht 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 - und Wertepaar ein.

f. Wählen Sie Weiter.

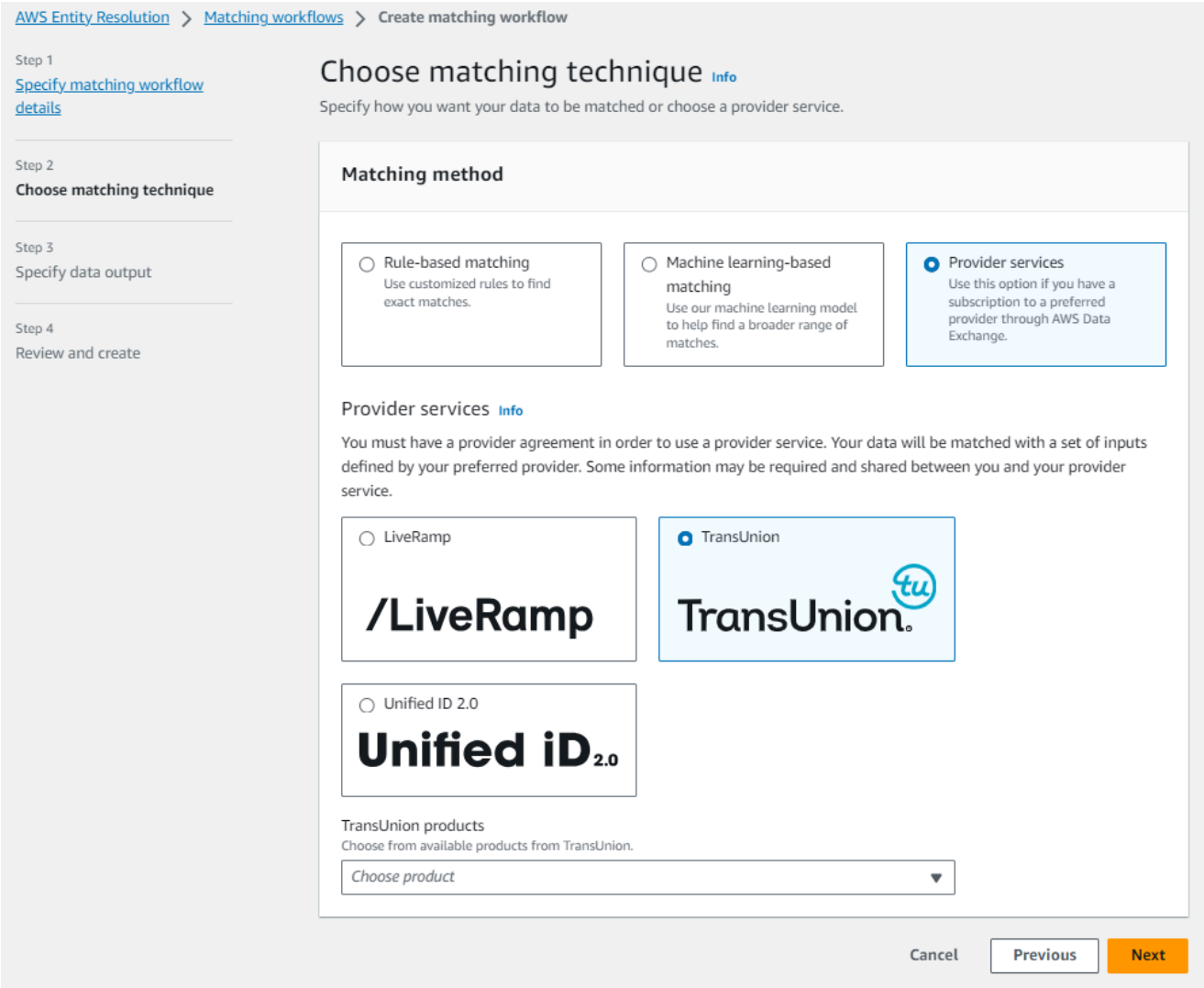
5. Für Schritt 2: Passende Technik wählen:

a. Wählen Sie als Abgleichmethode die Option Provider-Services 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 Dienstanbieters entsprechen.

c. Wählen Sie für TransUnion Produkte ein Produkt aus der Drop-down-Liste aus.



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

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

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

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

b. Wenn Sie für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie AWS KMS Schlüssel ARN.

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 einschließen, 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 auf Eingeschlossen bei.
Felder ausblenden (von der Ausgabe ausschließen)	Wählen Sie das Ausgabefeld und dann Ausblenden aus.
Felder maskieren	Wählen Sie das Ausgabefeld und dann Hash-Ausgabe aus.
Setzen Sie die vorherigen Einstellungen zurück	Klicken Sie auf Reset (Zurücksetzen).

e. Sehen Sie sich für die vom System generierte Ausgabe alle enthaltenen Felder an.

f. Wählen Sie Weiter.

8. Für Schritt 4: Überprüfen und erstellen:

   a. Überprüfen Sie die Auswahlen, 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 passende Workflow erstellt und der Job gestartet wurde.

9. 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
- Die Zeit, in der der Workflow-Job abgeschlossen wurde.
- Die Anzahl der verarbeiteten Datensätze.
- Die Anzahl der nicht verarbeiteten Datensätze.
- Das IDsgenerierte eindeutige Match.
- Die Anzahl der Eingabedatensätze.

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

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

Einen passenden Workflow mit UID 2.0 erstellen

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

Der Unified ID 2.0-Dienst bietet Raw UID 2, das für die Erstellung von Werbekampagnen auf der The Trade Desk-Plattform verwendet wird. UID2.0 wird mit einem Open-Source-Framework generiert.

In einem Workflow können Sie entweder **`Email Address`** oder **`Phone number`** für die UID2 Rohgenerierung 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 Schemazuweisung, der zwar zugeordnet, aber **`Email Address`** nicht zugeordnet **`Phone number`** ist. Erstellen Sie dann einen zweiten Workflow mit dieser neuen Schemazuordnung.

> **Note**
>
> Rohkost UID2s entsteht durch Zugabe von Salzen aus Salzkübeln, die etwa einmal pro Jahr rotiert werden, sodass auch UID2 das Rohöl rotiert wird. Daher wird empfohlen, das Rohprodukt UID2s täglich aufzufrischen. Weitere Informationen finden Sie unter https://unifiedid.com/docs/how-often-should-uidgetting-started/gs-faqs# 2 -incremental-updates. s-be-refreshed-for

So erstellen Sie einen passenden Workflow mit UID 2.0:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie auf der Seite Abgleichende 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 Dateneingabe eine AWS Glue Wählen Sie in der Dropdownliste die Datenbank AWS Glue Tabelle, und wählen Sie dann das entsprechende Schema-Mapping 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 unter Normalisierung von E-Mail-Adressen in der UID 2.0-Dokumentation.

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

   d. 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 Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautet `entityresolution-matching-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 ein AWS KMS Schlüssel, der zur Entschlüsselung 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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

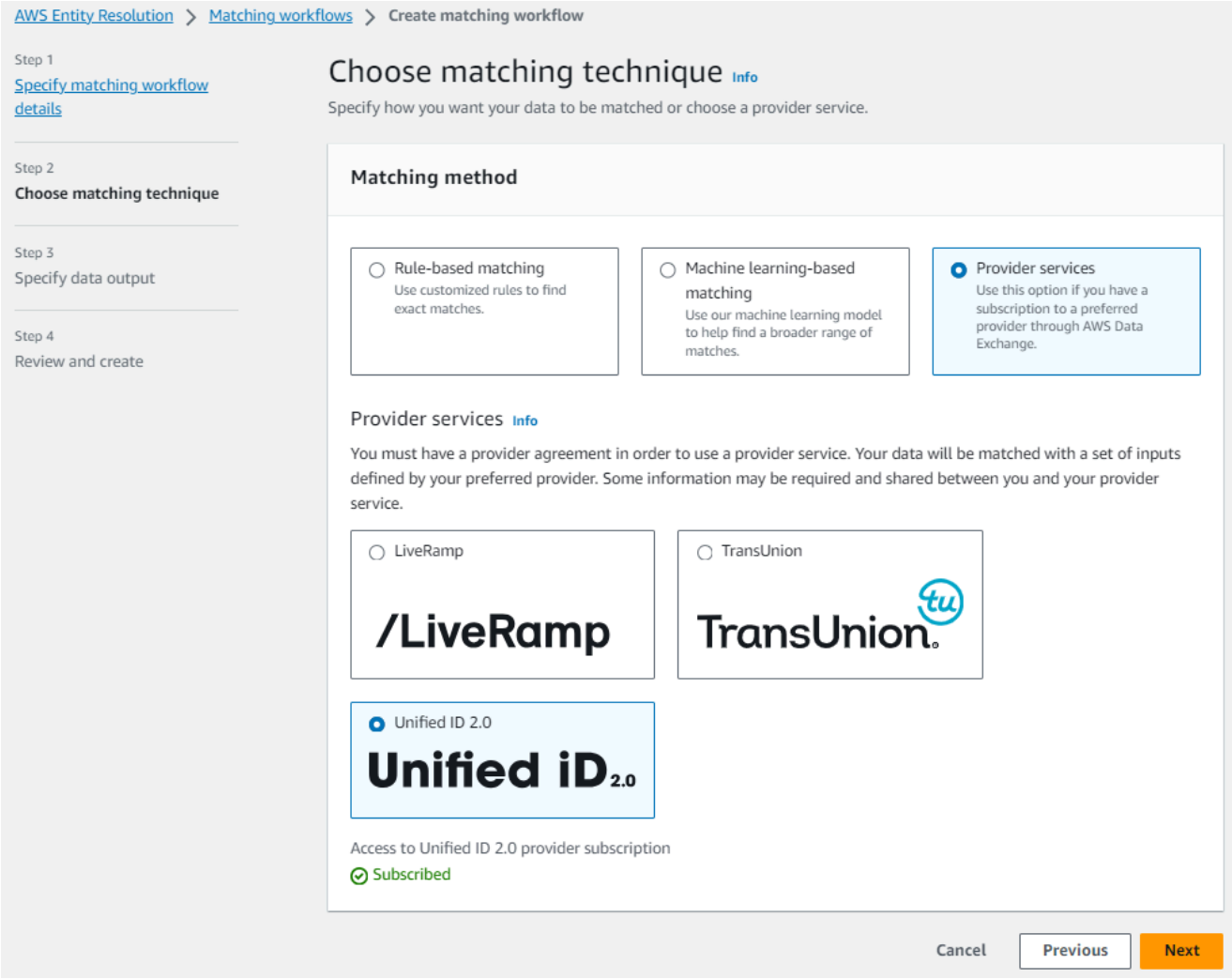
e. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.

f. Wählen Sie Weiter.

5. Für Schritt 2: Passende Technik wählen:

a. Wählen Sie als Abgleichmethode die Option Provider-Services aus.

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



c. Wählen Sie Weiter.

6. Für Schritt 3: Datenausgabe angeben:

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

   b. Wenn Sie für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie AWS KMS Schlüssel ARN.

   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 auf Eingeschlossen bei.
Felder ausblenden (von der Ausgabe ausschließen)	Wählen Sie das Ausgabefeld und dann Ausblenden aus.
Felder maskieren	Wählen Sie das Ausgabefeld und dann Hash-Ausgabe aus.
Setzen Sie die vorherigen Einstellungen zurück	Klicken Sie auf Reset (Zurücksetzen).

e. Sehen Sie sich für die vom System generierte Ausgabe alle enthaltenen Felder an.

f. Wählen Sie Weiter.

7. Für Schritt 4: Überprüfen und erstellen:

   a. Überprüfen Sie die Auswahlen, 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 passende Workflow erstellt und der Job gestartet wurde.

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.
   - 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 IDsgenerierte eindeutige Match.
   - Die Anzahl der Eingabedatensätze.

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

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

Einen passenden Workflow bearbeiten

So bearbeiten Sie einen passenden Workflow:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
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 entsprechenden Workflow-Details in der oberen rechten Ecke die Option Bearbeiten aus.
5. Nehmen Sie auf der Seite Passende Workflow-Details angeben die erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
6. Nehmen Sie auf der Seite Abgleichstechnik auswählen die erforderlichen Änderungen vor und klicken Sie dann auf Weiter.
7. Nehmen Sie auf der Seite „Datenausgabe angeben“ die erforderlichen Änderungen vor und klicken Sie dann auf Weiter.
8. Nehmen Sie auf der Seite Überprüfen und speichern die erforderlichen Änderungen vor und wählen Sie dann Speichern aus.

Einen passenden Workflow löschen

So löschen Sie einen passenden Workflow:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
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 entsprechenden Workflow-Details in der oberen rechten Ecke die Option Löschen aus.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

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

Nachdem Sie einen regelbasierten Abgleichs-Workflow ausgeführt haben, können Sie die entsprechende Match-ID und die zugehörige Regel für die verarbeiteten Datensätze finden.

So finden Sie eine Match-ID für einen regelbasierten Abgleichs-Workflow:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie den regelbasierten Abgleichs-Workflow aus, der verarbeitet wurde (Auftragsstatus ist Abgeschlossen).
4. Wählen Sie auf der Seite mit den entsprechenden Workflow-Details die Registerkarte „Match-ID suchen“ aus.
5. Führen Sie eine der folgenden Aktionen aus:

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

6. Erweitern Sie die Übereinstimmungsregeln.
7. Geben Sie für jeden Match-Schlüssel einen Wert ein.

   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.

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

8. Wählen Sie Look up.
9. Sehen Sie sich die entsprechende Match-ID und die zugehörige Regel an, die für den Abgleich verwendet wurde.

Löschen von Datensätzen aus einem regelbasierten oder ML-basierten Abgleichs-Workflow

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

Um Datensätze aus einem regelbasierten oder ML-basierten Abgleichs-Workflow zu löschen

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie den regelbasierten oder den ML-basierten Abgleichs-Workflow.
4. Wählen Sie auf der Seite mit den entsprechenden Workflow-Details in der Dropdownliste Aktionen die Option Eindeutig löschen IDs aus.
5. Geben Sie die eindeutige ID, die Sie löschen möchten, im IDs Abschnitt Eindeutig ein.

   Sie können bis zu 10 eindeutige Zeichen eingebenIDs.
6. Geben Sie die Eingangsquelle an, aus der das eindeutige Objekt gelöscht werden sollIDs.

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

   Wenn Sie nur eine Eingabequelle angeben, wirkt sich dies nicht auf die eindeutigen IDs Eingabequellen aus anderen Eingabequellen aus.
7. Wählen Sie Eindeutig löschen IDs.

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

- MatchID
- 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.

Zuordnen von Eingabedaten mithilfe eines ID-Mapping-Workflows

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:

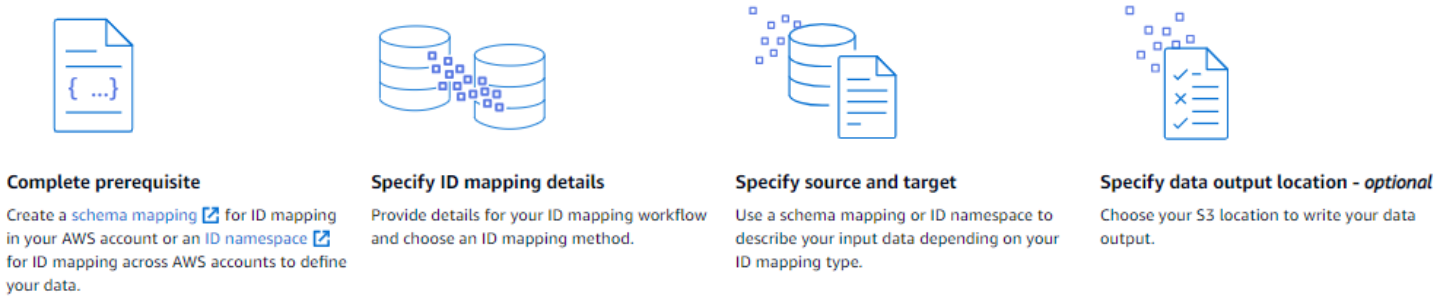
- Regelbasierte ID-Zuordnung — Sie verwenden Abgleichsregeln, um Erstanbieter-Daten von einer Quelle in ein Ziel zu übersetzen.
- ID-Zuordnung von Providerdiensten — Sie verwenden den LiveRamp Provider-Service, um Drittanbieterdaten von einer Quelle in ein Ziel zu übersetzen.

> **Note**
>
> Der Workflow zur ID-Zuordnung von Providerdiensten in AWS Entity Resolution ist derzeit in integriert LiveRamp. Wenn Sie ein Abonnement für den LiveRamp Dienst haben, können Sie einen ID-Zuordnungs-Workflow erstellen, LiveRamp um die Transcodierung durchzuführen. Mit der LiveRamp Transcodierung können Sie einen Satz von Quell-R ampIDs 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 unter Perform Translation Through ADX auf der LiveRamp Dokumentationswebsite.

In jedem der folgenden Szenarien können Sie eine ID-Zuordnung zwischen zwei Datensätzen 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
- Arbeitsablauf für die ID-Zuordnung zwischen zwei AWS-Konten
- Einen Workflow für die ID-Zuordnung ausführen
- Ausführen eines Workflows zur ID-Zuordnung mit einem neuen Ausgabeziel
- 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 Workflow zur ID-Zuordnung für einen AWS-Kontoermöglicht es Ihnen, die ID-Zuordnung zwischen zwei Datensätzen selbst durchzuführen AWS-Konto.

Bevor Sie selbst einen ID-Mapping-Workflow erstellen AWS-Konto, müssen Sie zuerst 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 zur Erstellung 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 einen ID-Zuordnungs-Workflow für einen erstellen AWS-Konto Wenn Sie entweder die regelbasierte Methode oder die ID-Zuordnungsmethode für Providerdienste verwenden, müssen Sie zunächst Folgendes tun:

- Führen Sie die Aufgaben unter AWSEntitätsauflösung einrichten aus.
- Erstellen Sie eine Schemazuordnung 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, die Ihnen den Zugriff auf den Daten-Staging-Bucket ermöglicht.

```
{
    "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>* mit Ihren eigenen Informationen.

staging-bucket	Der Amazon S3 S3-Bucket, der Ihre Daten vorübergehend speichert, während ein auf Anbieterdiensten basierender Workflow ausgeführt wird.

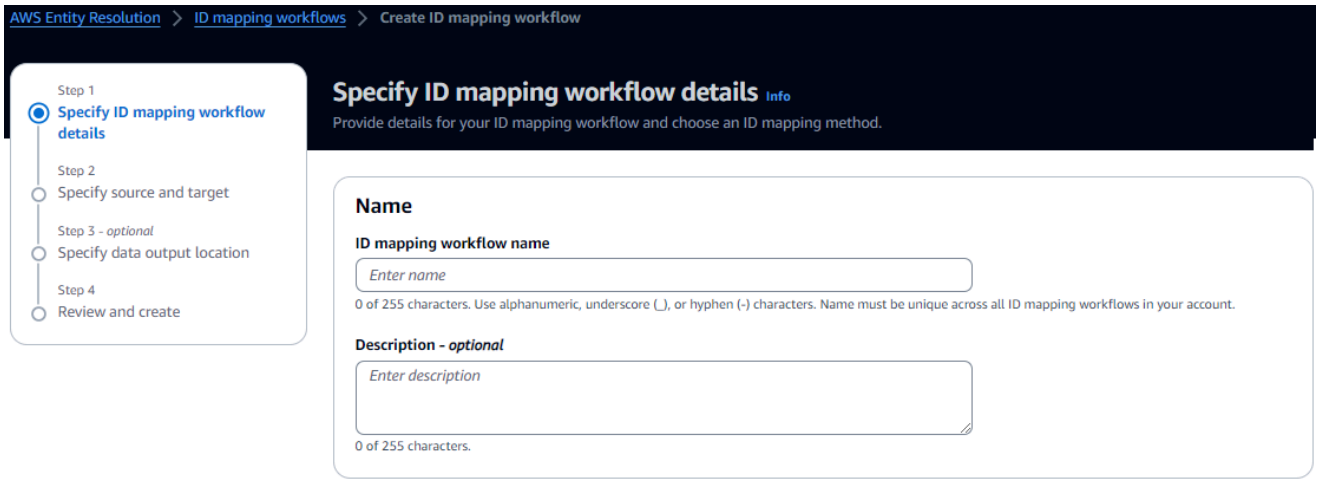
Erstellen eines Workflows zur ID-Zuordnung (regelbasiert)

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

Um einen regelbasierten ID-Zuordnungs-Workflow für einen zu erstellen AWS-Konto

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Mapping 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 die Option Regelbasiert aus.

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

d. Wählen Sie Weiter.

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 Ihre eigene AWS Glue-Datenbank, AWS Glue-Tabelle und Schema-Mapping im ID-Mapping-Workflow.	1. Wählen Sie Schema-Mapping. 2. Wählen Sie ein AWS GlueWählen Sie im Drop-down-Menü die Datenbank AWS Glue Tabelle, und wählen Sie dann das entsprechende Schema-Mapping aus. Sie können bis zu 19 Dateneingaben hinzufügen.

Szenario	Empfohlene Aktion
Verwenden Sie einen vorhandenen Abgleichsworkflow, der auf die Datensatz daten 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. 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 beschränk t, führt dies zu einem Fehler.
Schemazuordnung	Überspringen Sie diesen Schritt.

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

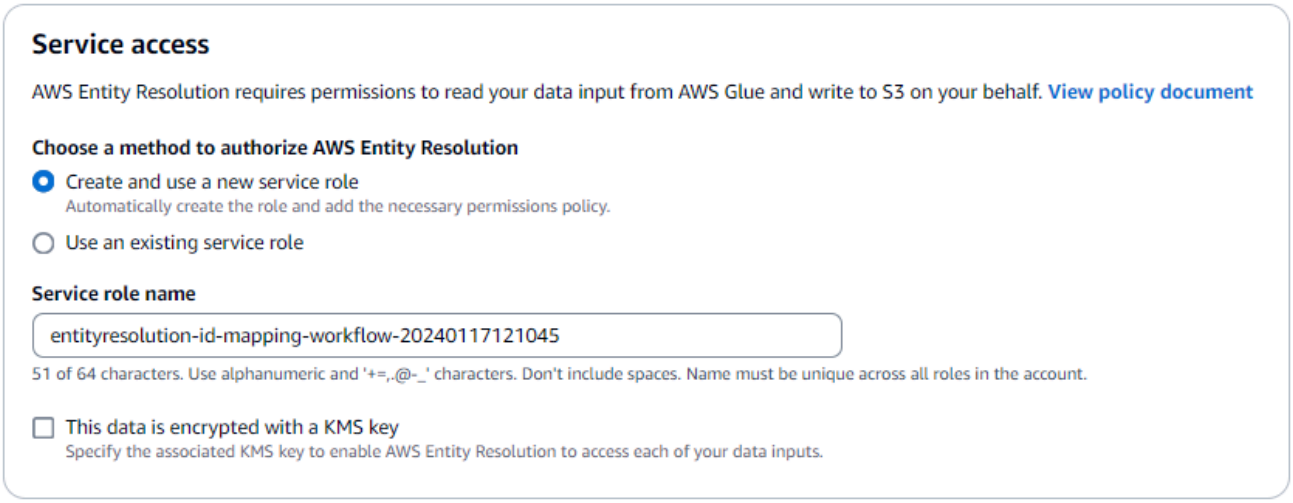
Dies liegt daran, dass beide Teilnehmer diese Option zuvor ausgewählt hatten.

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 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 ein AWS KMS Schlüssel, der zur Entschlüsselung 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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

6. Wählen Sie Weiter.
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 für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS geben Sie den Schlüssel ein ARN oder wählen Sie Create an AWS KMS Schlüssel.
   b. Wählen Sie Weiter.
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 Create (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.

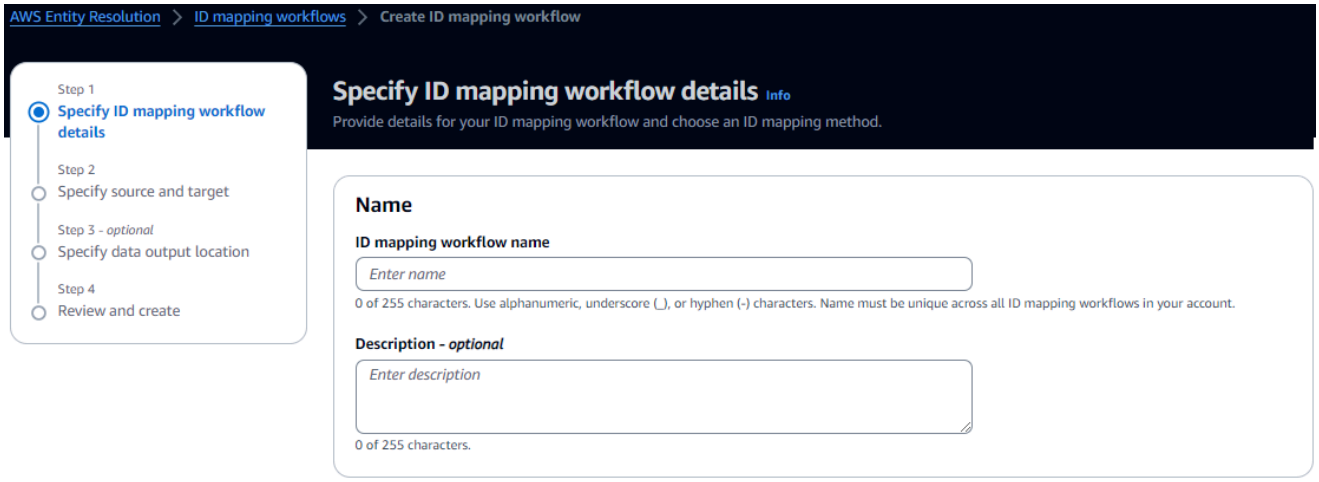
Erstellen eines Workflows für die ID-Zuordnung (Provider-Services)

In diesem Thema wird beschrieben, wie Sie einen Workflow für die ID-Zuordnung für einen Computer erstellen AWS-Konto mithilfe eines Anbieterdienstes namens LiveRamp. LiveRamp übersetzt eine Menge von Quelle R in eine andere MengeampIDs , wobei entweder beibehaltenes oder abgeleitetes R ampIDs verwendet wird.

Um einen auf einem Provider-Service basierenden ID-Zuordnungs-Workflow für einen zu erstellen AWS-Konto

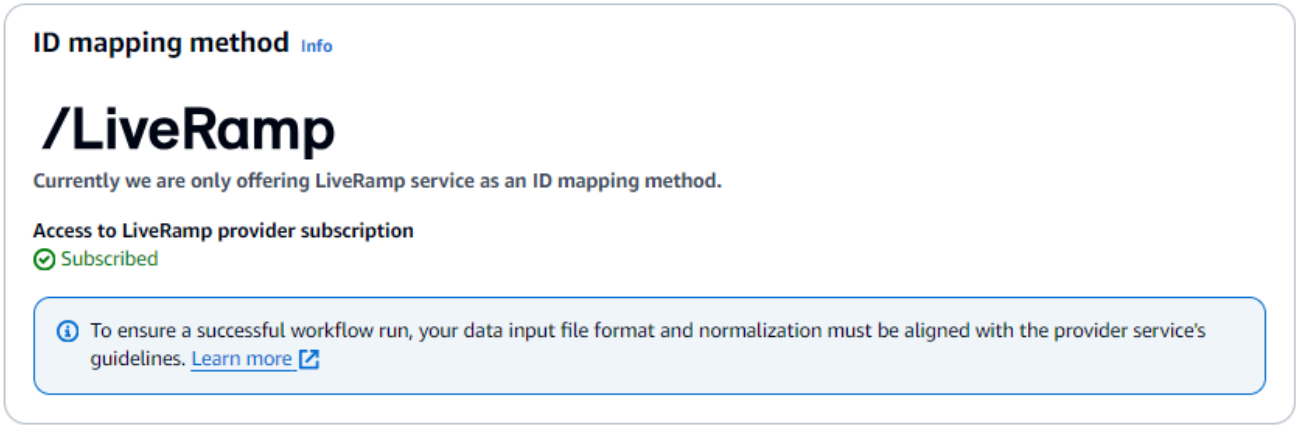
1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Mapping aus.
3. Wählen Sie auf der Seite mit den Workflows für die ID-Zuordnung 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:

- Client-ID-Manager ARN
- Geheimer Manager des Kunden 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.

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.

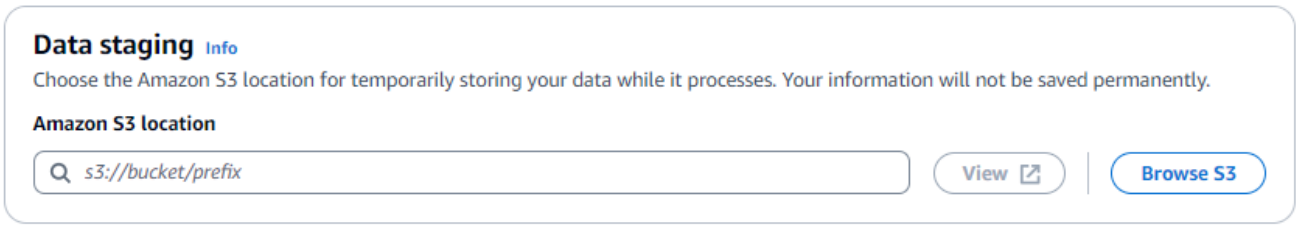
Szenario	Empfohlene Aktion
Verwenden Sie Ihre eigene AWS Glue-Datenbank, AWS Glue-Tabelle und Schema-Mapping im ID-Mapping-Workflow.	1. Wählen Sie Schema-Mapping. 2. Wählen Sie ein AWS GlueWählen Sie im Drop-down-Menü die Datenbank AWS Glue Tabelle, und wählen Sie dann das entsprechende Schema-Mapping aus. Sie können bis zu 19 Dateneingaben hinzufügen.

Szenario	Empfohlene Aktion
Verwenden Sie einen vorhandenen Abgleichsworkflow, der auf die Datensatz daten 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.

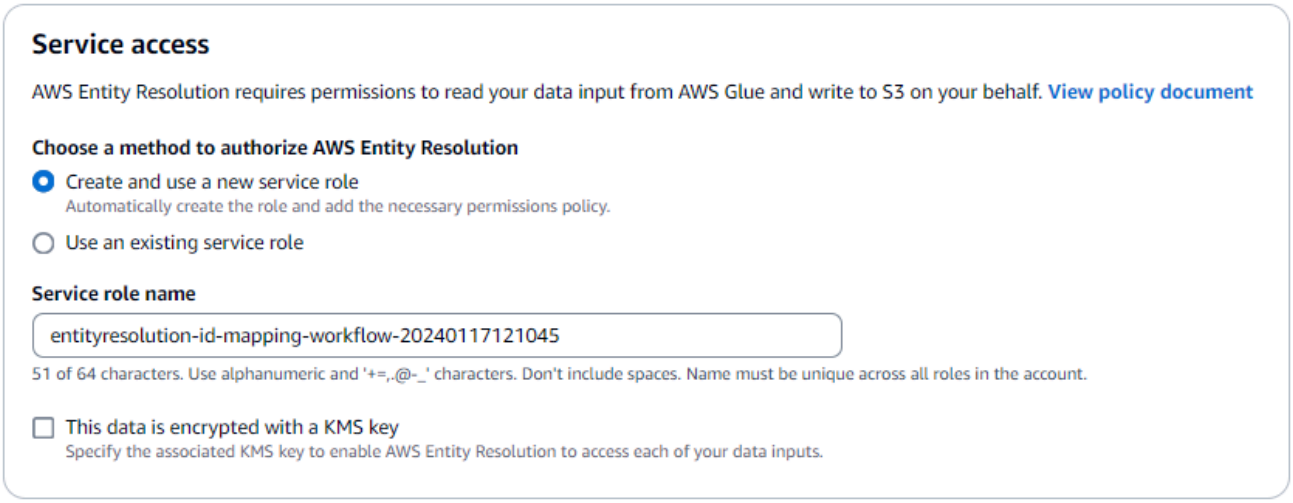
b. Führen Sie für Target je nach der von Ihnen ausgewählten ID-Zuordnungsmethode eine der folgenden Aktionen aus.

Methode zur ID-Zuordnung	Empfohlene Aktion
Regelbasiert	Wählen Sie einen vorhandenen Matching-Workflow aus der Drop-down-Liste aus.
Dienste des Anbieters	Geben Sie die für die Transcodierung vorgesehene LiveRamp Client-Do mänenkennung ein, die LiveRamp in der Zieldomäne bereitgestellt wird. 

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.



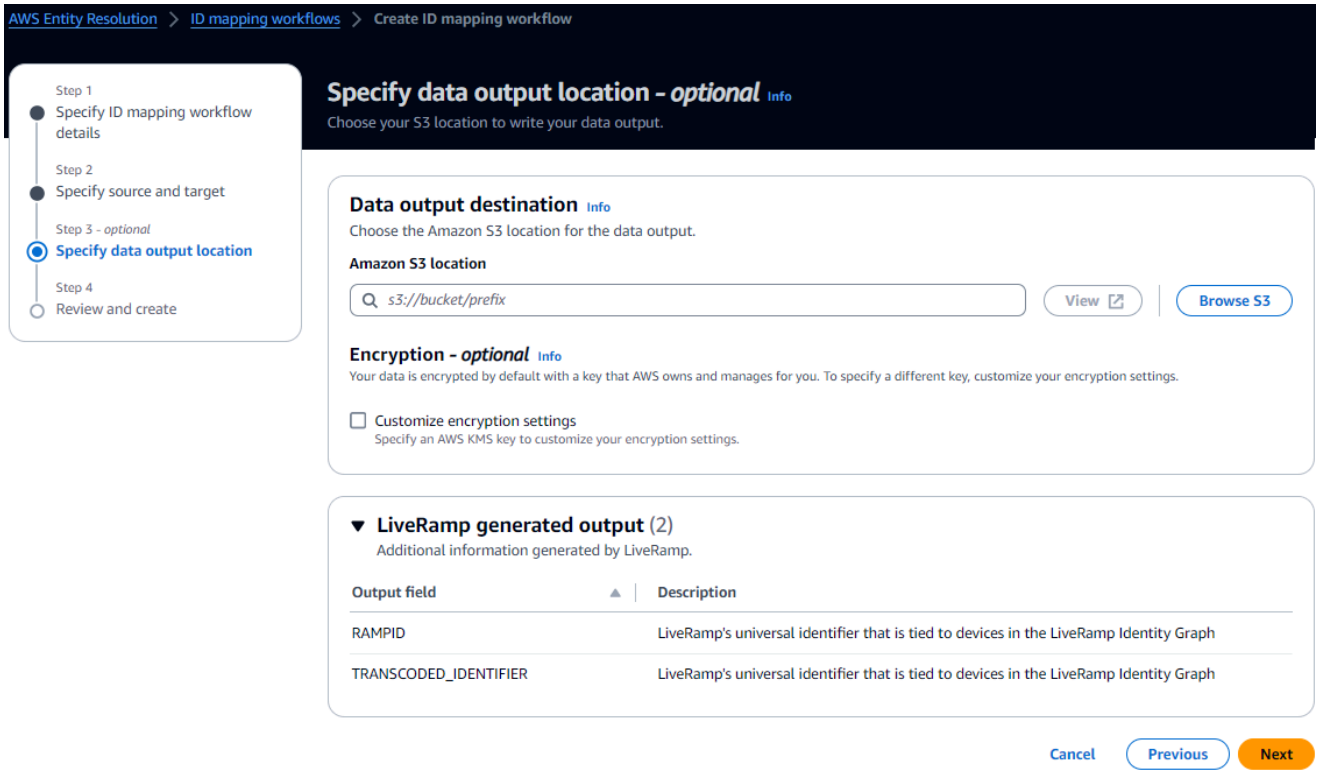
d. Um die Zugriffsberechtigungen für den Service festzulegen, wählen Sie eine Option und ergreifen Sie die empfohlene Maßnahme.



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 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 ein AWS KMS Schlüssel, der zur Entschlüsselung 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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

6. Wählen Sie Weiter.
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 für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS geben Sie den Schlüssel ein ARN oder wählen Sie Create an AWS KMS Schlüssel.
   b. Sehen Sie sich die LiveRamp generierte Ausgabe an.
   c. Wählen Sie Weiter.



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 Create (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.

Arbeitsablauf für die ID-Zuordnung zwischen zwei AWS-Konten

Ein ID-Mapping-Workflow für zwei AWS-Kontenermöglicht es Ihnen, eine ID-Zuordnung zwischen zwei Datensätzen über zwei durchzuführen AWS-Konten. Dies geschieht normalerweise zwischen Ihren eigenen AWS-Konto und noch einer AWS-Konto.

Beispielsweise kann ein Herausgeber einen ID-Mapping-Workflow mit seinem eigenen Ziel-ID-Namespace (in seinem eigenen) erstellen AWS-Konto) und den Quell-ID-Namespace eines Werbetreibenden (in einem anderen AWS-Konto).

Bevor Sie einen Workflow für die ID-Zuordnung erstellen, der zwei Elemente umfasst AWS-Konten, müssen Sie zuerst die Voraussetzungen erfüllen.

Nachdem Sie einen ID-Zuordnungs-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 aus zwei Komponenten besteht AWS-Konten:

Themen

Voraussetzungen

Bevor Sie einen Workflow für die ID-Zuordnung erstellen, der zwei Elemente umfasst AWS-Konten, 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) Erstellen eines Workflows für die ID-Zuordnung zwischen zwei AWS-Konten erfordert die Erlaubnis für LiveRamp den Zugriff auf den S3-Bucket und den AWS Key Management Service (AWS KMS) vom Kunden verwalteter Schlüssel.

  Bevor Sie einen Workflow für die ID-Zuordnung erstellen, der zwei Elemente umfasst AWS-Konten mit LiveRamp fügen Sie die folgende Berechtigungsrichtlinie hinzu, die den LiveRamp Zugriff auf den S3-Bucket und den vom Kunden verwalteten Schlüssel ermöglicht.

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

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

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

<KMSKeyARN>	Das ARN von einem AWS KMS Vom Kunden verwalteter Schlüssel.

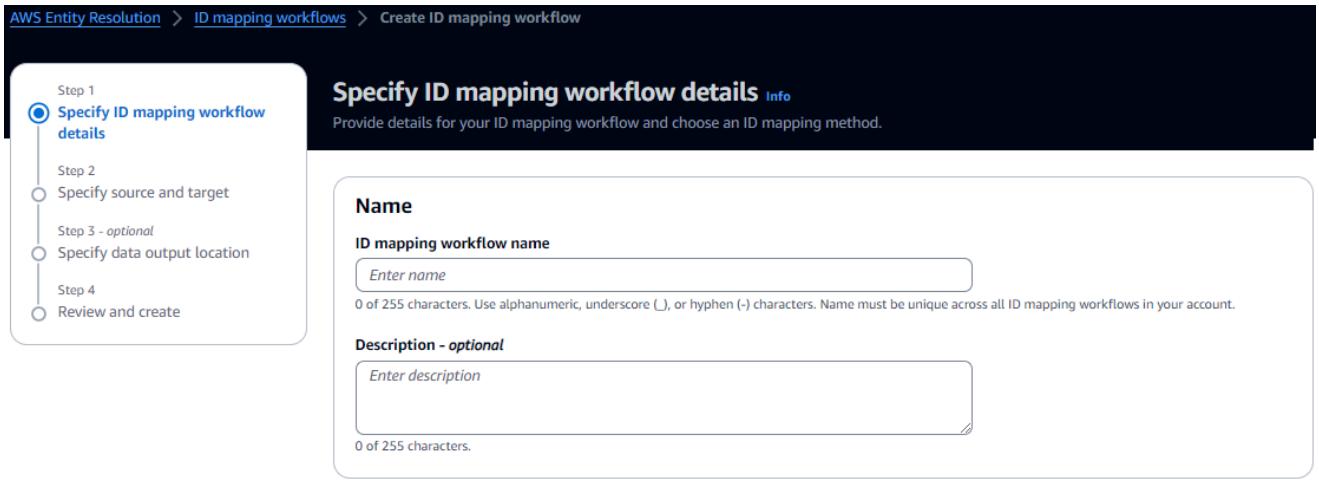
Erstellen eines Workflows zur ID-Zuordnung (regelbasiert)

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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Mapping 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 die Option Regelbasiert aus.

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

d. Wählen Sie Weiter.

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.

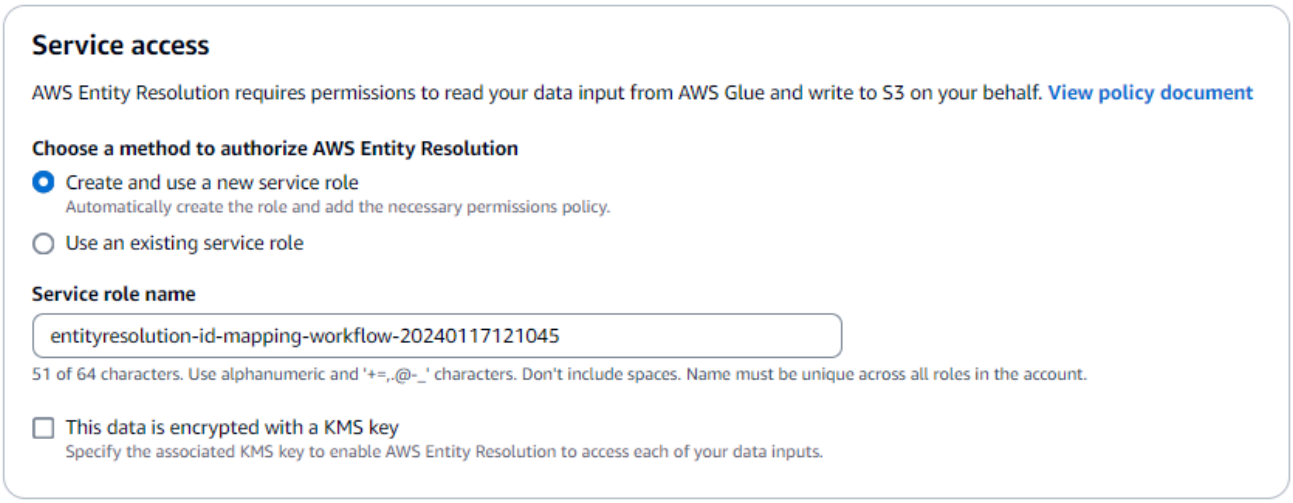
Ihr Ziel	Empfohlene Option
Suchen Sie nach einer beliebigen Kombination von Übereinstimmungen in Daten, die in mehreren Eingabefeldern gespeichert sind, unabhängig davon, ob sich die Daten im selben oder in einem anderen Eingabefeld befinden.	Mehrere Eingabefelder
Beschränken Sie den Vergleich innerhalb eines einzelnen Eingabefe ldes, wenn ähnliche Daten, die in mehreren Eingabefeldern gespeichert sind, nicht abgeglichen werden sollen.	Einzelnes Eingabefeld

ii. Geben Sie den Abgleichstyp 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 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 ein AWS KMS Schlüssel, der zur Entschlüsselung 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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

6. Wählen Sie Weiter.
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 für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS geben Sie den Schlüssel ein ARN oder wählen Sie Create an AWS KMS Schlüssel.
   b. Sehen Sie sich die LiveRamp generierte Ausgabe an.
   c. Wählen Sie Weiter.

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 Create (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.

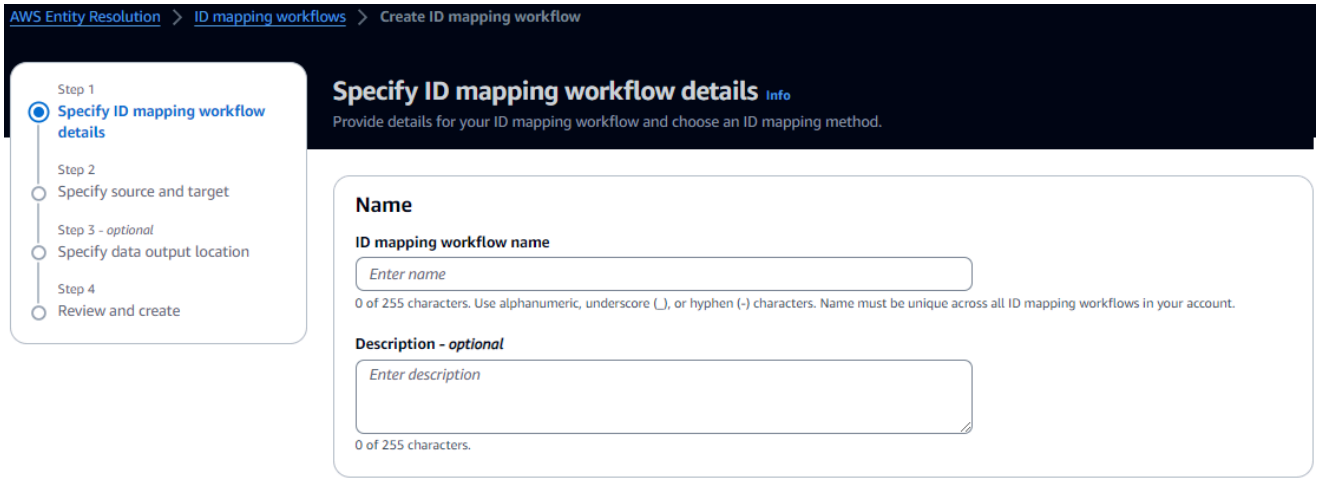
Erstellen eines Workflows für die ID-Zuordnung (Provider-Services)

Nachdem Sie die Voraussetzungen erfüllt haben, können Sie mithilfe des LiveRamp Providerdienstes einen oder mehrere Workflows für die ID-Zuordnung erstellen. LiveRamp übersetzt eine Menge von Quelle R in eine andere MengeampIDs , wobei entweder beibehaltenes oder abgeleitetes R ampIDs verwendet wird.

Um einen ID-Zuordnungs-Workflow mit dem Provider-Service zu erstellen

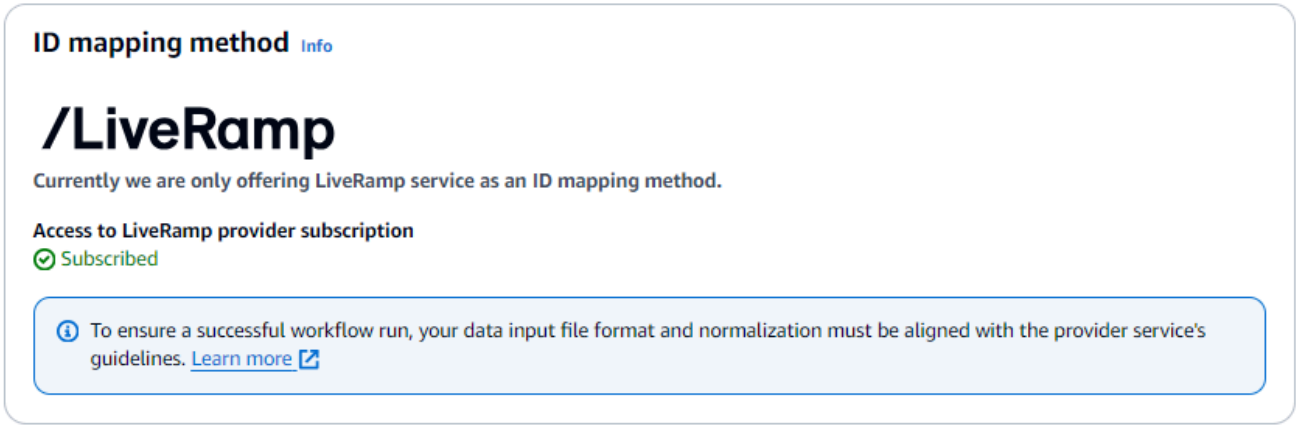
1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Mapping aus.
3. Wählen Sie auf der Seite mit den Workflows für die ID-Zuordnung 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:

- Client-ID-Manager ARN
- Geheimer Manager des Kunden ARN

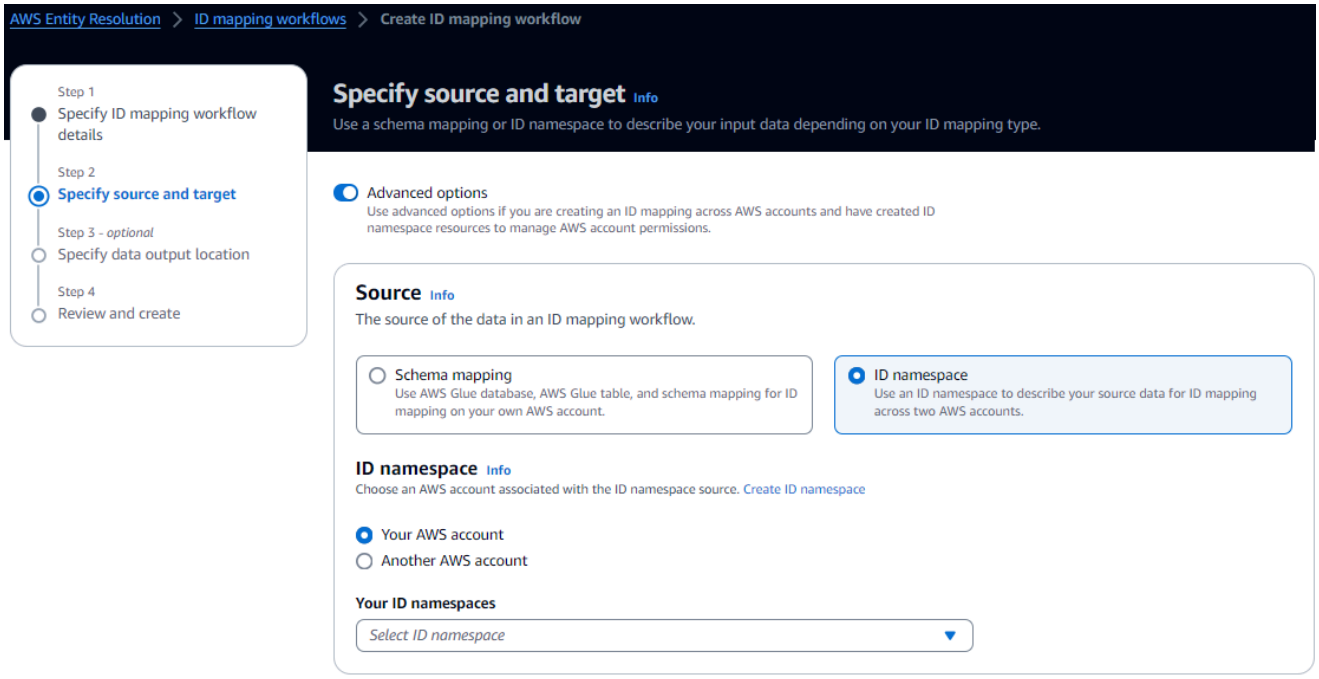
d. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

e. Wählen Sie Weiter.

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

a. Aktivieren Sie „Erweiterte Optionen“.

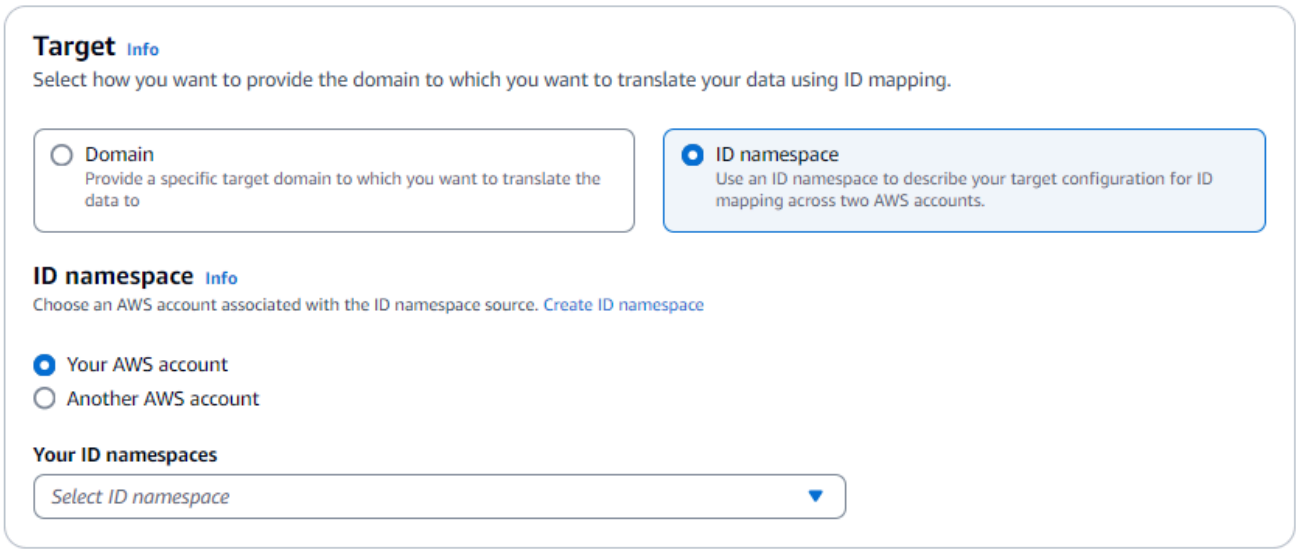
b. Wählen Sie als Quelle den ID-Namespace aus.



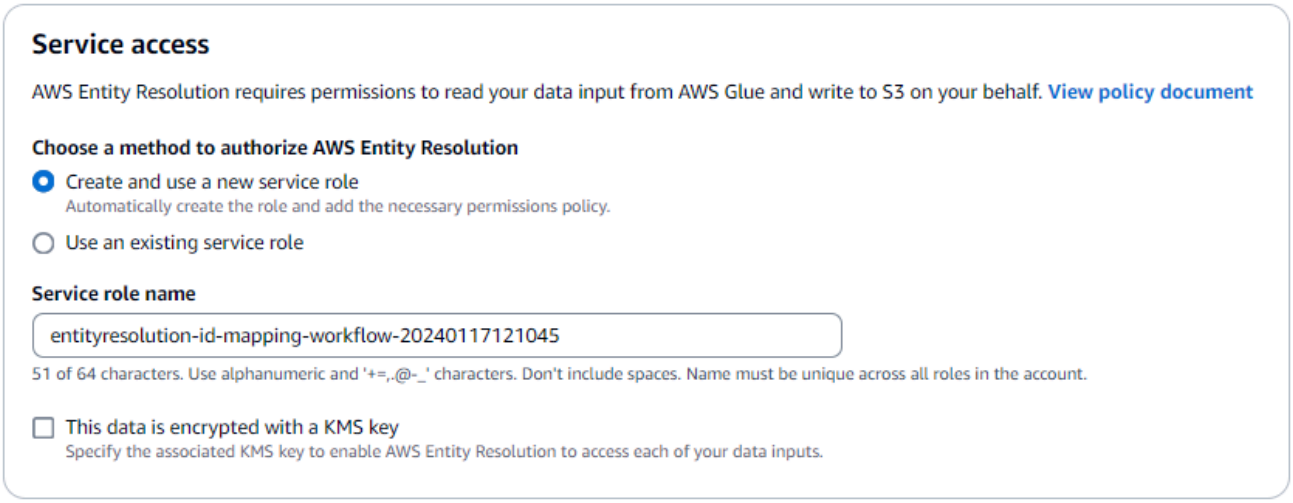
c. Identifizieren Sie für ID-Namespace, wo sich der ID-Namespace befindet, und ergreifen Sie dann die empfohlene Maßnahme.

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.



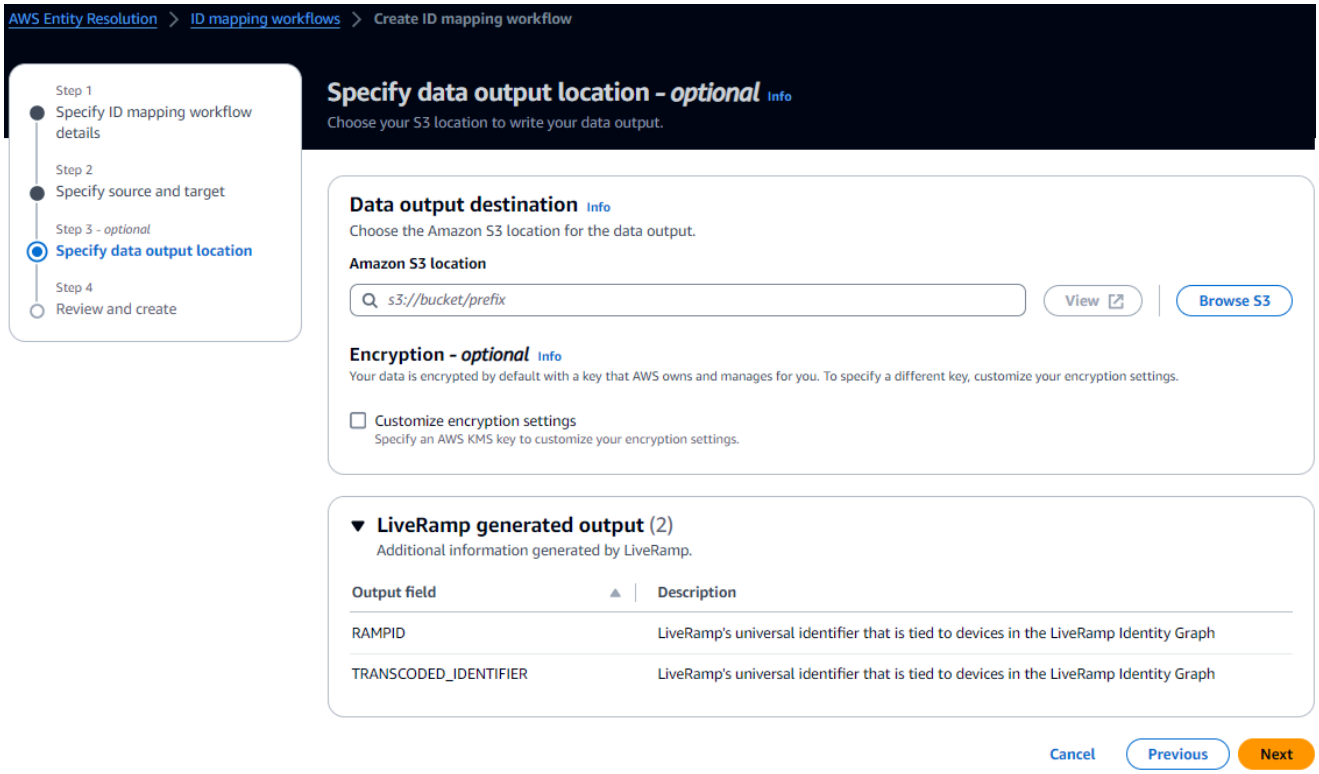
e. Um die Dienstzugriffsberechtigungen anzugeben, wählen Sie eine Option und ergreifen Sie die empfohlene Maßnahme.



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 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 ein AWS KMS Schlüssel, der zur Entschlüsselung 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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

6. Wählen Sie Weiter.
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 für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS geben Sie den Schlüssel ein ARN oder wählen Sie Create an AWS KMS Schlüssel.
   b. Sehen Sie sich die LiveRamp generierte Ausgabe an.
   c. Wählen Sie Weiter.



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 Create (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.

Einen Workflow für die ID-Zuordnung ausführen

Nachdem Sie einen ID-Mapping-Workflow für einen erstellt haben AWS-Kontooder erstellen Sie einen Workflow für die ID-Zuordnung, der zwei Elemente umfasst AWS-Konten, können Sie den ID-Mapping-Workflow ausführen. Der ID-Zuordnungs-Workflow gibt eine CSV Datei aus.

Um einen ID-Mapping-Workflow auszuführen

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Mapping 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
   - 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

   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 dem verbinden`TRANSCODED_ID`.

Ausführen eines Workflows zur ID-Zuordnung mit einem neuen Ausgabeziel

Nachdem Sie einen ID-Mapping-Workflow für einen erstellt haben AWS-Kontooder erstellen Sie einen Workflow für die ID-Zuordnung, der zwei Elemente umfasst AWS-Konten, Sie können einen anderen S3-Speicherort wählen, um Ihre Datenausgabe zu schreiben.

Um einen ID-Mapping-Workflow mit einem neuen Ausgabeziel auszuführen

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Mapping 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 aus der Dropdownliste Workflow ausführen die Option Mit neuem Ausgabeziel ausführen aus.
5. Gehen Sie für das Datenausgabeziel wie folgt vor.

   a. Wählen Sie den Amazon S3 S3-Standort für die Datenausgabe.

   b. Wenn Sie für Verschlüsselung die Option Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS geben Sie den Schlüssel ein ARN oder wählen Sie Create an AWS KMS Schlüssel.
6. 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 Richtlini e für diese Tabelle. • Der Standardname der Servicerolle lautet`entityresolution-id-mapping-workflow-<timestamp>` . • Sie müssen über die erforderlichen Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüs selt sind, wählen Sie die Option Diese Daten werden mit einem KMS Schlüssel verschlüsselt. Geben Sie dann ein AWS KMS Schlüssel, der zur Entschlüsselung 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 den Link In IAM extern anzeigen wählen. Standardmäßig AWS Entity Resolution versucht nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderlichen Berechtigungen hinzuzufügen.

7. Wählen Sie Ausführen aus.
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

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 dem verbinden`TRANSCODED_ID`.

Bearbeitung eines Workflows zur ID-Zuordnung

So bearbeiten Sie einen Workflow für die ID-Zuordnung:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Mapping 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

So löschen Sie einen Workflow für die ID-Zuordnung:

1. Melden Sie sich an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Mapping 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 an bei AWS Management Console und öffne das AWS Entity Resolution Konsole mit deinem AWS-Konto, falls du es noch nicht getan hast.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Mapping 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.

Integrieren mit AWS Entity Resolution als Anbieter

AWS Entity Resolution Integrationen von Drittanbietern helfen Kunden dabei, die Privatsphäre der Verbraucher zu schützen und die Gesetze zur Datenhoheit einzuhalten. 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 andere Länder exportiert werden AWS verwaltete Systeme. Dieser Abschnitt enthält Anleitungen für Anbieter zur Integration AWS Entity Resolution zur Kodierung oder Transkodierung von Verbraucher-Identifikatoren in Werbung IDs zur Verwendung in einem auf Anbieterdiensten basierenden Matching-Workflow.

Weitere Informationen zu den Anbieterdiensten, die derzeit integriert sind in AWS Entity Resolution, finden Sie unter Einen auf Provider-Services basierenden Abgleichs-Workflow erstellen.

Themen

Voraussetzungen

Vor der Integration als Dienstanbieter mit AWS Entity Resolution, erfüllen Sie die folgenden Anforderungen.

Themen

Einen Anbieterdienst auflisten auf AWS Data Exchange

Als Drittanbieter müssen Sie Ihr Produkt im AWSData Exchange (ADX) -Produktkatalog auflisten. Nachdem Ihr Produkt auf der AWS Data Exchange Im Produktkatalog können Abonnenten Ihr Produkt entweder über ein öffentliches oder ein privates Angebot abonnieren.

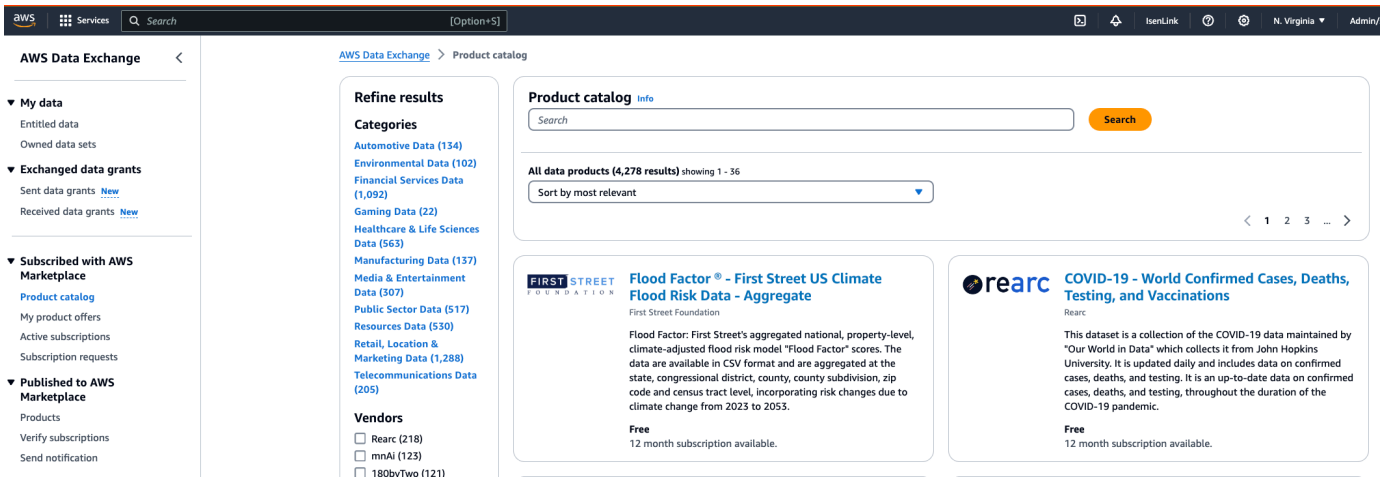
Um einen Anbieterdienst aufzulisten auf AWS Data Exchange

1. Wenn Sie ein neuer Anbieter von Datenprodukten sind AWS Data Exchange, führen Sie die Schritte im Abschnitt Erste Schritte als Anbieter in der AWS Data Exchange Benutzerleitfaden.
2. Erstellen Sie einen REST API Datensatz und veröffentlichen Sie ein neues Produkt, das Folgendes enthält APIs AWS Data Exchange indem Sie die Schritte im Abschnitt So veröffentlichen Sie ein Produkt befolgen, das APIs in AWS Data Exchange Benutzerleitfaden. Sie können den Vorgang abschließen, indem Sie entweder AWS Data Exchange Konsole oder 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 gesetzt haben, führen Sie die Schritte im Abschnitt Benutzerdefinierte Angebote erstellen in der AWS Data Exchange Benutzerhandbuch, abhängig von Ihrem Anwendungsfall.

   Die folgende Abbildung zeigt ein Beispiel für ein verfügbares Produkt in AWS Data Exchange Produktkatalog.



3. Nachdem das Produkt auf der AWS Data Exchange Im Produktkatalog 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.
   - Verwenden Sie das Angebot „Bring Your Own“ -Abonnement (BYOS).

Weitere Informationen finden Sie unter Abonnieren und Zugreifen auf ein Produkt, das APIs in der AWS Data Exchange Benutzerleitfaden.

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 an die AWS Entity Resolution Business Development-Team unter `<aws-entity-resolution-bd@amazon .com>` zur weiteren Überprüfung, bevor Sie fortfahren.

Fordern Sie das an AWS Entity Resolution APISpezifikation öffnen

AWS Entity Resolution hat eine API Open-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 APISpezifikation öffnen.

Um die API Open-Definition anzufordern, wenden Sie sich an AWS Entity Resolution Team für Geschäftsentwicklung unter `<aws-entity-resolution-bd@amazon .com>`.

Verwendung der AWS Entity Resolution APISpezifikation öffnen

Die API Open-Spezifikation definiert alle Protokolle, die mit verknüpft sind AWS Entity Resolution. Diese Spezifikation ist notwendig, um die Integration zu implementieren.

Die API Open-Definition enthält die folgenden API Operationen:

- `POST AssignIdentities`
- `POST CreateJob`
- `GET GetJob`
- `POST StartJob`
- `POST MapIdentities`
- `GET Schema`

Um die API Open-Spezifikation anzufordern, wenden Sie sich an AWS Entity Resolution Team für Geschäftsentwicklung unter `<aws-entity-resolution-bd@amazon .com>`.

Die API Open-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 API Open-Spezifikation erhalten haben, implementieren Sie die Art der Verarbeitungsintegration für Ihren Anwendungsfall.

Themen

Integration der Stapelverarbeitung

Die Integration der Stapelverarbeitung folgt einem asynchronen Entwurfsmuster. Nachdem ein Workflow initiiert wurde am AWS Data Exchange, übermittelt 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 verfügbar ist über AWS Data Exchange in der folgenden Reihenfolge:

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.

Dies 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`: Dadurch weiß API der Anbieter, dass er den Job auf der Grundlage der `JobId` bereitgestellten Daten starten soll. Auf diese Weise kann der Anbieter alle erforderlichen Validierungen von bis `CreateJob` durchführen. `StartJob`

Dies API gibt a`JobId`, das `Status` für den Jobstatus`Message`, 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`: Das API informiert AWS Entity Resolution ob der Job abgeschlossen wurde oder ein anderer Status.

   Dies API gibt a`JobId`, das `Status` für den Jobstatus`Message`, das und zurück`statusCode`.

   Beispielanforderung für die Kodierung

   ```
   GET /jobs/{jobId}
   ```

   Beispielantwort

   ```
   {
     "jobId": "string",
     "status": "PENDING",
     "statusMessage": "string",
     "statusCode": 200
   }
   ```

Die vollständige Definition dieser APIs Informationen finden Sie in AWS Entity Resolution Öffnen Sie die API Spezifikation.

Integration der synchronen Verarbeitung

Die Lösung für die synchrone Verarbeitung ist für Anbieter wünschenswerter, die über eine Reaktionszeit nahezu in Echtzeit mit einer Reaktionszeit in Echtzeit mit höherem Durchsatz und mehr verfügen. TPS Dieser AWS Entity Resolution Ein Workflow partitioniert den Datensatz und stellt mehrere API Anfragen parallel. Das Tool AWS Entity Resolution Der Workflow kümmert sich dann um 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`: Dadurch werden Daten unter Verwendung einer `source_id` Kennung, die diesem Datensatz `recordFields` zugeordnet ist, an den Anbieter API gesendet.

Dies API gibt den 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 dieser APIs Informationen finden Sie in AWS Entity Resolution Öffnen Sie die API Spezifikation.

Je nachdem, welchen Ansatz der Anbieter wählt, AWS Entity Resolution erstellt eine Konfiguration für den Anbieter, der für die Initiierung der Kodierung oder Transcodierung verwendet wird. Darüber hinaus stehen diese Konfigurationen den Kunden zur Verfügung, die die von APIs bereitgestellten AWS Entity Resolution.

Auf diese Konfiguration kann über einen Amazon-Ressourcennamen (ARN) zugegriffen werden, der von der Stelle abgeleitet ist, an der das Serviceangebot des Anbieters am AWS Data Exchange wird gehostet, und der Typ des Anbieterdienstes. AWS Entity Resolution bezeichnet dies ARN als`providerServiceARN`.

Testen einer Anbieterintegration

Während AWS Entity Resolution hostet Datenabgleichsdienste, eine Anbieterintegration ist jedoch eine wichtige Drittanbieterkomponente für den end-to-end Abgleichs-Workflow. Es gibt mehrere Tests, die AWS Entity Resolution hat für die Anbieter definiert, dass eine Schutzmaßnahme hinzugefügt wird, falls 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 der auszuführen AWS Entity Resolution Software-Entwicklungskit (SDK). Wenn es irgendwelche Probleme von Anbietern gibt, AWS Entity Resolution verwendet den bevorzugten Eskalationspfad, um das Problem zu eskalieren. Darüber hinaus müssen die Anbieter ihre eigene

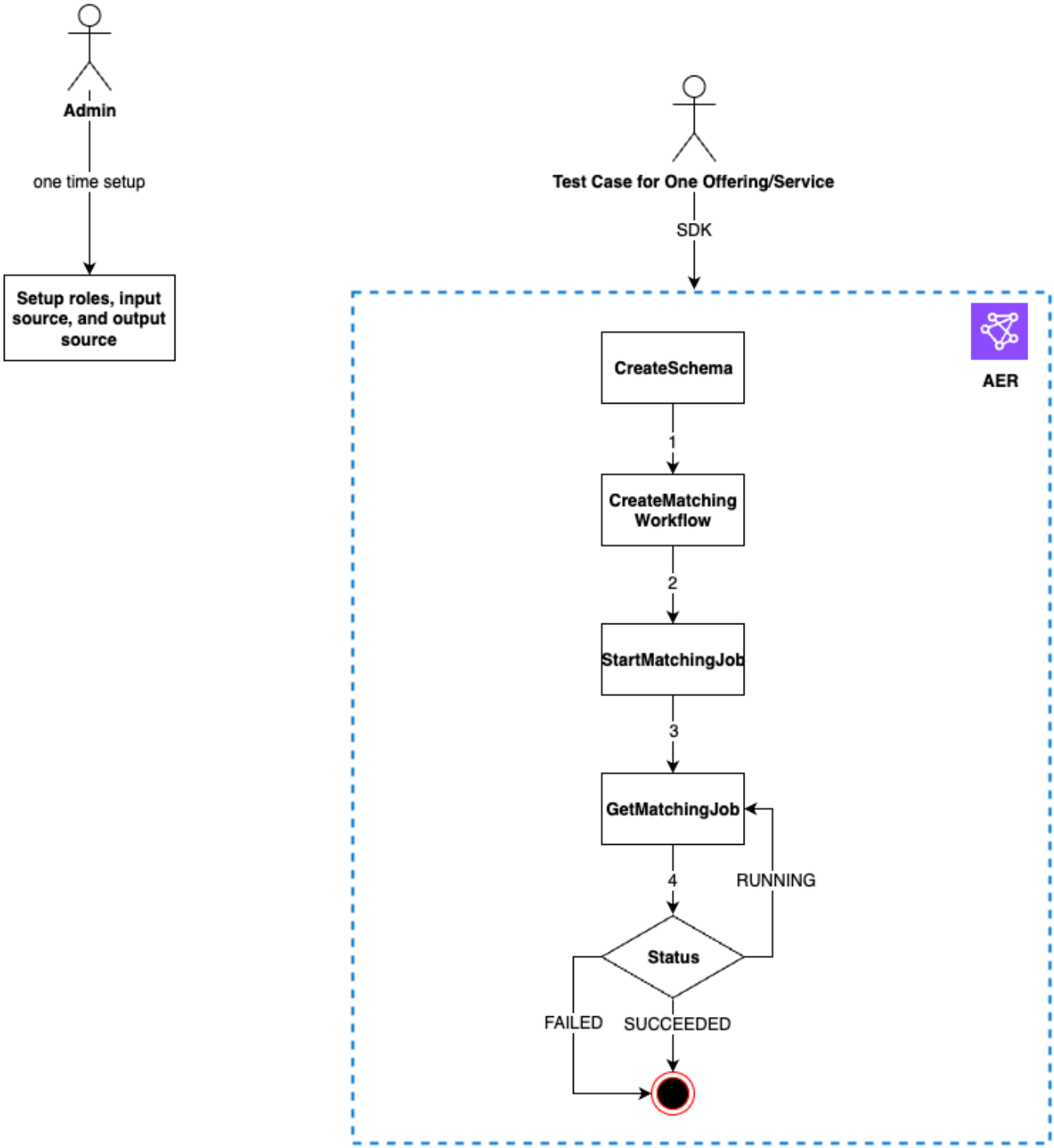
Überwachung der Testergebnisse einrichten. Die Anbieter müssen ihre AWS-Konto IDsdie verwendet werden, um diese Tests durchzuführen mit AWS Entity Resolution.

Ein erfolgreicher Lauf bedeutet, dass ein Anbieter seine Daten einrichten und seinen eigenen Dienst nutzen kann AWS Entity Resolution, und der Auftragsstatus wird ohne Fehler auf Abgeschlossen zurückgesetzt. Dies kann programmgesteuert mit dem bereitgestellten Befehl erreicht werden APIs 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 entscheiden sich Anbieter für ihre Dienste, die über angeboten werden, SDK und führen einen end-to-end Test für sie durch AWS Data Exchange mithilfe ihrer Testkonten. Von den Anbietern wird erwartet, dass sie diese Tests für jedes ihrer Angebote oder Dienste durchführen.

> **Note**
>
> Anbieter müssen Folgendes bereitstellen AWS Entity Resolution die AWS-Konto ID (`accountId`)die sie verwenden, um diese Workflows zu Testzwecken auszuführen. Darüber hinaus müssen Anbieter diese Tests überwachen und sicherstellen, dass sie erfolgreich sind. Das bedeutet, dass Anbieter bei Ausfällen Benachrichtigungen 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 ein für 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 dem zu testen AWS Entity Resolution Konsole oderAPIs.

2. Testen Sie die Anbieterintegration entweder mit AWS Entity Resolution APIsoder Konsole.

API

Um eine Anbieterintegration mit dem zu testen AWS Entity Resolution APIs

1. Erstellen Sie eine Schemazuordnung mit dem CreateSchemaMapping API. Eine vollständige Liste der unterstützten Programmiersprachen finden Sie im Abschnitt Siehe auch der CreateSchemaMapping API.

   Schema-Mapping ist der Prozess, anhand dessen Sie Folgendes feststellen AWS Entity Resolution wie Sie Ihre Daten für den Abgleich interpretieren. 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 enthält **`id`** und **`email`** verwendet SDK

Im Folgenden finden Sie ein Beispiel für eine Schemazuordnung für eine Datenquelle, die Java enthält `id` und `email` verwendetSDK:

```
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 einen passenden Workflow mit dem CreateMatchingWorkflow API. Eine vollständige Liste der unterstützten Programmiersprachen finden Sie im Abschnitt Siehe auch der CreateMatchingWorkflow API.

   Example Einen passenden Workflow mit Java erstellen SDK

   Im Folgenden finden Sie ein Beispiel für einen passenden Workflow unter Verwendung von JavaSDK:

```
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 einen passenden Workflow mit dem aus StartMatchingJob API. 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 Java ausführen SDK

   Im Folgenden finden Sie ein Beispiel für einen laufenden Matching-Workflow unter Verwendung von JavaSDK:

   ```
   EntityResolutionClient.startMatchingJob(StartMatchingJobRequest.builder()
                   .workflowName(<name-of-workflow-from-step3)
                   .build()
   )
   ```

4. Überwachen Sie den Status eines Workflows mithilfe von GetMatchingJob API.

Dadurch werden der Status, die Metriken und Fehler (falls vorhanden) API zurückgegeben, die mit einem Job verknüpft sind.

Example Überwachung eines passenden Workflows mithilfe von Java SDK

Im Folgenden finden Sie ein Beispiel für die Überwachung eines passenden Workflow-Jobs mithilfe von JavaSDK:

```
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 dem zu testen AWS Entity Resolution Konsole

1. Erstellen Sie eine Schemazuordnung, indem Sie die Schritte unter befolgenEine Schema-Mapping erstellen.

   Schema-Mapping ist der Prozess, anhand dessen Sie Folgendes feststellen AWS Entity Resolution wie Sie Ihre Daten für den Abgleich interpretieren. Sie definieren das Schema der gewünschten Eingabedatentabelle AWS Entity Resolution zum Einlesen in einen passenden Workflow.

   Bei der Erstellung einer Schemazuordnung muss jeder Zeile mit Eingabedaten ein eindeutiger Bezeichner zugewiesen werden AWS Entity Resolution liest. 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 auszuführenEinen auf Provider-Services basierenden Abgleichs-Workflow erstellen.

   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, wenn ein Konto über ein Abonnement bei einem Anbieterdienst verfügt AWS Data Exchange, können Sie 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.

   Das Tool AWS Entity Resolution Die 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 Metriken für den letzten Job 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 IDsgenerierte 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

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die eingerichtet wurden, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für AWS Entity Resolution gelten, finden Sie unter Im Rahmen des Compliance-Programms zugelassene AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den 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 geteilten Verantwortung bei der Verwendung von AWS Entity Resolution einsetzen können. Die folgenden Themen veranschaulichen, wie Sie AWS Entity Resolution zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren außerdem, wie Sie andere AWS-Services verwenden, um Ihre AWS Entity Resolution-Ressourcen zu überwachen und zu schützen.

Themen

Datenschutz in AWS Entity Resolution

Das Tool AWS Modell der der 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

AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre Inhalte zu behalten, die auf dieser Infrastruktur gehostet werden. Sie sind auch verantwortlich für die Sicherheitskonfiguration und die Verwaltungsaufgaben für AWS-Services die Sie verwenden. Weitere Informationen zum Datenschutz finden Sie in der Datenschutzerklärung FAQ. Informationen zum Datenschutz in Europa finden Sie auf der AWS Modell der geteilten Verantwortung und GDPR Blogbeitrag auf der AWS Blog zum Thema Sicherheit.

Aus Datenschutzgründen empfehlen wir Ihnen, AWS-Konto Anmeldeinformationen und richten Sie einzelne Benutzer ein mit AWS IAM Identity Center or AWS Identity and Access Management (IAM). 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).
- Verwenden SieSSL/TLS, um mit zu kommunizieren AWS Ressourcen schätzen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail. Für Informationen zur Verwendung von CloudTrail Spuren zum Erfassen AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden in der AWS CloudTrail Benutzeranleitung.
- 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 FIPS 140-3 validierte kryptografische Module benötigen AWS über eine Befehlszeilenschnittstelle oder einenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten 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. Dazu gehört auch, wenn Sie mit arbeiten AWS Entity Resolution oder andere AWS-Services mit der KonsoleAPI, AWS CLI, oder AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu validieren.

Datenverschlüsselung im Ruhezustand für AWS Entity Resolution

AWS Entity Resolution bietet standardmäßig Verschlüsselung zum Schutz vertraulicher Kundendaten im Speicher mithilfe von AWS eigene Verschlüsselungsschlüssel.

AWSeigene Schlüssel — AWS Entity Resolution verwendet diese Schlüssel standardmäßig, um persönlich identifizierbare Daten automatisch zu verschlüsseln. Sie können es nicht anzeigen, verwalten oder verwenden AWS Sie besaßen Schlüssel oder überprüfen deren Verwendung. Sie müssen jedoch keine Maßnahmen ergreifen, um die Schlüssel zu schützen, mit denen Ihre Daten verschlüsselt werden. Weitere Informationen finden Sie unter AWSEigene Schlüssel im AWS Key Management Service Leitfaden für Entwickler.

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 sensiblen 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 in der AWS Key Management Service Leitfaden für Entwickler.

Weitere Informationen zur AWS KMS, siehe 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 Sie eine CreateGrantAnfrage senden an AWS KMS. Zuschüsse in AWS KMS werden verwendet, um zu geben AWS Entity Resolution Zugriff auf einen KMS Schlüssel in einem Kundenkonto. AWS Entity Resolution erfordert den Zuschuss, um Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen zu verwenden:

- Senden Sie GenerateDataKeyAnfragen an AWS KMS um Datenschlüssel zu generieren, 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 du das tust, AWS Entity Resolution kann auf 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 Servicezugriff auf Ihren Schlüssel durch die Gewährung entfernen und versuchen, einen Job für einen passenden, mit einem Kundenschlüssel verschlüsselten Workflow zu starten, würde der Vorgang einen `AccessDeniedException` Fehler zurückgeben.

Einen vom Kunden verwalteten Schlüssel erstellen

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen, indem Sie den AWS Management Console, oder das AWS KMS APIs.

Einen symmetrischen kundenverwalteten Schlüssel erstellen

AWS Entity Resolution unterstützt die Verschlüsselung mit symmetrischen KMS Verschlüsselungsschlüsseln. Folgen Sie den Schritten zum Erstellen eines symmetrischen, vom Kunden verwalteten Schlüssels in AWS Key Management Service Leitfaden für Entwickler.

Wichtige Grundsatzerklärung

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 vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Verwaltung des Zugriffs auf vom Kunden verwaltete Schlüssel in der AWS Key Management Service Leitfaden für Entwickler.

Um Ihren vom Kunden verwalteten Schlüssel mit Ihrem zu verwenden AWS Entity Resolution Ressourcen, die folgenden API Operationen müssen in der Schlüsselrichtlinie zulässig sein:

- `kms:DescribeKey`— Stellt Informationen wie den SchlüsselARN, das Erstellungsdatum (und gegebenenfalls das Löschdatum), den Schlüsselstatus und das Herkunfts- und Ablaufdatum (falls vorhanden) des Schlüsselmaterials bereit. Es enthält z. B. Felder`KeySpec`, mit denen Sie verschiedene KMS Schlüsseltypen unterscheiden können. Außerdem werden die Schlüsselverwendung (Verschlüsselung, Signierung oder Generierung und ÜberprüfungMACs) und die vom KMS Schlüssel unterstützten Algorithmen angezeigt. AWS Entity Resolution bestätigt, dass das `KeySpec` ist `SYMMETRIC_DEFAULT` und `KeyUsage` ist. `ENCRYPT_DECRYPT`
- `kms:CreateGrant`: Fügt einem kundenverwalteten Schlüssel eine Erteilung hinzu. Gewährt Kontrollzugriff auf einen bestimmten KMS Schlüssel, der den Zugriff auf Grant-Operationen ermöglicht AWS Entity Resolution erfordert. Weitere Informationen zur Verwendung von Zuschüssen finden Sie im AWS Key Management Service Leitfaden für Entwickler.

Das ermöglicht AWS Entity Resolution um Folgendes zu 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.
- Richten Sie einen Principal ein, der in den Ruhestand geht, `RetireGrant` damit der Dienst

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 KMS Standardschlüsselrichtlinie jedem Benutzer, der Zugriff auf die erforderlichen KMS Aktionen hat, 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 eine DescribeKeyund eine CreateGrantAnfrage an AWS KMS in Ihrem Namen. Dies setzt voraus, dass die IAM Entität, die die `CreateMatchingWorkflow` Anfrage mit einem vom Kunden verwalteten KMS Schlüssel stellt, über die `kms:DescribeKey` erforderlichen Berechtigungen für die KMS Schlüsselrichtlinie verfügt.

Während einer `CreateIdMappingWorkflowStartIdMappingJob`AND-Anfrage AWS Entity Resolution sendet eine DescribeKeyund eine CreateGrantAnfrage an AWS KMS in Ihrem Namen. Dies setzt voraus, dass die IAM Entität, die den `CreateIdMappingWorkflow` und die `StartIdMappingJob` Anfrage mit einem vom Kunden verwalteten KMS Schlüssel stellt, über die `kms:DescribeKey` erforderlichen Berechtigungen für die KMS Schlüsselrichtlinie verfügt. Anbieter können auf den vom Kunden verwalteten Schlüssel zugreifen, um die darin enthaltenen Daten zu entschlüsseln AWS Entity Resolution Amazon-S3-Bucket.

Im Folgenden finden Sie Beispiele für Richtlinienerklärungen, die Sie hinzufügen können, damit Anbieter die Daten in der AWS Entity Resolution Amazon S3 S3-Bucket:

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

Ersetzen Sie jeden *<user input placeholder>* mit Ihren eigenen Informationen.

<KMSKeyARN>	AWS KMS Amazon-Ressourcenname.

Ähnlich verhält es sich mit der IAM Entität, die das `StartMatchingJobAPI`Must Have `kms:Decrypt` und die `kms:GenerateDataKey` Berechtigungen für den vom Kunden verwalteten KMS Schlüssel aufruft, die im entsprechenden Workflow bereitgestellt wurden.

Weitere Informationen zum Angeben von Berechtigungen in einer Richtlinie finden Sie in AWS Key Management Service Leitfaden für Entwickler.

Weitere Informationen zur Fehlerbehebung beim Zugriff auf Schlüssel finden Sie im AWS Key Management Service Leitfaden für Entwickler.

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 KMSArn, indem Sie einen eingeben AWS Entity Resolution verwendet, um die von der Ressource gespeicherten identifizierbaren persönlichen Daten zu verschlüsseln.

KMSArn— Geben Sie einen Schlüssel einARN, bei dem es sich um eine Schlüssel-ID für einen AWS KMS vom Kunden verwalteter Schlüssel.

Sie können einen vom Kunden verwalteten Schlüssel als zweite Verschlüsselungsebene für die folgenden Ressourcen angeben, wenn Sie einen ID-Mapping-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 ID-Zuordnungs-Workflow-Job starten, können Sie den Datenschlüssel angeben, indem Sie einen eingeben KMSArn, welcher AWS Entity Resolution verwendet, um die von der Ressource gespeicherten identifizierbaren persönlichen Daten zu verschlüsseln.

KMSArn— Geben Sie einen Schlüssel einARN, bei dem es sich um eine Schlüssel-ID für einen AWS KMS vom Kunden verwalteter Schlüssel.

Überwachen Sie Ihre Verschlüsselungsschlüssel für AWS Entity Resolution Service

Wenn Sie eine verwenden AWS KMS vom Kunden verwalteter Schlüssel mit Ihrem AWS Entity Resolution Serviceressourcen, die Sie verwenden können, AWS CloudTrailoder Amazon CloudWatch Logs, um Anfragen zu verfolgen, die AWS Entity Resolution sendet an AWS KMS.

Die folgenden Beispiele sind AWS CloudTrail Ereignisse für`CreateGrant`,`GenerateDataKey`, und`Decrypt`, `DescribeKey` die überwacht werden sollen AWS KMS Operationen, die aufgerufen wurden von AWS Entity Resolution um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden:

Themen

- CreateGrant
- DescribeKey
- GenerateDataKey
- Decrypt

CreateGrant

Wenn Sie eine verwenden AWS KMS vom Kunden verwalteter Schlüssel zur Verschlüsselung Ihrer passenden Workflow-Ressource, AWS Entity Resolution sendet in Ihrem Namen eine `CreateGrant` Anfrage für den Zugriff auf den KMS Schlüssel in Ihrem AWS-Konto. Der Zuschuss, der AWS Entity Resolution kreiert, sind spezifisch für die Ressource, die mit dem verknüpft ist AWS KMS vom Kunden verwalteter Schlüssel. Darüber hinaus AWS Entity Resolution verwendet 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 AWS KMS Ein vom Kunden verwalteter Schlüssel, der mit Ihrer passenden Ressource verknüpft ist, ist im Konto und in der Region vorhanden.

Das folgende Beispielereignis zeichnet den `DescribeKey` Vorgang 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 eine aktivieren AWS KMS vom Kunden verwalteter Schlüssel für Ihre passende Workflow-Ressource, AWS Entity Resolution sendet eine `GenerateDataKey` Anfrage über Amazon Simple Storage Service (Amazon S3) an AWS KMS das spezifiziert die AWS KMS vom Kunden verwalteter Schlüssel für die Ressource.

Das folgende Beispielereignis zeichnet den `GenerateDataKey` Vorgang 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 eine aktivieren AWS KMS vom Kunden verwalteter Schlüssel für Ihre passende Workflow-Ressource, AWS Entity Resolution sendet eine `Decrypt` Anfrage über Amazon Simple Storage Service (Amazon S3) an AWS KMS das spezifiziert die AWS KMS vom Kunden verwalteter Schlüssel für die Ressource.

Das folgende Beispielereignis zeichnet den `Decrypt` Vorgang 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, vom Kunden verwalteten 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 Leitfaden für Entwickler.

Weitere Informationen zu bewährten Sicherheitsmethoden für AWS Key Management Service finden Sie im AWS Key Management Service Leitfaden für Entwickler.

Zugriff AWS Entity Resolution mithilfe eines Schnittstellenendpunkts (AWS PrivateLink)

Sie können Folgendes verwenden … AWS PrivateLink um eine private Verbindung zwischen deinem VPC und herzustellen AWS Entity Resolution. Sie können darauf zugreifen AWS Entity Resolution als ob es in Ihrem wäreVPC, ohne die Verwendung eines Internet-Gateways, NAT Geräts, einer VPN Verbindung oder AWS Direct Connect Verbindung. Für den Zugriff auf Ihre Instanzen sind VPC keine öffentlichen IP-Adressen erforderlich AWS Entity Resolution.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellenendpunkt erstellen, der von AWS PrivateLink. Wir erstellen in jedem Subnetz, das Sie für den Schnittstellenendpunkt aktivieren, eine Endpunkt-Netzwerkschnittstelle. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Datenverkehr dienen AWS Entity Resolution.

Weitere Informationen finden Sie unter Access AWS-Services durch AWS PrivateLink in der AWS PrivateLink Führer.

Überlegungen zu AWS Entity Resolution

Bevor Sie einen Schnittstellenendpunkt einrichten für AWS Entity Resolution, lesen Sie Überlegungen im AWS PrivateLink Leitfaden.

AWS Entity Resolution unterstützt das Aufrufen all seiner API Aktionen über den Schnittstellenendpunkt.

VPCEndpunktrichtlinien werden unterstützt für AWS Entity Resolution. Standardmäßig voller Zugriff auf AWS Entity Resolution ist über den Schnittstellenendpunkt erlaubt. Alternativ können Sie den Netzwerkschnittstellen des Endpunkts eine Sicherheitsgruppe zuordnen, um den Datenverkehr zu den Endpunkten zu kontrollieren AWS Entity Resolution über den Schnittstellenendpunkt.

Erstellen Sie einen Schnittstellenendpunkt für AWS Entity Resolution

Sie können einen Schnittstellenendpunkt erstellen für AWS Entity Resolution entweder mit der VPC Amazon-Konsole oder dem AWS Command Line Interface (AWS CLI). Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts in der AWS PrivateLink Leitfaden.

Erstellen Sie einen Schnittstellen-Endpunkt für AWS Entity Resolution unter Verwendung des folgenden Dienstnamens:

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

Wenn Sie Private DNS für den Schnittstellenendpunkt aktivieren, können Sie API Anfragen stellen an AWS Entity Resolution unter Verwendung des standardmäßigen regionalen DNS Namens. Beispiel, `entityresolution.us-east-1.amazonaws.com`.

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM Ressource, die Sie an einen Schnittstellenendpunkt anhängen können. Die standardmäßige Endpunktrichtlinie ermöglicht vollen Zugriff auf AWS Entity Resolution über den Endpunkt der Schnittstelle. Um den Zugriff zu kontrollieren AWS Entity Resolution Fügen Sie von Ihrem VPC dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Principals, 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 Dienste mithilfe von Endpunktrichtlinien in der AWS PrivateLink Leitfaden.

Beispiel: VPC Endpunktrichtlinie für AWS Entity Resolution actions

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellenendpunkt anhängen, gewährt sie Zugriff auf die aufgelisteten AWS Entity Resolution Aktionen für alle Principals auf allen Ressourcen.

```
{
   "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) ist ein AWS-Service das hilft einem Administrator, den Zugriff auf sicher zu kontrollieren AWS Ressourcen schätzen. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und zur Nutzung autorisiert werden kann (über Berechtigungen verfügt) AWS Entity Resolution Ressourcen schätzen. IAMist ein AWS-Service das Sie ohne zusätzliche Kosten nutzen können.

> **Note**
>
> AWS Entity Resolution unterstützt kontoübergreifende Richtlinien. Weitere Informationen finden Sie IAMim IAMBenutzerhandbuch unter Kontoübergreifender Ressourcenzugriff.

Themen

Zielgruppe

Wie benutzt du AWS Identity and Access Management (IAM) unterscheidet sich je nach der Arbeit, die Sie in AWS Entity Resolution.

Servicebenutzer — Wenn Sie den AWS Entity Resolution Dienst, um Ihre Arbeit zu erledigen, dann stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Je mehr Sie verwenden AWS Entity Resolution Funktionen, um Ihre Arbeit zu erledigen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in nicht auf eine Funktion zugreifen können AWS Entity Resolution, finden Sie unter Fehlerbehebung AWS Entity Resolution Identität und Zugriff.

Serviceadministrator — Wenn Sie verantwortlich sind für AWS Entity Resolution Ressourcen in Ihrem Unternehmen, auf die Sie wahrscheinlich vollen Zugriff haben AWS Entity Resolution. Es ist Ihre Aufgabe, herauszufinden, welche AWS Entity Resolution Funktionen und Ressourcen, auf die Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Dienstbenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Um mehr darüber zu erfahren, wie Ihr Unternehmen Folgendes nutzen IAM kann AWS Entity Resolution, finden Sie unter Wie AWS Entity Resolution funktioniert mit IAM.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf AWS Entity Resolution. Um ein Beispiel anzusehen AWS Entity Resolution Identitätsbasierte Richtlinien, die Sie in verwenden könnenIAM, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich anmelden AWS mit Ihren Identitätsdaten. Sie müssen authentifiziert (angemeldet) sein AWS) als Root-Benutzer des AWS-Kontos, als IAM Benutzer oder indem Sie eine IAM Rolle übernehmen.

Sie können sich anmelden bei AWS als föderierte Identität mithilfe von Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAMIdentity Center) - Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie darauf zugreifen AWS Wenn Sie den Verbund verwenden, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der anmelden AWS Management Console oder das AWS Zugangsportal. Weitere Informationen zur Anmeldung bei AWS, siehe So melden Sie sich bei Ihrem an AWS-Konto in der AWS-Anmeldung Benutzerleitfaden.

Wenn Sie darauf zugreifen AWS programmatisch AWS stellt ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie es nicht verwenden AWS Tools, Sie müssen Anfragen selbst unterschreiben. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie unter Signieren AWS APIAnfragen im IAMBenutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. Zum Beispiel AWS empfiehlt, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center Benutzerhandbuch und Verwendung der Multi-Faktor-Authentifizierung () MFA in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie eine erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle hat AWS-Services und Ressourcen im Konto. Diese Identität wird als AWS-Konto Root-Benutzer. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann.

Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Verbundidentität

Es hat sich bewährt, menschlichen Benutzern, einschließlich Benutzern, die Administratorzugriff benötigen, vorzuschreiben, für den Zugriff den Verbund mit einem Identitätsanbieter zu verwenden AWS-Services mithilfe temporärer Anmeldeinformationen.

Eine föderierte Identität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web-Identitätsanbieter, AWS Directory Service, das Identity Center-Verzeichnis oder ein beliebiger Benutzer, der zugreift AWS-Services mithilfe von Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für eine zentralisierte Zugriffsverwaltung empfehlen wir die Verwendung AWS IAM Identity Center. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten und Anwendungen. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? in der AWS IAM Identity Center Benutzerleitfaden.

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres AWS-Konto das über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe ist eine Identität, die eine Sammlung von IAM Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität in deinem AWS-Konto das hat spezifische Berechtigungen. Es ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie einen anrufen AWS CLI or AWS APIOperation oder mithilfe eines benutzerdefiniertenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center Benutzerleitfaden.
- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um jemandem (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Allerdings mit einigen AWS-Services, Sie können eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

- Serviceübergreifender Zugriff — Einige AWS-Services Funktionen in anderen verwenden AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen in AWS, Sie gelten als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Rechte des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage AWS-Service um Anfragen an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, die Interaktionen mit anderen erfordert AWS-Services oder zu vervollständigende Ressourcen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an ein AWS-Service im IAM-Benutzerhandbuch.
  - Dienstverknüpfte Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen durchzuführen. Mit Diensten verknüpfte Rollen erscheinen in Ihrem AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon laufen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS CLI or AWS APIAnfragen. Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instanz vorzuziehen. Um eine zuzuweisen AWS Sie erstellen ein EC2 Instanzprofil, das an die Instanz angehängt ist. Sie müssen einer Instanz eine Rolle zuweisen und sie allen ihren Anwendungen zur Verfügung stellen. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff in AWS indem Sie Richtlinien erstellen und diese anhängen AWS Identitäten oder Ressourcen. Eine Richtlinie ist ein Objekt in AWS das, wenn es mit einer Identität oder Ressource verknüpft ist, ihre Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Principal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien sind gespeichert in AWS als JSON Dokumente. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

Administratoren können Folgendes verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der abrufen AWS Management Console, der AWS CLI, oder der AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie

mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können nicht verwenden AWS verwaltete Richtlinien aus IAM einer ressourcenbasierten Richtlinie.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 S3, AWS WAF, und Amazon VPC sind Beispiele für Dienste, die unterstützenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der

identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.

- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen AWS Organizations. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer AWS-Konten den Ihr Unternehmen besitzt. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und finden Sie SCPs unter Richtlinien zur Servicesteuerung in der AWS Organizations Benutzerleitfaden.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Um zu erfahren, wie AWS bestimmt, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, siehe Bewertungslogik für Richtlinien im IAMBenutzerhandbuch.

Wie AWS Entity Resolution funktioniert mit IAM

Vor der Verwendung IAM zur Verwaltung des Zugriffs auf AWS Entity Resolution, erfahren Sie, welche IAM Funktionen Ihnen zur Verfügung stehen AWS Entity Resolution.

IAMFunktionen, mit denen Sie arbeiten können AWS Entity Resolution

IAMMerkmal	AWS Entity Resolution Support
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC(Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Zugriffssitzungen weiterleiten (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Um einen allgemeinen Überblick darüber zu erhalten, wie AWS Entity Resolution und andere AWS Dienste funktionieren mit den meisten IAM Funktionen, siehe AWS Dienste, mit denen IAM im IAMBenutzerhandbuch gearbeitet werden kann.

Identitätsbasierte Richtlinien für AWS Entity Resolution

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie im IAMBenutzerhandbuch unter Referenz zu IAM JSON Richtlinienelementen.

Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Um Beispiele anzusehen für AWS Entity Resolution Identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Ressourcenbasierte Richtlinien innerhalb AWS Entity Resolution

Unterstützt ressourcenbasierte Richtlinien: Ja

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services.

Um den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Erlaubnis erteilen, auf die Ressource zuzugreifen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie IAMim IAMBenutzerhandbuch unter Kontoübergreifender Ressourcenzugriff.

Politische Maßnahmen für AWS Entity Resolution

Unterstützt Richtlinienaktionen: Ja

Administratoren können verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörigen AWS APIBetrieb. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur Berechtigungen erforderlich sind und für die es keine entsprechende Operation gibt. API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Um eine Liste von zu sehen AWS Entity Resolution Aktionen finden Sie unter Aktionen, die definiert sind von AWS Entity Resolutionin der Referenz zur Serviceautorisierung.

Politische Maßnahmen in AWS Entity Resolution verwenden Sie vor der Aktion das folgende Präfix:

```
entityresolution
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Um Beispiele zu sehen 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 Folgendes verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Um eine Liste von zu sehen AWS Entity Resolution Ressourcentypen und ihreARNs, siehe Ressourcen definiert durch AWS Entity Resolutionin der Referenz zur Serviceautorisierung. Informationen zu den Aktionen, mit denen Sie die ARN einzelnen Ressourcen spezifizieren können, finden Sie unter Aktionen definiert durch AWS Entity Resolution.

Hier finden Sie Beispiele für AWS Entity Resolution Identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Schlüssel für die Bedingungen der Richtlinien für AWS Entity Resolution

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können Folgendes verwenden AWS JSONRichtlinien, um festzulegen, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. 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.

Wenn Sie mehrere `Condition` Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition` Element angeben, AWS wertet sie mithilfe einer logischen `AND` Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Um alle zu sehen AWS globale Bedingungsschlüssel finden Sie unter AWS Kontexttasten für globale Bedingungen im IAMBenutzerhandbuch.

Um eine Liste von zu sehen AWS Entity Resolution Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Entity Resolutionin der Referenz zur Serviceautorisierung. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen, die definiert sind von AWS Entity Resolution.

Hier finden Sie Beispiele für AWS Entity Resolution Identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

ACLsin AWS Entity Resolution

UnterstütztACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

ABACmit AWS Entity Resolution

Unterstützungen ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. In AWS, diese Attribute werden Tags genannt. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele Entitäten anhängen AWS Ressourcen schätzen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt vonABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

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 finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Verwenden temporärer Anmeldeinformationen mit AWS Entity Resolution

Unterstützt temporäre Anmeldeinformationen: Ja

Etwas AWS-Services funktioniert nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Für zusätzliche Informationen, einschließlich AWS-Services mit temporären Anmeldeinformationen arbeiten, finden Sie unter AWS-Services mit denen IAM im IAMBenutzerhandbuch gearbeitet werden kann.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich bei der AWS Management Console mit einer beliebigen Methode außer einem Benutzernamen und einem Passwort. Zum Beispiel, wenn Sie darauf zugreifen AWS Wenn Sie den Single Sign-On-Link (SSO) Ihres Unternehmens verwenden, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter Wechseln zu einer Rolle (Konsole) im IAMBenutzerhandbuch.

Sie können temporäre Anmeldeinformationen manuell erstellen, indem Sie AWS CLI or AWS API. Sie können dann diese temporären Anmeldeinformationen für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen unter IAM.

Zugriffssitzungen weiterleiten für AWS Entity Resolution

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen in AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in

einem anderen Service initiieren. FASverwendet die Rechte des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage AWS-Service um Anfragen an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, die Interaktionen mit anderen erfordert AWS-Services oder zu vervollständigende Ressourcen. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Entity Resolution

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an ein AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann fehlerhaft sein AWS Entity Resolution Funktionalität. Bearbeiten Sie Servicerollen nur, wenn AWS Entity Resolution bietet Anleitungen dazu.

Mit Diensten verknüpfte Rollen für AWS Entity Resolution

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einem verknüpft ist AWS-Service. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen durchzuführen. Mit Diensten verknüpfte Rollen erscheinen in Ihrem AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS Dienste, 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

Standardmäßig sind Benutzer und Rollen nicht berechtigt, etwas zu erstellen oder zu ändern AWS Entity Resolution Ressourcen schätzen. Sie können auch keine Aufgaben mit dem ausführen AWS Management Console, AWS Command Line Interface (AWS CLI), oder AWS API. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, definiert von AWS Entity Resolution, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Entity Resolutionin der Referenz zur Serviceautorisierung.

Themen

- Bewährte Methoden für Richtlinien
- Verwendung der AWS Entity Resolution Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand etwas erstellen, darauf zugreifen oder löschen kann AWS Entity Resolution Ressourcen in Ihrem Konto. Diese Aktionen können Kosten für Sie verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Fangen Sie an mit AWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Um zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie AWS verwaltete Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie Folgendes definieren AWS vom Kunden verwaltete Richtlinien, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien oder AWS verwaltete Richtlinien für Jobfunktionen im IAMBenutzerhandbuch.

- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über eine bestimmte AWS-Service, wie beispielsweise AWS CloudFormation. Weitere Informationen finden Sie unter IAMJSONRichtlinienelemente: Zustand im IAMBenutzerhandbuch.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, das IAM Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, schalten Sie MFA für zusätzliche Sicherheit ein. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Verwendung der AWS Entity Resolution Konsole

Um auf die zuzugreifen AWS Entity Resolution Für die Konsole benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu auflisten und anzuzeigen AWS Entity Resolution Ressourcen in Ihrem AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die erforderlichen Mindestberechtigungen,

funktioniert die Konsole für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie nicht wie vorgesehen.

Sie müssen Benutzern, die nur Anrufe tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS CLI oder das AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen das weiterhin verwenden können AWS Entity Resolution Konsole, hängen Sie auch das an AWS Entity Resolution *ConsoleAccess* oder *ReadOnly* AWS verwaltete Richtlinie für die Entitäten. Weitere Informationen finden Sie im Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM Benutzer.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die internen und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von AWS CLI or AWS 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 allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete 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, Tagging AWS Glue, AWS KMS sodass die Konsole Optionen anzeigen und die ausgewählten

Optionen verwenden kann, um Aktionen zur Entitätsauflösung durchzuführen. Einige Ressourcen sind auf den Dienstnamen eingegrenzt. `entityresolution`

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.

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

```
    "Statement": [
        {
            "Sid": "EntityResolutionAccess",
            "Effect": "Allow",
            "Action": [
                "entityresolution:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GlueSourcesConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "glue:GetSchema",
                "glue:SearchTables",
                "glue:GetSchemaByDefinition",
                "glue:GetSchemaVersion",
                "glue:GetSchemaVersionsDiff",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetTableVersion",
                "glue:GetTableVersions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3BucketsConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3SourcesConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:ListBucketVersions",
                "s3:GetBucketVersioning"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "TaggingConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListRolesToPickRoleForPassing",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PassRoleToEntityResolutionService",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*entityresolution*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "entityresolution.amazonaws.com"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "ManageEventBridgeRules",
            "Effect": "Allow",
            "Action": [
               "events:PutRule",
               "events:DeleteRule",
               "events:PutTargets",
            ],
            "Resource": [
                 "arn:aws:events:*:*:rule/entity-resolution-automatic*"
            ]
        },
        {
            "Sid": "ADXReadAccess",
            "Effect": "Allow",
            "Action": [
                "dataexchange:GetDataSet"
            ],
            "Resource": "*"
        },
    ]
}
```

AWS 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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EntityResolutionRead",
            "Effect": "Allow",
            "Action": [
```

```
                "entityresolution:Get*",
                "entityresolution:List*"
            ],
            "Resource": "*"
        },
    ]
}
```

AWS Entity Resolution Aktualisierungen der verwalteten Richtlinien AWS

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter 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.

Änderung	Beschreibung	Datum
`AWSEntityResolutionConsoleFullAccess` – Aktualisierung auf eine bestehende Richtlinie	Die Option Provider-Services wurde im Matching-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

Fehlerbehebung AWS Entity Resolution Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, auf die Sie bei der Arbeit mit AWS Entity Resolution undIAM.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Entity Resolution
- Ich bin nicht berechtigt, iam auszuführen: PassRole

- Ich möchte Leute außerhalb meines AWS-Konto um auf meine zuzugreifen AWS Entity Resolution Ressourcen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Entity Resolution

Wenn das Symbol AWS Management Console teilt Ihnen mit, dass Sie nicht berechtigt sind, eine Aktion auszuführen. Wenden Sie sich dann an Ihren Administrator, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven *`my-example-widget`* Ressource anzuzeigen, aber nicht über die fiktiven `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 auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an übergeben können AWS Entity Resolution.

Etwas 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 auszuführen in AWS Entity Resolution. Für die Aktion muss der Dienst jedoch über Berechtigungen verfügen, die von einer Servicerolle erteilt 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 AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Leute außerhalb meines AWS-Konto um auf meine zuzugreifen AWS Entity Resolution Ressourcen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden 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:

- Um zu erfahren, ob AWS Entity Resolution unterstützt diese Funktionen, sieheWie AWS Entity Resolution funktioniert mit IAM.
- Um zu erfahren, wie Sie Zugriff auf Ihre Ressourcen gewähren können AWS-Konten die Ihnen gehören, finden Sie unter Gewähren des Zugriffs für einen IAM Benutzer in einem anderen AWS-Konto die Sie besitzen, finden Sie im IAMBenutzerhandbuch.
- Um zu erfahren, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren AWS-Konten, siehe Zugriff gewähren auf AWS-Konten Eigentum Dritter im IAMBenutzerhandbuch.
- Informationen zur Bereitstellung des Zugriffs über einen Identitätsverbund finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Konformitätsvalidierung für AWS Entity Resolution

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

  > **Note**
  >
  > Nicht alle sind berechtigt AWS-Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien für Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zusammengefasst.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.

- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

AWS Entity Resolution bewährte Verfahren zur Einhaltung von Vorschriften

In diesem Abschnitt finden Sie bewährte Verfahren und Empfehlungen zur Einhaltung der Vorschriften bei der Verwendung von AWS Entity Resolution.

Datensicherheitsstandards der Zahlungskartenbranche (PCIDSS)

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 zum AWS PCI Compliance-Paket PCIDSS, einschließlich der Beantragung einer Kopie, finden Sie unter PCIDSSStufe 1.

System- und Organisationskontrollen (SOC)

AWS Entity Resolution entspricht den Maßnahmen der System- und Organisationskontrollen (SOC), einschließlich SOC 1, SOC 2 und SOC 3. SOCBei Berichten handelt es sich um 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 SOCCompliance-Website verfügbar. Dort finden Sie in den veröffentlichten Berichten weitere Informationen zu den Kontrollen, 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, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Themen

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 AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem 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 dem CloudTrail UserIdentity-Element.

Grundlegendes zu Einträgen AWS Entity Resolution in Protokolldateien

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.

Ressourcen zur AWS Entitätsauflösung erstellen mit AWS CloudFormation

AWSEntity Resolution ist in einen Service integriert AWS CloudFormation, der Ihnen hilft, Ihre AWS Ressourcen zu modellieren und einzurichten, 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 AWS CloudFormation bereitstellt und konfiguriert.

Wenn Sie sie verwenden AWS 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.

AWSAuflösung und AWS CloudFormation Vorlagen für Entitäten

Um Ressourcen für AWS Entity Resolution und verwandte Dienste bereitzustellen und zu konfigurieren, müssen Sie sich mit AWS CloudFormation Vorlagen auskennen. Vorlagen sind formatierte Textdateien in JSON oderYAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder nicht vertraut sind, können Sie AWS CloudFormation Designer verwendenYAML, um Ihnen bei den ersten Schritten mit AWS CloudFormation Vorlagen zu helfen. Weitere Informationen finden Sie unter Was ist AWS CloudFormation -Designer? im AWS CloudFormation -Benutzerhandbuch.

AWSEntity Resolution unterstützt das Erstellen AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace und Eingeben AWS::EntityResolution::PolicyStatement . AWS CloudFormation Weitere Informationen, einschließlich Beispielen 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 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 Datenverarbeitungsauftrags speichert.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::EntityResolution::MatchingWorkflow im AWS CloudFormation -Benutzerhandbuch

  CreateMatchingWorkflowin der AWS Entity Resolution APIReferenz

- 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 AWS CloudFormation -Benutzerhandbuch

  CreateSchemaMappingin der AWS Entity Resolution APIReferenz

- Arbeitsablauf bei der 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 AWS CloudFormation -Benutzerhandbuch

  CreateIdMappingWorkflowin der AWS Entity Resolution APIReferenz

- 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 AWS CloudFormation -Benutzerhandbuch

  CreateIdNamespacein der AWS Entity Resolution APIReferenz

- PolicyStatement

Erstellen Sie ein `PolicyStatement`-Objekt.

Weitere Informationen finden Sie unter den folgenden Themen:

AWS::EntityResolution::PolicyStatement im AWS CloudFormation -Benutzerhandbuch

AddPolicyStatementin der AWS Entity Resolution APIReferenz

Erfahre mehr über AWS CloudFormation

Weitere Informationen AWS CloudFormation dazu finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- AWS CloudFormation APIReferenz
- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Kontingente für AWS Entity Resolution

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden AWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. 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	Anpassbar	Beschreibung
Gleichzeitige Jobs zur ID-Zuordnung	1	Nein	Die maximale Anzahl von ID-Zuordn ungsaufträgen, die in der aktuellen Version gleichzeitig verarbeitet werden können. AWS-Region
Gleichzeitige übereinstimmende Jobs	1	Nein	Die maximale Anzahl übereinst immender Jobs, die in der aktuellen Version gleichzeitig verarbeitet werden können. AWS-Region
Gleichzeitige Zuordnung von Aufträgen durch den Provider-Service	1	Nein	Die maximale Anzahl von Aufträgen zum Abgleich von Providerdiensten, die in der aktuellen Version gleichzei tig verarbeitet werden können. AWS-Region
Dateneingabe	20	Nein	Dies ist die Liste der Eingabeta bellen, die Sie in einem Abgleichs-Workflow verwenden möchten. Jede Eingabe entspricht einer Spalte in Ihrer

Name	Standard	Anpassbar	Beschreibung
			AWS Glue Eingabedatentabelle, die den Spaltennamen und zusätzliche Informationen enthält, die für Abgleichszwecke AWS Entity Resolution verwendet werden. Eingaben müssen eine eindeutige ID sowie mindestens ein zusätzliches Eingabefeld enthalten.
Datenausgabe	750	Nein	Dies ist 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.
Datenschema	25	Nein	Die maximale Anzahl von Eingabefeldern für das Datenschema.
Workflows zur ID-Zuordnung	10	Ja	Die maximale Anzahl von ID-Mapping-Workflows, die Sie AWS-Konto in dieser aktuellen Version erstellen können AWS-Region.
ID-Namespaces	10	Ja	Die maximale Anzahl von ID-Namespaces, die Sie in diesem aktuellen Zustand erstellen können. AWS-Konto AWS-Region
IDs abgleichen	500	Nein	Die maximale Anzahl von Datensätzen, die unter einer MatchID pro Workload konsolidiert werden können.

Name	Standard	Anpassbar	Beschreibung
Zuordnungsregel	15	Nein	Bei regelbasiertem Abgleich ist dies die angewendete Regelnummer, mit der ein übereinstimmender Datensatz generiert wurde. Dies ist Teil des Abgleichs von Workflow-Metadaten , die in die Ausgabe aufgenommen werden.
Passende Workflows	10	Ja	Die maximale Anzahl übereinst immender Workflows.
Anzahl der Regeln pro Workflow	15	Nein	Die maximale Anzahl von Regeln pro übereinstimmendem Workflow.
Rate of `GetMatchId` API requests (Rate der API-Anfor derungen)	50	Ja	Die maximale Anzahl von `GetCustom erID` API-Anfragen pro Sekunde.
Schemazuo rdnungen	50	Ja	Die maximale Anzahl von Schemazuo rdnungen, die Sie in diesem Konto in der aktuellen Region erstellen können. AWS

Name	Standard	Anpassbar	Beschreibung
Eindeutige Match-Schlüssel pro Across-Regelsatz	15	Nein	Die maximale Anzahl eindeutiger Vergleichsschlüssel pro Regelsatz. Ein Vergleichsschlüssel gibt an AWS Entity Resolution , welche Eingabefelder als ähnliche Daten und welche als unterschiedliche Daten zu betrachten sind. Auf diese Weise können regelbasierte Abgleichsregeln AWS Entity Resolution automatisch konfiguriert und ähnliche Daten, die in verschiedenen Eingabefeldern gespeichert sind, verglichen werden.

API-Drosselungskontingente

Ressource	Standard	Beschreibung
Rate der Anfragen `GetMatchId`	50 TPS	Maximale Anzahl von `GetMatchId` API-Aufrufen pro Sekunde.

Dokumentenverlauf für das AWS Entity Resolution Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für beschrieben AWS Entity Resolution.

Wenn Sie über Aktualisierungen dieser Dokumentation informiert werden möchten, können Sie den RSS Feed abonnieren. Um RSS Updates zu abonnieren, muss für den von Ihnen verwendeten Browser ein RSS Plug-in aktiviert sein.

Änderung	Beschreibung	Datum
Anbieterintegration	Update nur für die Dokumentation. 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
Passender Arbeitsablauf — Update	Kunden können die Datensätze jetzt entweder aus einem regelbasierten oder einem ML-basierten Abgleichs-Workflow löschen, um die Einhaltung der Datenverwaltungsvorschriften zu gewährleisten.	8. April 2024
Arbeitsablauf bei der ID-Zuordnung — Aktualisierung	Kunden können jetzt einen ID-Mapping-Workflow für mehrere verwenden AWS-Konten.	2. April 2024

AWS CloudFormation Ressourcen — Neue und aktualisierte Ressourcen	AWSEntity Resolution hat die folgenden Ressource n hinzugefügt: `AWS::Enti tyResolution::IdNa mespace` `AWS::Enti tyResolution::Poli cyStatement` und die folgende Ressource aktualisi ert:`AWS::EntityResolut ion::IdMappingWork flow` .	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
Passender Arbeitsablauf — Update	AWS Entity Resolution unterstützt jetzt die PII basierte RAMPID Zuweisung im auf LiveRamp Anbieterdiensten basierenden Matching-Workflow.	12. Februar 2024
AWS PrivateLink	AWS Entity Resolution unterstützt jetzt zusätzliche Datensicherheit AWS PrivateLi nk , sodass Kunden privat auf Dienste zugreifen können, auf denen gehostet wird AWS.	20. Oktober 2023

AWS 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 der bestehenden 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
AWS CloudFormation Integration	AWS Entity Resolution integriert sich jetzt mit AWS 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)

Eine eindeutige Kennung für AWS Ressourcen. ARNssind 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 (AmazonRDS) -Tags und Aufrufen. API

Automatische Verarbeitung

Eine Option für den Verarbeitungsrhythmus für einen passenden Workflow-Job, mit der dieser automatisch ausgeführt werden kann, wenn sich Ihre Dateneingabe ändert.

Diese Option ist nur für den regelbasierten Abgleich verfügbar.

Standardmäßig ist der Verarbeitungsrhythmus für einen passenden Workflow-Auftrag 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 erhalten up-to-date.

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.

Klartext

Daten, die nicht kryptografisch geschützt sind.

Konfidenzniveau () ConfidenceLevel

Beim 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.

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, eines sogenannten Schlüssels, in eine Form kodiert werden, die zufällig erscheint. Ohne Zugriff auf den Schlüssel ist es unmöglich, den ursprünglichen Klartext zu ermitteln.

Group name (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 eingeben, wie **`full_name`** für den Abgleich und die Ausgabe.

Hash

Hashing bedeutet, einen kryptografischen Algorithmus anzuwenden, der eine unumkehrbare und eindeutige Zeichenfolge mit fester Größe erzeugt, die als Hash bezeichnet wird. AWS Entity Resolution verwendet das 256-Bit-Hash-Protokoll (SHA256) des Secure Hash Algorithm und gibt eine 32-Byte-Zeichenfolge aus. In können Sie wählen AWS Entity Resolution, ob Sie Datenwerte in Ihrer Ausgabe hashen möchten.

Hash-Protokoll (HashingProtocol)

AWS Entity Resolution verwendet das 256-Bit-Hash-Protokoll (SHA256) des Secure Hash Algorithm und gibt eine 32-Byte-Zeichenfolge aus. Dies ist Teil der passenden Workflow-Metadaten, die in die Ausgabe aufgenommen werden.

Methode zur ID-Zuordnung

Wie die ID-Zuordnung durchgeführt werden soll.

Es gibt zwei Methoden zur ID-Zuordnung:

- Regelbasiert — Die Methode, mit der Sie Abgleichsregeln verwenden, um First-Party-Daten in einem ID-Mapping-Workflow von einer Quelle in ein Ziel zu übersetzen.
- Anbieterdienste — Die Methode, mit der Sie einen Provider-Service verwenden, um in einem ID-Mapping-Workflow von Drittanbietern codierte Daten von einer Quelle in ein Ziel zu übersetzen.

  AWS Entity Resolution unterstützt derzeit die LiveRamp auf Providerdiensten basierende ID-Mapping-Methode. 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 bei der ID-Zuordnung

Ein Datenverarbeitungsjob, der Daten aus einer Eingabedatenquelle einem Eingabedatenziel auf der Grundlage der angegebenen ID-Zuordnungsmethode zuordnet. Es erzeugt 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-Mapping-Workflow so einrichten, dass er entweder in Ihrem eigenen AWS-Konto oder in zwei Schritten ausgeführt wird AWS-Konten.

ID-Namespace

Eine Ressource AWS Entity Resolution , die Metadaten enthält, die mehrere Datensätze AWS-Konten und die Verwendung dieser Datensätze in einem ID-Mapping-Workflow erläutern.

Es gibt zwei Arten von ID-Namespaces: und. `SOURCE` `TARGET` Das `SOURCE` enthält Konfigurationen für die Quelldaten, die in einem ID-Mapping-Workflow verarbeitet werden. Das `TARGET` enthält eine Konfiguration der Zieldaten, in die alle Quellen aufgelöst werden. Um die Eingabedaten zu definieren, die Sie über zwei auflösen möchten AWS-Konten, erstellen Sie eine ID-Namespace-Quelle und ein ID-Namespace-Ziel, um Ihre Daten von einem Satz (`SOURCE`) in einen anderen () 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 für die ID-Zuordnungstabelle auszuführen und die Daten zu analysieren.

Weitere Informationen finden Sie im AWS Clean Rooms -Benutzerhandbuch.

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.

Eingabetyp

Der Typ der Eingabedaten. Sie wählen es aus einer vorkonfigurierten Werteliste wie Name, Adresse, Telefonnummer oder E-Mail-Adresse aus. Der Eingabetyp gibt an, AWS Entity Resolution welche Art von Daten Sie präsentieren, sodass sie ordnungsgemäß klassifiziert und normalisiert werden können.

Auf maschinellem Lernen basierendes Matching

Der auf maschinellem Lernen basierende Matching (ML-Matching) findet Übereinstimmungen in Ihren Daten, die möglicherweise unvollständig sind oder nicht exakt gleich aussehen. Der ML-Abgleich ist ein voreingestellter Prozess, bei dem versucht wird, Datensätze aus allen von Ihnen eingegebenen Daten abzugleichen. Der ML-Abgleich gibt eine Match-ID und ein Konfidenzniveau für jeden übereinstimmenden Datensatz zurück.

Manuelle Verarbeitung

Eine Option für die Schrittfrequenz eines passenden Workflow-Auftrags, 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.

Viele-zu-Viele-Abgleich

Beim any-to-many M-Matching werden mehrere Instanzen ähnlicher Daten verglichen. Werte in Eingabefeldern, denen derselbe Abgleichsschlüssel zugewiesen wurde, werden miteinander

abgeglichen, unabhängig davon, ob sie sich im selben Eingabefeld oder in unterschiedlichen Eingabefeldern befinden.

Beispielsweise haben Sie möglicherweise mehrere Eingabefelder für Telefonnummern wie `mobile_phone` und `home_phone` die gleiche Abgleichstaste „Telefon“. Verwenden many-to-many Sie den Abgleich, um Daten im `mobile_phone` Eingabefeld mit Daten im `mobile_phone` Eingabefeld und Daten im `home_phone` Eingabefeld zu vergleichen.

Mit Abgleichsregeln werden Daten in mehreren Eingabefeldern mit demselben Abgleichsschlüssel mit einer (oder) -Operation ausgewertet, und beim one-to-many Abgleich werden Werte aus mehreren Eingabefeldern verglichen. Das bedeutet, dass, wenn eine Kombination von `mobile_phone` oder zwischen zwei Datensätzen `home_phone` übereinstimmt, die Vergleichstaste „Telefon“ eine Übereinstimmung zurückgibt. Für die Suchtaste „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-Matching ist dies die ID, die von jeder übereinstimmenden Datensatzgruppe generiert AWS Entity Resolution und auf diese angewendet wird. Dies ist Teil der passenden Workflow-Metadaten, die in die Ausgabe aufgenommen werden.

Schlüssel abgleichen (MatchKey)

Der Abgleichsschlüssel AWS Entity Resolution gibt an, welche Eingabefelder als ähnliche Daten und welche als unterschiedliche Daten betrachtet werden sollen. Auf diese Weise können regelbasierte Abgleichsregeln AWS Entity Resolution automatisch konfiguriert und ähnliche Daten, die in verschiedenen Eingabefeldern gespeichert sind, verglichen werden.

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 die Abgleichstaste „Telefon“ geben. Anschließend kann der regelbasierte Abgleich so konfiguriert werden, dass Daten mithilfe von „oder“ -Anweisungen in allen Eingabefeldern mit dem Abgleichsschlüssel „Telefon“ verglichen werden (siehe Definitionen für Eins-zu-Eins-Abgleich und Viele-zu-Viele-Abgleich im Abschnitt Abgleichs-Workflow).

Wenn Sie möchten, dass beim regelbasierten Abgleich verschiedene Arten von Telefonnummerninformationen vollständig getrennt berücksichtigt werden, können Sie spezifischere

Abgleichsschlüssel wie „Mobile_Phone“ und „Home_Phone“ erstellen. Anschließend können Sie beim Einrichten eines Workflows für den Abgleich angeben, wie die einzelnen Telefonzuordnungsschlüssel beim regelbasierten Abgleich verwendet werden sollen.

Wenn für ein bestimmtes Eingabefeld kein Wert angegeben MatchKey ist, kann es nicht für den Abgleich verwendet werden, sondern es kann den Abgleichs-Workflow-Prozess durchlaufen und bei Bedarf ausgegeben werden.

Schlüsselname abgleichen

Der einem Match Key zugewiesene Name.

Zuordnungsregel (MatchRule)

Bei regelbasiertem Abgleich ist dies die angewendete Regelnummer, mit der ein übereinstimmender Datensatz generiert wurde. 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. entweder durch Abgleichsregeln oder Modelle) ermittelt wird, welche davon ähnlich sind — oder „übereinstimmen“.

Arbeitsablauf beim Abgleich

Der Prozess, den Sie eingerichtet haben, um anzugeben, welche Eingabedaten miteinander abgeglichen werden sollen und wie der Abgleich durchgeführt werden soll.

Beschreibung des passenden Workflows

Eine optionale Beschreibung des passenden Workflows, die Sie möglicherweise eingeben möchten. 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**
>
> Übereinstimmende 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 Informationen sind bei der Ausgabe erforderlich.

Normalisierung () ApplyNormalization

Wählen Sie aus, 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 Eingabetyp hat und die Werte in der `PHONE_NUMBER` Eingabetabelle als formatiert sind`(123) 456-7890`, AWS Entity Resolution werden die Werte auf normalisiert. `1234567890`

In den folgenden Abschnitten werden die Normalisierungsregeln beschrieben.

Themen

- Name
- Email
- Phone
- Adresse
- Gehasht
- Quell-ID

Name

- TRIM= Schneidet führende und nachfolgende Leerzeichen ab
- LOWERCASE= Alle Alphazeichen werden in Kleinbuchstaben geschrieben
- CONVERT_ ACCENT = Buchstaben mit verdecktem Akzent in einen normalen Buchstaben umwandeln
- REMOVE_ _ ALL NON _ ALPHA = Entfernt alle Nicht-Alpha-Zeichen [a-zA-Z]

Email

- TRIM= Schneidet führende und nachfolgende Leerzeichen ab
- LOWERCASE= Alle Alphazeichen werden in Kleinbuchstaben geschrieben
- CONVERT_ ACCENT = Buchstaben mit verdecktem Akzent in einen normalen Buchstaben umwandeln
- REMOVE_ _ ALL _ NON EMAIL _ CHARS = Entfernt alle non-alpha-numeric Zeichen [a-zA-Z0-9] und [.@-]

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

Adresse

- TRIM= Schneidet führende und nachfolgende Leerzeichen ab
- LOWERCASE= Alle Alphazeichen werden in Kleinbuchstaben geschrieben
- CONVERT_ ACCENT = Buchstaben mit verdecktem Akzent in einen normalen Buchstaben umwandeln
- REMOVE_ _ ALL NON _ ALPHA = Entfernt alle Nicht-Alpha-Zeichen [a-zA-Z]
- RENAME_ WORDS mit ADDRESS _ _ RENAME WORD _ MAP = ersetzt Wörter in der Adresszeichenfolge durch Wörter aus _ _ _ ADDRESS RENAME WORD MAP

- RENAME_ _ ADDRESS RENAME DELIMITER _ DELIMITERS verwenden MAP = Trennzeichen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_ _ _ RENAME ersetzen DELIMITER MAP
- RENAME_ _ ADDRESS RENAME DIRECTION _ DIRECTIONS verwenden MAP = Trennzeichen in der Adresszeichenfolge durch eine Zeichenfolge aus _ _ _ ersetzen ADDRESS RENAME DIRECTION MAP
- RENAME_ NUMBERS mit ADDRESS _ _ RENAME NUMBER _ MAP = ersetzt Zahlen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_ _ _ RENAME NUMBER MAP
- RENAME_ SPECIAL _ _ ADDRESS _ RENAME SPECIAL CHAR _ CHARS verwenden MAP = Sonderzeichen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_ _ RENAME _ SPECIAL CHAR _ ersetzen 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 Zahlenfolgen, die bei der Normalisierung der Adresszeichenfolge umbenannt werden.

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

```
 "num": "number"
```

ADDRESS_RENAME_SPECIAL_CHAR_MAP

Dies sind die Sonderzeichenfolgen, die bei der Normalisierung der Adresszeichenfolge umbenannt werden.

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

Gehasht

- TRIM= Schneidet führende und nachfolgende Leerzeichen ab

Quell-ID

- TRIM= Schneidet führende und nachfolgende Leerzeichen ab

Eins-zu-Eins-Abgleich

Beim ne-to-one O-Matching werden einzelne Instanzen ähnlicher Daten verglichen. Eingabefelder mit demselben Abgleichsschlüssel und Werten im selben Eingabefeld werden miteinander abgeglichen.

Beispielsweise haben Sie möglicherweise mehrere Eingabefelder für Telefonnummern wie `mobile_phone` und`home_phone`, die denselben Abgleichsschlüssel „Telefon“ haben. Verwenden one-to-one Sie den 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. Daten im `mobile_phone` Eingabefeld werden nicht mit Daten im `home_phone` Eingabefeld verglichen.

Mit Abgleichsregeln werden Daten in mehreren Eingabefeldern mit demselben Abgleichsschlüssel mit einer (oder) -Operation ausgewertet, und one-to-many beim Abgleich werden Werte innerhalb eines einzelnen Eingabefeldes verglichen. Das heißt, wenn zwei Datensätze `home_phone` mit `mobile_phone` oder übereinstimmen, gibt die Vergleichstaste „Telefon“ eine Übereinstimmung

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`.

Abgleichsregeln werten Daten in Eingabefeldern mit unterschiedlichen Zuordnungsschlüsseln mit einer (und) -Operation aus. Wenn Sie möchten, dass beim regelbasierten Abgleich verschiedene Arten von Telefonnummerninformationen vollständig getrennt berücksichtigt werden, können Sie spezifischere Zuordnungsschlüssel wie „mobile_phone“ und „home_phone“ erstellen. Wenn Sie beide Vergleichstasten in einer Regel verwenden möchten, um Treffer zu finden,. `Record One mobile_phone = Record Two mobile_phone` AND `Record One home_phone = Record Two home_phone`

Output

Eine Liste von OutputAttributeObjekten, 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 3Path 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 hat. ApplyNormalization

Dienstbasiertes Matching auf Anbieterbasis

Beim Abgleich auf Anbieterdiensten handelt es sich um einen Prozess, bei dem Ihre Datensätze mit bevorzugten Datendienstanbietern und lizenzierten Datensätzen abgeglichen, verknüpft und erweitert werden. Sie müssen über ein Abonnement beim Anbieter AWS Data Exchange verfügen, um diese Abgleichstechnik verwenden zu können.

AWS Entity Resolution ist derzeit in die folgenden Datendienstanbieter integriert:

- LiveRamp

- TransUnion
- UID2.0

Regelbasierter Abgleich

Beim regelbasierten Abgleich handelt es sich um einen Prozess, der darauf abzielt, exakte Übereinstimmungen zu finden. Beim regelbasierten Abgleich handelt es sich um einen hierarchischen Satz von Wasserfall-Abgleichsregeln, die von Ihnen vorgeschlagen, auf der Grundlage der von AWS Entity Resolution Ihnen eingegebenen Daten vorgeschlagen und vollständig von Ihnen konfiguriert werden können. Alle in den Regelkriterien angegebenen Vergleichsschlüssel müssen exakt übereinstimmen, damit die verglichenen Daten als Treffer deklariert und die zugehörigen Metadaten ausgegeben werden können. Beim regelbasierten Abgleich werden für jeden übereinstimmenden Datensatz eine Match-ID und eine Regelnummer zurückgegeben.

Wir empfehlen, Regeln zu definieren, mit denen eine Entität eindeutig identifiziert werden kann. Ordnen Sie Ihre Regeln so an, dass zuerst genauere Treffer gefunden werden.

Nehmen wir zum Beispiel an, Sie haben zwei Regeln, Regel 1 und Regel 2.

Diese Regeln haben die folgenden Zuweisungsschlüssel:

- 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 sie alle nach Regel 1 gefunden worden wären.

Um nach Übereinstimmungen zu suchen, die nach Telefonnummer unterschieden werden, ordnen Sie die Regeln wie folgt neu an:

- Regel 2 umfasst den vollständigen Namen, die Adresse und die Telefonnummer
- Regel 1 beinhaltet den vollständigen Namen und die Adresse

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, zwischen Schemazuordnungen zu unterscheiden, wenn Sie mehr als eine 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.

Schemazuordnung

Schema-Mapping AWS Entity Resolution ist der Prozess, mit dem Sie festlegen, AWS Entity Resolution wie Ihre Daten für den Abgleich interpretiert werden sollen. Sie definieren das Schema der Eingabedatentabelle, die Sie in einen Abgleichs-Workflow einlesen möchten AWS Entity Resolution .

Schemazuordnung ARN

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.

In verschiedenen Tabellen kann die Unique ID doppelte Werte haben.

Wenn der passende Workflow ausgeführt wird, wird der Datensatz zurückgewiesen, wenn die eindeutige ID:

- ist nicht angegeben
- ist innerhalb derselben Tabelle nicht eindeutig
- überschneidet sich in Bezug auf den Attributnamen zwischen den Quellen.
- mehr als 38 Zeichen (nur bei regelbasierten 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.