User Guide

AWS Entity Resolution

AWS Entity Resolution: User Guide

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

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

Themen

Sind Sie ein Erstbenutzer? AWS Entity Resolution

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

- Funktionen von AWS Entity Resolution
- Zugreifen AWS Entity Resolution

- Einrichten AWS Entity Resolution

Funktionen von AWS Entity Resolution

AWS Entity Resolution beinhaltet die folgenden Funktionen:

- Flexible und anpassbare Datenaufbereitung

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

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

  - 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 Vergleichstechnik AWS Entity Resolution generiert werden. Jeder Match-Gruppe ist die Regelnummer zugeordnet, die zur Generierung des Matches verwendet wurde, um Ihnen das Verständnis des Matches zu erleichtern. Die Regelnummer kann beispielsweise die Genauigkeit jeder Spielgruppe belegen, sodass Regel eins genauer ist als Regel zwei.

- Vorkonfigurierter, 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.

- Datensätze mit Datendienstanbietern abgleichen

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

- Manuelle Massenverarbeitung und automatische inkrementelle Verarbeitung

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

- Suche nahezu in Echtzeit

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

- Datenschutz und Regionalisierung von Haus aus

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

- Transcodierung für mehrere Parteien

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

Zugehörige Services

Folgendes bezieht AWS-Services sich auf AWS Entity Resolution:

- Amazon S3

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

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

- AWS Glue

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

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

- AWS CloudTrail

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

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

- 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 Erstellen von AWS Entity Resolution-Ressourcen mit AWS CloudFormation.

Zugreifen AWS Entity Resolution

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

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

Preisgestaltung für AWS Entity Resolution

Preisinformationen finden Sie unter AWS Entity Resolution – Preise.

Einrichten AWS Entity Resolution

Führen Sie AWS Entity Resolution vor der ersten Verwendung die folgenden Aufgaben aus.

Themen

Melden Sie sich an für AWS

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

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
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, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

Erstellen Sie einen Administratorbenutzer

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)	Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS. Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.	Beachtung der Anweisungen unter Erste Schritte im AWS IAM Identity Center - Benutzerhandbuch.	Konfigurieren Sie den programmatischen Zugriff, indem Sie die AWS CLI zu verwendende Konfiguration AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch konfigurieren.
In IAM (Nicht empfohlen)	Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS.	Beachtung der Anweisungen unter Erstellen Ihres ersten IAM-Administratorbenutzers und Ihrer ersten Benutzergruppe im IAM-Benutzerhandbuch.	Programmgesteuerten Zugriff unter Verwendung der Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im IAM-Benutzerhandbuch konfigurieren.

Abonnieren Sie einen Anbieter-Service auf AWS Data Exchange

Führen Sie das folgende Verfahren aus, wenn Sie einen auf Providerdiensten basierenden Matching-Workflow oder einen ID-Zuordnungs-Workflow verwenden. Wenn Sie keinen auf Providerdiensten basierenden Abgleichsworkflow oder ID-Zuordnungsworkflow verwenden, können Sie diesen Schritt überspringen.

In können Sie wählen AWS Entity Resolution, ob Sie einen passenden Workflow mit einem der folgenden Anbieterdienste ausführen möchten, wenn Sie ein Abonnement bei diesem Anbieter abgeschlossen haben. AWS Data Exchange Ihre Daten werden mit einer Reihe von Eingaben abgeglichen, die von Ihrem bevorzugten Anbieter definiert wurden.

- LiveRamp
  - LiveRamp Auflösung der Identität
  - LiveRamp Transcodierung
- TransUnion
  - TransUnion TruAudience Identitätsauflösung und -anreicherung ohne Übertragung
  - TransUnion TruAudience Identitätslösung ohne Übertragung
- Einheitliche ID 2.0
  - Einheitliche ID 2.0-Identitätslösung

Darüber hinaus können Sie einen ID-Mapping-Workflow mit ausführen, LiveRamp wenn Sie ein Abonnement bei diesem Anbieter haben.

- LiveRamp
  - LiveRamp Transcodierung

Es gibt zwei Möglichkeiten, einen Anbieterdienst zu abonnieren:

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

Subscription) im AWS Data Exchange Benutzerhandbuch, um ein BYOS-Angebot anzunehmen. AWS Data Exchange

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

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

Bereiten Sie Datentabellen vor

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

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

Die Vorbereitung Ihrer Datentabellen umfasst die folgenden Schritte:

Themen

Schritt 1: Bereiten Sie Ihre Eingabedaten vor

Gehen Sie wie folgt vor, wenn Sie einen passenden Workflow mit einem Provider-Service verwenden. Wenn Sie keinen passenden Workflow mit einem Anbieterdienst verwenden, können Sie diesen Schritt überspringen.

Weitere Informationen finden Sie unter Abonnieren Sie einen Anbieter-Service auf AWS Data Exchange.

Wenn Sie einen Abgleichsworkflow mit einem auf einem Provider-Service basierenden Abgleichsworkflow oder einem ID-Zuordnungsworkflow ausführen möchten, ziehen Sie die folgende Tabelle zur Vorbereitung Ihrer Eingabedaten zurate:

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

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

Anbieter-Service	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 Haushaltsschlüssel E und HHID sind spezifisch für den Client-Namespace.
		• **`Phone number`** sollte aus 10 Ziffern bestehen und darf keine Sonderzeichen wie Leerzeichen oder Bindestriche enthalten.
		• **`Addresses`** sollte aufgeteilt werden in
		  • eine einzelne Adresszeile (kombinieren Sie die Adresszeilen 1 und 2, falls vorhanden)
		  • city
		  • zip (oder zip plus4), ohne Sonderzeichen wie Leerzeichen oder Bindestriche

Anbieter-Service	Eindeutige ID erforderlich?	Aktionen
		• Bundesland, angegeben als 2-Buchstaben-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. • **`Last Name`**können Klein- oder Großbuchstaben sein, mittlere Initialen sollen ausgeschlossen werden.

Anbieter-Service	Eindeutige ID erforderlich?	Aktionen
Vereinheitlichte ID 2.0	Ja	Stellen Sie Folgendes sicher: • Die eindeutige ID kann kein Hash sein. • UID2 unterstützt sowohl E-Mail als auch Telefonnummer für die UID2-Generierung. Wenn jedoch beide Werte in der Schemazuordnung vorhanden sind, dupliziert der Workflow jeden Datensatz in der Ausgabe. Ein Datensatz verwendet die E-Mail für die UID2-Generierung und der zweite Datensatz verwendet die Telefonnummer. Wenn Ihre Daten eine Mischung aus E-Mails und Telefonnummern enthalten und Sie diese doppelte Anzahl von Datensätzen in der Ausgabe vermeiden möchten, ist es am besten, für jeden einen eigenen Workflow mit separaten Schemazuordnungen zu erstellen. Führen Sie in diesem Szenario die Schritte zweimal durch: Erstellen Sie einen Workflow für E-Mails und einen separaten für Telefonnummern.

Anbieter-Service	Eindeutige ID erforderlich?	Aktionen
		Note Eine bestimmte E-Mail oder Telefonnummer zu einem bestimmten Zeitpunkt führt zu demselben UID2-Rohwert, unabhängig davon, wer die Anfrage gestellt hat. Roh-UID2-Werte werden durch Zugabe von Salzen aus Salzkübeln erzeugt, die etwa einmal pro Jahr rotiert werden, sodass auch die Roh-UID2 mit rotiert wird. Verschiedene Salzkübel wechseln im Laufe des Jahres zu unterschiedlichen Zeiten. AWS Entity Resolution verfolgt derzeit nicht die rotierenden Salzeimer und Roh-UID2. Es wird daher empfohlen, die rohen UID2 täglich zu regenerieren. Weitere Informationen finden Sie unter Wie oft sollten UID2s für inkrementelle Updates aktualisiert werden? in der UID 2.0-Dokumentation.

Schritt 2: Speichern Sie Ihre Eingabedatentabelle in einem unterstützten Datenformat

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

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

- Kommagetrennter Wert (CSV)

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

- Parquet

Schritt 3: Laden Sie Ihre Eingabedatentabelle auf Amazon S3 hoch

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

> **Note**
>
> Die Eingabedaten müssen in Amazon Simple Storage Service (Amazon S3) in demselben AWS-Konto Ordner gespeichert werden, 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 Amazon S3 S3-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Buckets und dann einen Bucket zum Speichern Ihrer Datentabelle aus.
3. Wählen Sie Hochladen und folgen Sie dann den Anweisungen.
4. Wählen Sie die Registerkarte Objekte, um das Präfix anzuzeigen, in dem Ihre Daten gespeichert sind. Notieren Sie sich den Namen des Ordners.

Sie können den Ordner auswählen, um die Datentabelle anzuzeigen.

Schritt 4: Erstellen Sie eine AWS Glue Tabelle

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

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

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

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

Um eine AWS Glue Tabelle zu erstellen

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

Sie können bei Bedarf auch eine IAM-Rolle erstellen wählen oder Ihren Administrator die IAM-Rolle erstellen lassen.

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

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

    b. Um das Schema einer Tabelle anzuzeigen, wählen Sie eine bestimmte Tabelle aus.
13. Notieren Sie sich den AWS Glue Datenbanknamen und den AWS Glue Tabellennamen.

Erstellen Sie eine IAM-Rolle für einen Konsolenbenutzer

So erstellen Sie eine IAM-Rolle

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

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

Eine neue Registerkarte wird geöffnet.

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

   - AWS verwaltete Richtlinie: AWSEntityResolutionConsoleFullAccess
   - AWS verwaltete Richtlinie: AWSEntityResolutionConsoleReadOnlyAccess

b. Wählen Sie Weiter: 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 Richtlinie erstellen aus.

   Sie haben eine Richtlinie für ein Kollaborationsmitglied erstellt.

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

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

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

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

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

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

   d. Wählen Sie Rolle erstellen aus.

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

   Sie können Rollen verwenden, um kurzfristige Anmeldeinformationen zu erstellen. Dies wird aus Sicherheitsgründen empfohlen. Sie können auch Benutzer auswählen, um langfristige Anmeldeinformationen zu erstellen.
3. Wählen Sie Rolle erstellen aus.
4. Wählen Sie im Assistenten zum Erstellen von Rollen unter Vertrauenswürdiger Entitätstyp die Option 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 aus.
7. Wählen Sie für Berechtigungen hinzufügen die Option Richtlinie erstellen aus.

   Eine neue Registerkarte wird angezeigt.

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

> **Note**
>
> Die folgende Beispielrichtlinie unterstützt die Berechtigungen, die zum Lesen entsprechender Datenressourcen wie Amazon S3 und erforderlich sind AWS Glue. Je nachdem, wie Sie Ihre Datenquellen eingerichtet haben, müssen Sie diese Richtlinie jedoch möglicherweise ändern.
> Ihre AWS Glue Ressourcen und die zugrunde liegenden Amazon S3 S3-Ressourcen müssen dieselben sein AWS-Region wie AWS Entity Resolution.
> Sie müssen keine AWS KMS Berechtigungen erteilen, 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"
            ]
        }
    ]
}
```

Ersetzen Sie jeden *{{Benutzereingabe-Platzhalter}}* durch Ihre eigenen Informationen.

AWS-Region	AWS-Region Ihrer Ressourcen. Ihre AWS Glue Ressourcen, die zugrunde liegenden Amazon S3 AWS KMS S3-Ressourcen und Ressourcen müssen dieselben sein AWS-Region wie`AWS Entity Resolution` .
accountId	Ihre AWS-Konto ID.
Eingabeeimer	Amazon S3 S3-Buckets, die die zugrunde liegenden Datenobjekte enthalten AWS Glue , aus denen gelesen `AWS Entity Resolution` werden soll.
Ausgabe-Buckets	Amazon S3 S3-Buckets, in denen die Ausgabedaten generiert `AWS Entity Resolution` werden.
Eingabedatenbanken	AWS Glue Datenbanken, aus denen gelesen `AWS Entity Resolution` werden soll.

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

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

Ersetzen Sie jeden *{{Platzhalter für Benutzereingaben}}* durch Ihre eigenen Informationen.

AWS-Region	AWS-Region Ihrer Ressourcen. Ihre AWS Glue Ressourcen, die zugrunde liegenden Amazon S3 AWS KMS S3-Ressourcen und Ressourcen müssen dieselben sein AWS-Region wie`AWS Entity Resolution` .
accountId	Ihre AWS-Konto ID.
Eingabetasten	Verwaltete Schlüssel ein. 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 sollen, 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 *{{Benutzereingabe-Platzhalter}}* durch Ihre eigenen Informationen.

AWS-Region	AWS-Region Ihrer Ressourcen. Ihre AWS Glue Ressourcen, die zugrunde liegenden Amazon S3 AWS KMS S3-Ressourcen und Ressourcen müssen dieselben sein AWS-Region wie`AWS Entity Resolution` .
accountId	Ihre AWS-Konto ID.
Ausgabetasten	Verwaltete Schlüssel ein. AWS Key Management Service Wenn Sie möchten, dass Ihre Ausgabequellen verschlüsselt werden, `AWS Entity Resolution` müssen Sie die Ausgabedaten mit Ihrem Schlüssel verschlüsseln.

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

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

Ersetzen Sie jeden *{{Platzhalter für Benutzereingaben}}* durch Ihre eigenen Informationen.

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

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

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

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

Die Workflow-Jobrolle für AWS Entity Resolution wurde erstellt.

Schema-Mapping erstellen

Um die Eingabedaten zu definieren, die Sie auflösen möchten, erstellen Sie ein Schema-Mapping. Der Schema-Mapping-Prozess führt Sie durch eine Reihe von Schritten zur Definition der Daten, die Sie auflösen möchten, indem Sie Ihre Eingabefelder und Attributtypen definieren und anschließend Ihre Vergleichsschlüssel definieren und gruppieren.

Es gibt drei Möglichkeiten, ein Schema-Mapping zu erstellen in AWS Entity Resolution:

- Verwenden eines geführten Ablaufs zum Importieren vorhandener Schemainformationen.
- Verwendung eines geführten Ablaufs zur manuellen Definition von Eingabedaten.
- Verwenden des JSON-Editors zum Erstellen, Einfügen oder Importieren einer Schemazuordnung.

Der folgende Prozess führt Sie durch die drei verschiedenen Methoden zum Erstellen einer Schemazuordnung.

Themen

- Erstellen Sie eine Schemazuordnung (vorab ausgefüllte Spalten)
- Erstellen Sie eine Schemazuordnung (manuell definierte Spalten)
- Erstellen Sie eine Schemazuordnung (JSON-Editor)

Erstellen Sie eine Schemazuordnung (vorab ausgefüllte Spalten)

In diesem Verfahren wird beschrieben, wie Sie mithilfe der AWS Glue Option Import von in der AWS Entity Resolution Konsole eine Schemazuordnung erstellen. Sie können diese Erstellungsmethode verwenden, um Eingabefelder zu definieren, die mit vorab ausgefüllten Spalten aus einer AWS Glue Tabelle beginnen.

So erstellen Sie eine Schemazuordnung mit vorausgefüllten Spalten:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie auf der Seite Schemazuordnungen in der oberen rechten Ecke die Option Schema-Mapping erstellen aus.

4. Gehen Sie für Schritt 1: Schemadetails angeben wie folgt vor:

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

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

   c. Wählen Sie die AWS Glue Datenbank aus der Dropdownliste und dann die AWS Glue Tabelle aus der Dropdownliste aus.

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

   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 verschiedenen Quellen überschneidet, wird der Datensatz AWS Entity Resolution zurückgewiesen, wenn der entsprechende Workflow ausgeführt wird.

   e. Wählen Sie für Eingabefelder 1—25 Spalten aus, die für den Abgleich und für die optionale Weiterleitung verwendet werden sollen.

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

      ii. Wählen Sie unter Weiterleiten — optional die Spalten aus, die als Passthrough-Spalten 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 aus.

5. Gehen Sie für Schritt 2: Eingabefelder zuordnen wie folgt vor:

   a. Geben Sie für Eingabefelder für den Abgleich den Eingabetyp und den Abgleichsschlüssel für jedes Eingabefeld an.

      Der Eingabetyp hilft Ihnen bei der Klassifizierung der Daten. Die Zuordnungstaste ermöglicht den Vergleich der Eingabefelder mit Ihrem Abgleichs-Workflow.

      > **Note**
      >
      > Wenn Sie ein Schema-Mapping für die Verwendung mit der auf dem LiveRamp Provider-Service basierenden Abgleichstechnik 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 Straßenanschrift übereinstimmen.

   b. Wählen Sie Weiter aus.

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 name`** **`Middle name`**`Last name`, und und geben Sie dann einen Gruppennamen mit dem Namen „**`Full name`**“ und einen Abgleichsschlüssel mit dem Namen „**`Full name`**“ ein, um den Vergleich zu ermöglichen.

   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 1 Home street address 2Home city`**, und und geben Sie dann einen Gruppennamen mit dem Namen „**`Shipping address`**“ und einen Abgleichsschlüssel mit dem Namen „**`Shipping address`**“ ein, um den Vergleich zu ermöglichen.

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

Example

Wählen Sie beispielsweise die Eingabefelder **`Home phone 1 Home phone 2Cell phone`**, und und 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 ermöglichen.

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

d. Wählen Sie Weiter aus.

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

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

b. Wählen Sie Schema-Mapping erstellen aus.

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

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

Erstellen Sie eine Schemazuordnung (manuell definierte Spalten)

In diesem Verfahren wird beschrieben, wie Sie mithilfe der Option Benutzerdefiniertes Schema erstellen in der AWS Entity Resolution Konsole eine Schemazuordnung erstellen. Verwenden Sie diese Erstellungsmethode, um die Eingabefelder mithilfe eines geführten Ablaufs manuell zu definieren.

Um eine Schemazuordnung mithilfe manuell definierter Spalten zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie auf der Seite Schemazuordnungen in der oberen rechten Ecke die Option Schema-Mapping erstellen aus.
4. Gehen Sie für Schritt 1: Schemadetails angeben wie folgt vor:

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

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

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

    Example

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

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

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

e. Wählen Sie Weiter aus.

5. Gehen Sie für Schritt 2: Eingabefelder zuordnen wie folgt vor:

a. Fügen Sie für Eingabefelder für den Abgleich das Eingabefeld, den Eingabetyp und den Abgleichsschlüssel hinzu.

Sie können bis zu 25 Eingabefelder hinzufügen.

Der Eingabetyp hilft Ihnen bei der Klassifizierung der Daten. Die Zuordnungstaste ermöglicht den Vergleich der Eingabefelder mit Ihrem Abgleichs-Workflow.

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

b. (Optional) Fügen Sie für Eingabefelder für die Weiterleitung die Eingabefelder hinzu, die nicht abgeglichen werden sollen.

c. Wählen Sie Weiter aus.

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 name`** **`Middle name`** **`Last name`**, und und geben Sie dann einen Gruppennamen mit dem Namen „**`Full name`**“ und einen Abgleichsschlüssel mit dem Namen „**`Full name`**“ ein, um den Vergleich zu ermöglichen.

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 1 Home street address 2Home city`**, und und geben Sie dann einen Gruppennamen mit dem Namen „**`Shipping address`**“ und einen Abgleichsschlüssel mit dem Namen „**`Shipping address`**“ ein, um den Vergleich zu ermöglichen.

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

Example

Wählen Sie beispielsweise die Eingabefelder **`Home phone 1 Home phone 2Cell phone`**, und und 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 ermöglichen.

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

d. Wählen Sie Weiter aus.

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

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

b. Wählen Sie Schema-Mapping erstellen aus.

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

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

Erstellen Sie eine Schemazuordnung (JSON-Editor)

Dieses Verfahren beschreibt den Prozess der Erstellung einer Schemazuordnung mithilfe der Option JSON-Editor verwenden in der AWS Entity Resolution Konsole. Verwenden Sie diese Erstellungsmethode, um mit einem JSON-Editor eine Schemazuordnung zu erstellen, einzufügen oder zu importieren. Die Felder „Eindeutige ID“ und „Eingabe“ sind bei dieser Option nicht verfügbar.

Um eine Schemazuordnung mit dem JSON-Editor zu erstellen

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

Wenn du willst...	Dann wähle...
Beginnen Sie mit der Erstellung Ihres Schema-Mappings	Fügen Sie ein JSON-Beispiel ein und bearbeiten Sie die Informati onen nach Bedarf.
Verwenden Sie eine vorhandene JSON-Datei	Aus einer Datei importieren

b. Wählen Sie Weiter aus.

6. Für Schritt 3: Überprüfen und erstellen:

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

   b. Wählen Sie Schema-Mapping erstellen aus.

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

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

Einen passenden Workflow erstellen

Nachdem Sie ein Schema-Mapping erstellt haben, können Sie einen oder mehrere Abgleichs-Workflows erstellen, um Dateneingaben und Normalisierungsschritte zu spezifizieren und die gewünschten Abgleichstechniken auszuwählen. Es gibt drei Vergleichstechniken:

- Beim regelbasierten Abgleich handelt es sich um einen hierarchischen Satz von Wasserfallabgleichsregeln, die von Ihnen vorgeschlagen werden AWS Entity Resolution, auf der Grundlage der von Ihnen eingegebenen Daten und vollständig von Ihnen konfigurierbar sind.
- Der auf maschinellem Lernen basierende Abgleich ist ein voreingestellter Prozess, bei dem versucht wird, Datensätze aus allen von Ihnen eingegebenen Daten abzugleichen.
- Mithilfe von Provider-Diensten können Sie Ihre bekannten Identifikatoren Ihrem bevorzugten Datendienstanbieter zuordnen.

  AWS Entity Resolution ist derzeit in die folgenden Datendienstanbieter integriert: LiveRamp TransUnion, und UID 2.0. Sie können ein öffentliches Abonnement für diese Anbieter nutzen AWS Data Exchange oder ein privates Angebot direkt mit dem Datenanbieter aushandeln. Weitere Informationen finden Sie unter Abonnieren Sie einen Anbieter-Service auf AWS Data Exchange.

AWS Entity Resolution liest Ihre Daten von dem/den von Ihnen angegebenen Standort (en) und schreibt die Ergebnisse an einen von Ihnen ausgewählten Ort. Falls gewünscht AWS Entity Resolution , können Sie die Ausgabedaten mit einem Hashwert versehen, sodass Sie die Kontrolle über Ihre Daten behalten.

Sie können die Ausgabe von regelbasiertem oder ML-Abgleich auch als Eingabe für den dienstbasierten Abgleich von Anbietern verwenden oder umgekehrt, um Ihren Geschäftsanforderungen gerecht zu werden. Sie können z. B. zunächst einen regelbasierten Abgleich durchführen, um Übereinstimmungen in Ihren Daten zu finden, und dann eine Teilmenge der Datensätze, die nicht zugeordnet wurden, an den dienstbasierten Abgleich des Anbieters senden, um Abonnementkosten für Anbieter zu sparen.

Themen

- Nächste Schritte

Erstellen Sie einen regelbasierten Abgleichsworkflow

Der regelbasierte Abgleichs-Workflow ermöglicht es Ihnen, Klartext- oder Hash-Daten zu vergleichen, um anhand von von Ihnen angepassten Kriterien exakte Übereinstimmungen zu finden.

Wenn AWS Entity Resolution eine Übereinstimmung zwischen zwei oder mehr Datensätzen in Ihren Daten gefunden wird, wird den Datensätzen im abgeglichenen Datensatz eine Match-ID zugewiesen.

Beim regelbasierten Abgleich wird die Regelnummer angewendet, die den Abgleich generiert hat.

So erstellen Sie einen regelbasierten Abgleichs-Workflow:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem 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 Datenbank aus der Dropdownliste, wählen Sie die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

    Sie können bis zu 19 Dateneingaben hinzufügen.

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

    d. Geben Sie die Dienstzugriffsberechtigungen an, indem Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden auswählen.

Wenn Sie wählen...	THEN
Eine neue Servicerolle erstellen und verwenden	• AWS Entity Resolution erstellt eine Servicerolle mit der

Wenn Sie wählen...	THEN
	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, können Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt auswählen und dann einen AWS KMS Schlüssel eingeben, der zur Entschlüsselung Ihrer Dateneingabe verwendet wird.

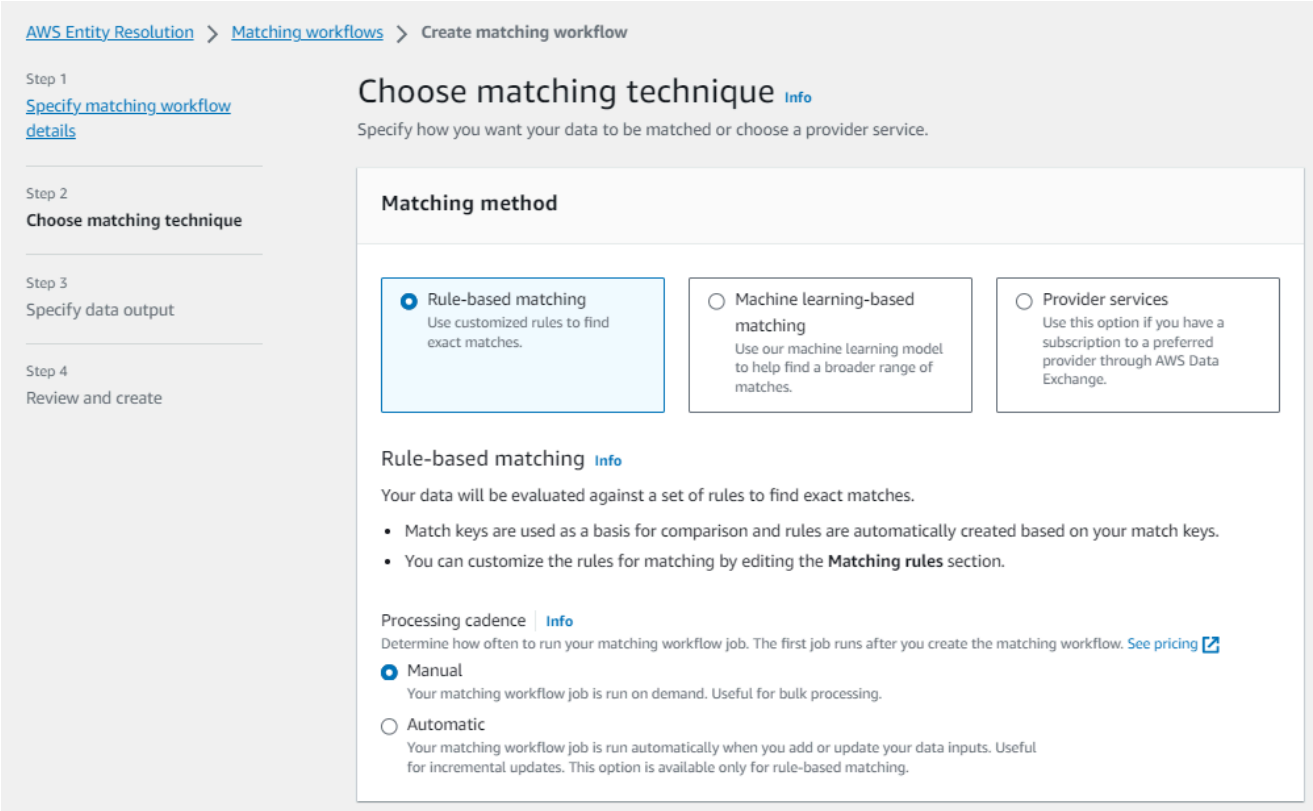
Wenn Sie wählen...	THEN
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtig t sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenric htlinie 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 aus.

5. Für Schritt 2: Passende Technik wählen:

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



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

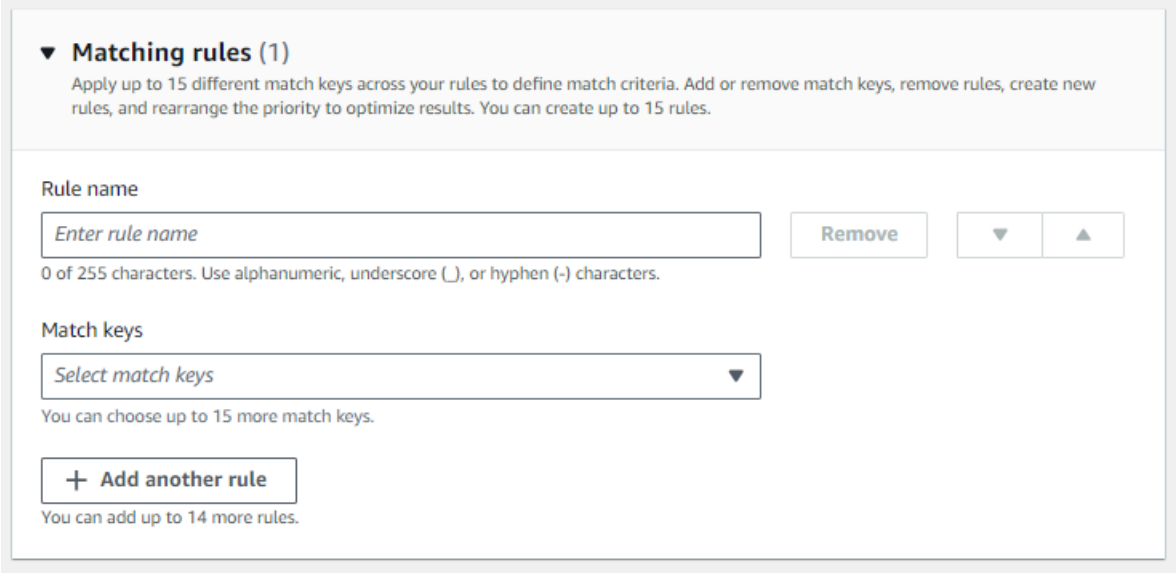
Wenn du möchtest...	Dann wähle...
Führen Sie bei Bedarf einen Workflow für ein Bulk-Update aus	Manuell
Führen Sie einen Workflow aus, sobald sich neue Daten in Ihrem S3-Bucket befinden	Automatisch

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

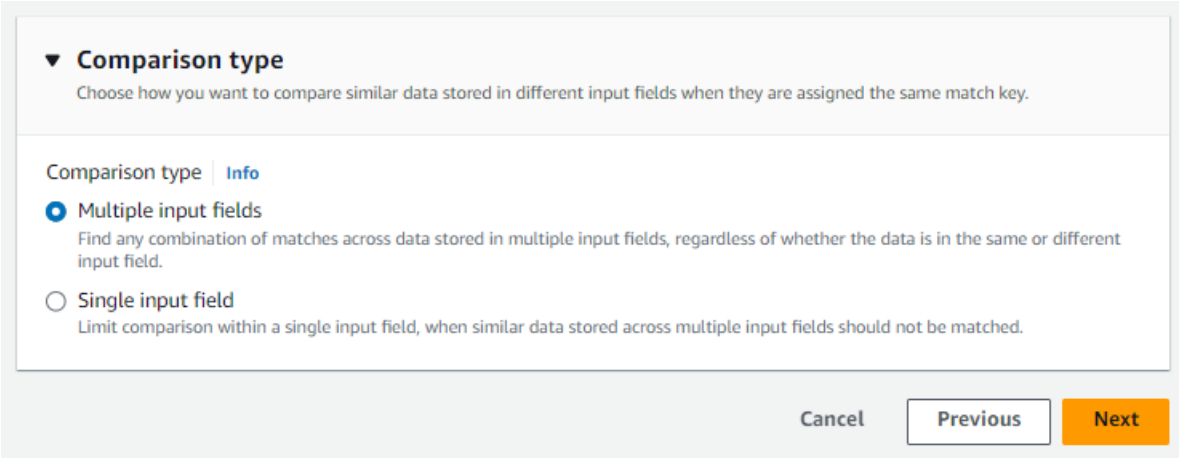
   Sie können bis zu 15 verschiedene Abgleichsschlüssel auf Ihre Regeln anwenden, um Vergleichskriterien zu definieren.

   Sie können bis zu 15 Regeln erstellen.



d. Wählen Sie als Vergleichstyp eine der folgenden Optionen aus.

Wenn Sie möchten...	Dann wähle...
Finden Sie eine beliebige Kombination von Übereinst immungen in Daten, die in mehreren Eingabefeldern gespeichert sind	Vergleich mehrerer Eingabefelder
Beschränken Sie den Vergleich auf ein einzelnes Eingabefeld	Vergleich eines einzelnen Eingabefeldes



e. Wählen Sie Weiter aus.

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 unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel ARN ein.

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

   d. Sehen Sie sich für die Datenausgabe alle enthaltenen Felder an.

   e. Legen Sie fest, ob Sie Felder einschließen, ausblenden oder maskieren möchten.

Wenn du willst...	Dann wähle...
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 (Zurückse tzen).

   f. Wählen Sie Weiter aus.

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.
   - Die generierten eindeutigen Match-IDs.
   - 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.

Sie sind jetzt bereit für:

- Bearbeiten Sie einen Abgleichsworkflow
- Löschen Sie einen passenden Workflow
- Führen Sie einen passenden Workflow aus

Erstellen Sie einen auf maschinellem Lernen basierenden Matching-Workflow

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.

Wenn AWS Entity Resolution eine Übereinstimmung zwischen zwei oder mehr Datensätzen in Ihren Daten gefunden wird, wird den Datensätzen im abgeglichenen Datensatz eine Match-ID zugewiesen.

Beim Abgleich, der auf maschinellem Lernen basiert, wird der Prozentsatz des Übereinstimmungskonfidenzniveaus angewendet.

So erstellen Sie einen ML-basierten Matching-Workflow:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem 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 Datenbank aus der Dropdownliste, wählen Sie die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

    Sie können bis zu 20 Dateneingaben hinzufügen.

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

    d. Geben Sie die Dienstzugriffsberechtigungen an, indem Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden auswählen.

Wenn Sie wählen...	THEN
Eine neue Servicerolle erstellen und verwenden	• 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, können Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt auswählen und dann einen AWS KMS Schlüssel eingeben, der zur Entschlüsselung Ihrer Dateneingabe verwendet wird.

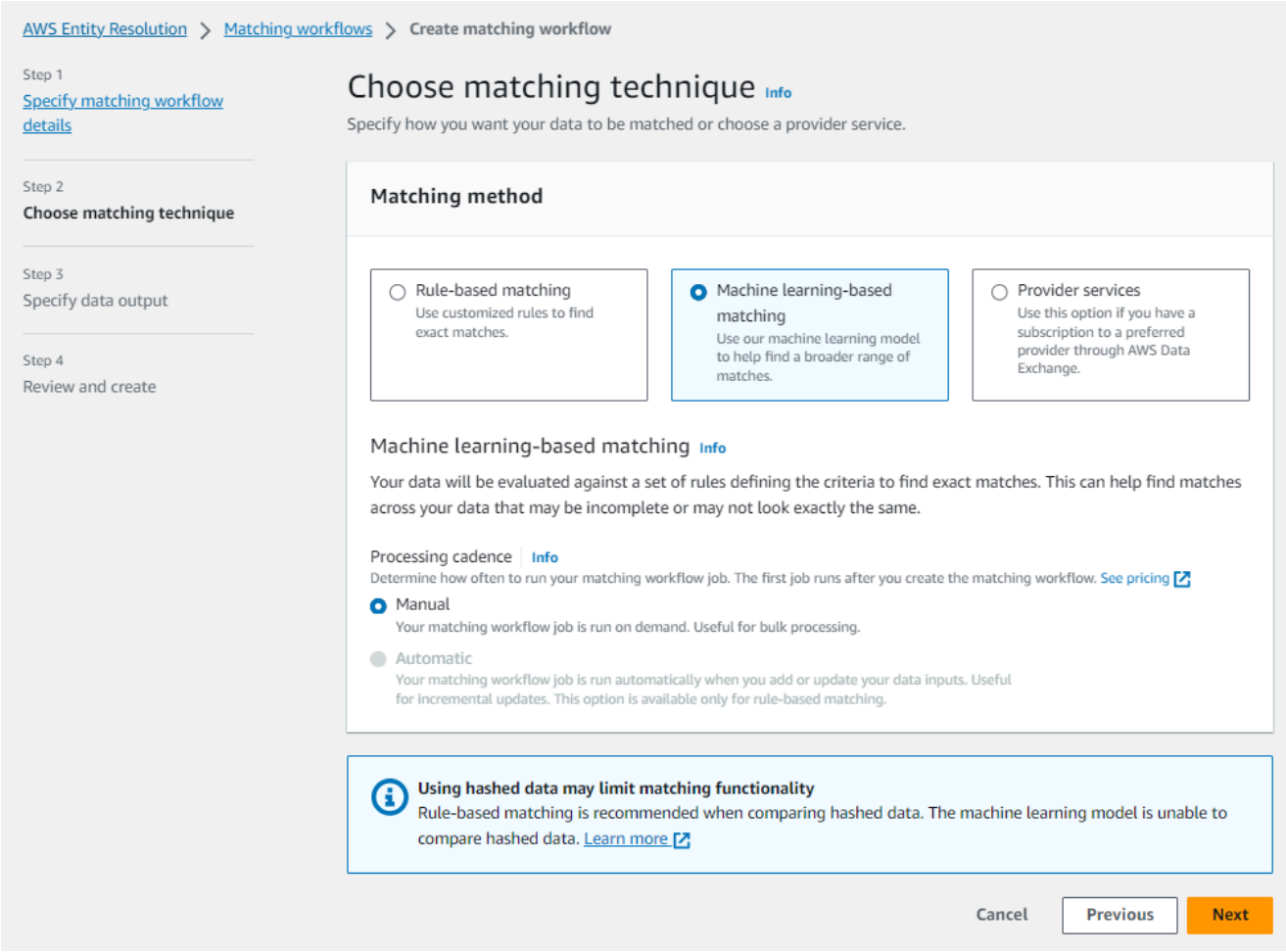
Wenn Sie wählen...	THEN
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtig t sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenric htlinie 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 aus.

5. Für Schritt 2: Passende Technik wählen:

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



b. Für den Verarbeitungsrhythmus ist die Option Manuell ausgewählt.

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

c. Wählen Sie Weiter aus.

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 unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel ARN ein.

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

   d. Sehen Sie sich für die Datenausgabe alle enthaltenen Felder an.

   e. Legen Sie fest, ob Sie Felder einschließen, ausblenden oder maskieren möchten.

Wenn du willst...	Dann wähle...
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 (Zurückse tzen).

f. Wählen Sie Weiter aus.

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.
   - Die generierten eindeutigen Match-IDs.
   - 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.

Sie sind jetzt bereit für:

- Bearbeiten Sie einen Abgleichsworkflow
- Löschen Sie einen passenden Workflow
- Führen Sie einen passenden Workflow aus

Erstellen Sie einen auf Providerdiensten basierenden Matching-Workflow

Wenn Sie ein Abonnement bei einem Anbieter abgeschlossen haben AWS Data Exchange, können Sie Ihre bekannten Kennungen Ihrem bevorzugten Anbieter zuordnen. AWS Entity Resolution unterstützt derzeit die folgenden Datenanbieterdienste:

- LiveRamp
- TransUnion
- Vereinheitlichte ID 2.0

Weitere Informationen zum Erstellen eines neuen Abonnements oder zur Wiederverwendung eines vorhandenen Abonnements für einen Anbieterdienst finden Sie unterAbonnieren Sie einen Anbieter-Service auf 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 verwendeten IDs auf Demand-Side-Plattformen, um eine Zielgruppe für eine Werbekampagne zu gewinnen. Mithilfe eines passenden Workflows mit können Sie LiveRamp Hash-E-Mail-Adressen in RampIDs auflösen.

> **Note**
>
> AWS Entity Resolution unterstützt die 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>durch Ihre 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 bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem 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 Datenbank aus der Dropdownliste aus, wählen Sie die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

   Sie können bis zu 20 Dateneingaben hinzufügen.

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

   Wenn Sie den reinen E-Mail-Auflösungsprozess verwenden, deaktivieren Sie die Option Daten normalisieren, da nur Hash-E-Mails für Eingabedaten verwendet werden.

d. Geben Sie die Dienstzugriffsberechtigungen an, indem Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden auswählen.

Wenn Sie wählen...	THEN
Eine neue Servicerolle erstellen und verwenden	• 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, können Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt auswählen und dann einen AWS KMS Schlüssel eingeben, der zur Entschlüsselung Ihrer Dateneingabe verwendet wird.

Wenn Sie wählen...	THEN
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtig t sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenric htlinie 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 aus.

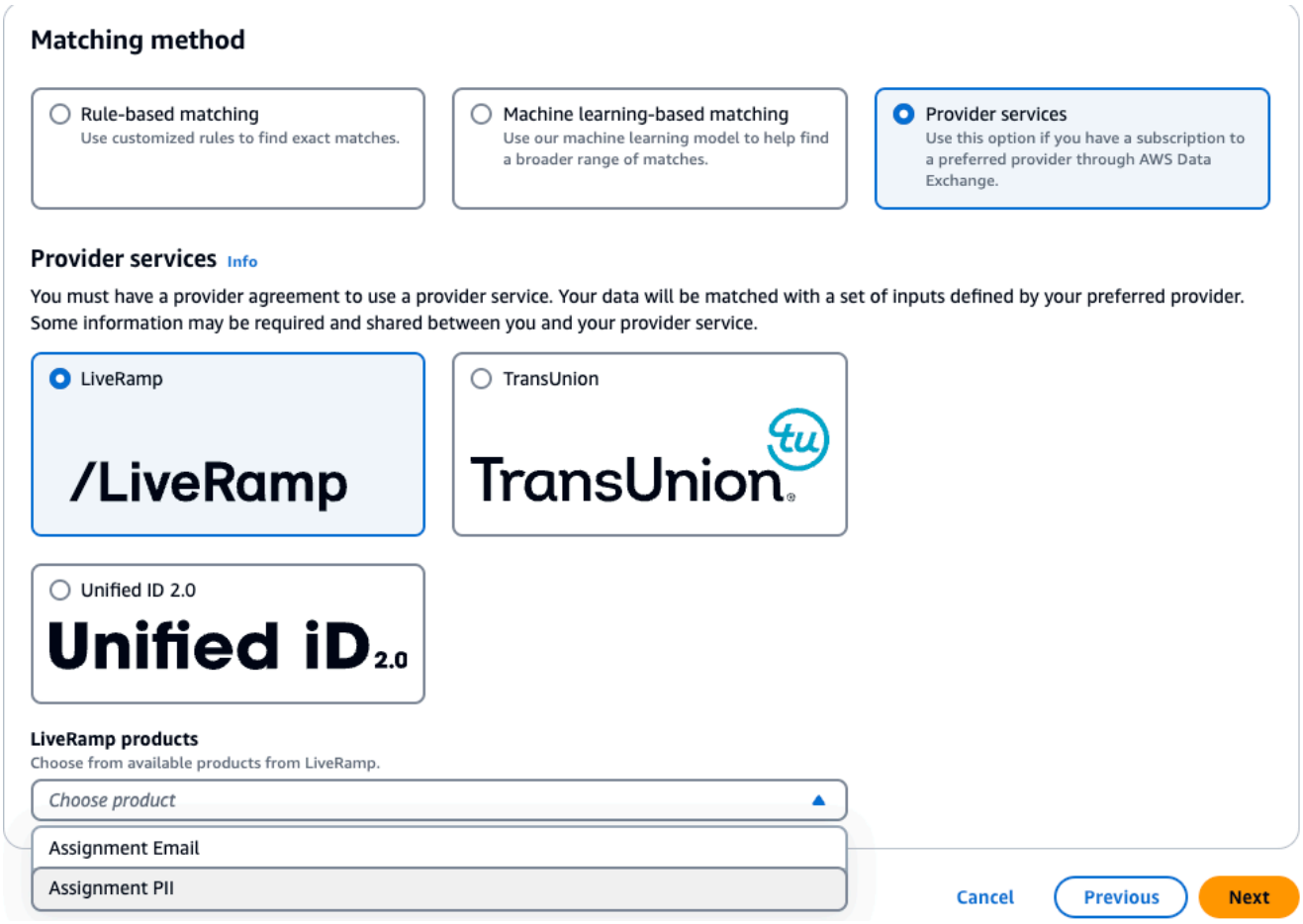
5. Für Schritt 2: Passende Technik wählen:

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

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

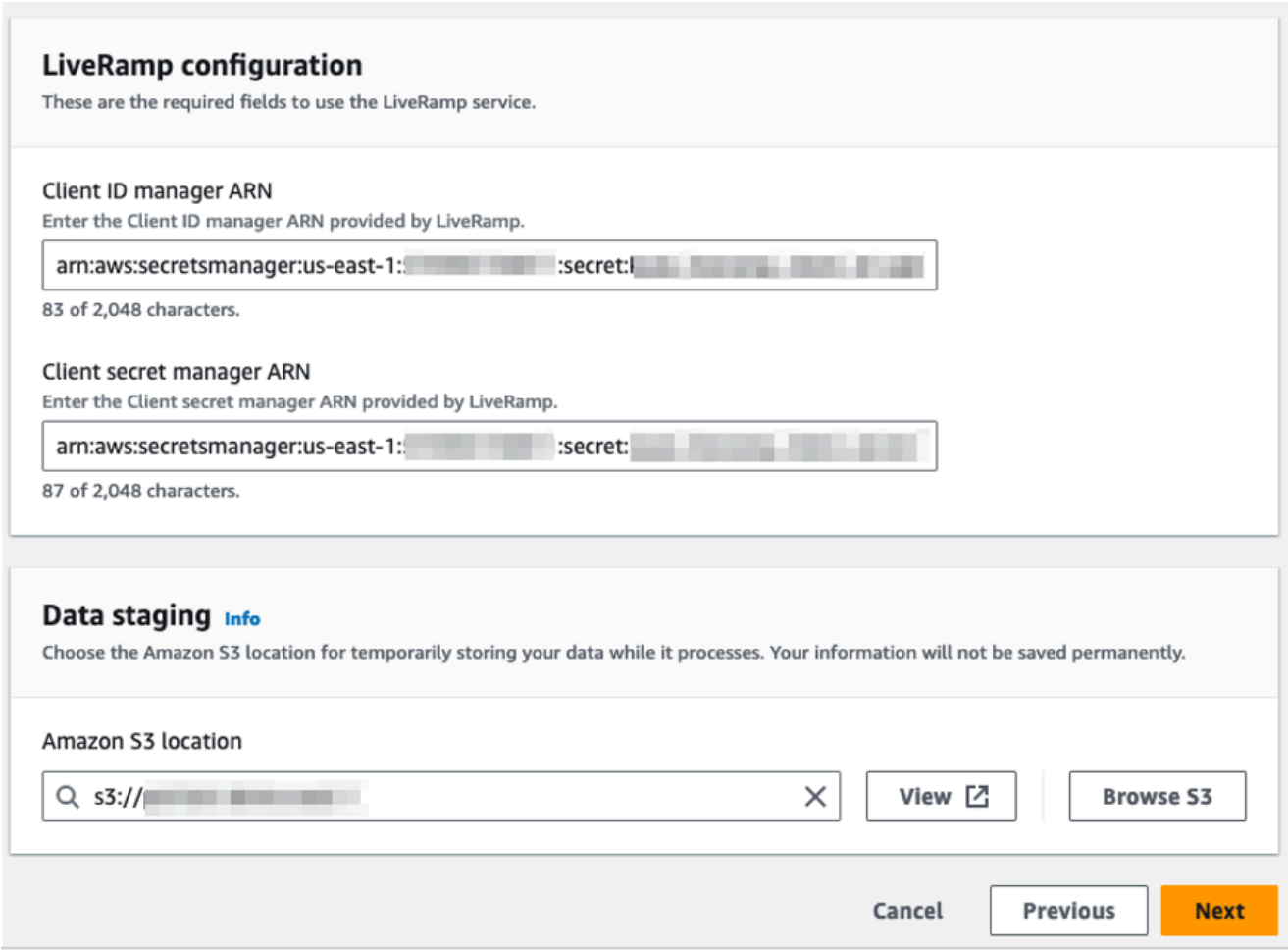
> **Note**
>
> Stellen Sie sicher, dass das Format und die Normalisierung Ihrer Dateneingabedatei den Richtlinien des Dienstanbieters entsprechen.
> Weitere Informationen zu den Richtlinien zur Formatierung von Eingabedateien für den Abgleichs-Workflow finden Sie in der Dokumentation unter Perform Identity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

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



> **Note**
>
> Wenn Sie Assignment PII wählen, müssen Sie bei der Entitätsauflösung mindestens eine Spalte angeben, in der es sich nicht um eine Identifikationsspalte handelt. Zum Beispiel GESCHLECHT.

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



e. Wählen Sie für 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 “Erstellen Sie eine 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 unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel ARN ein.

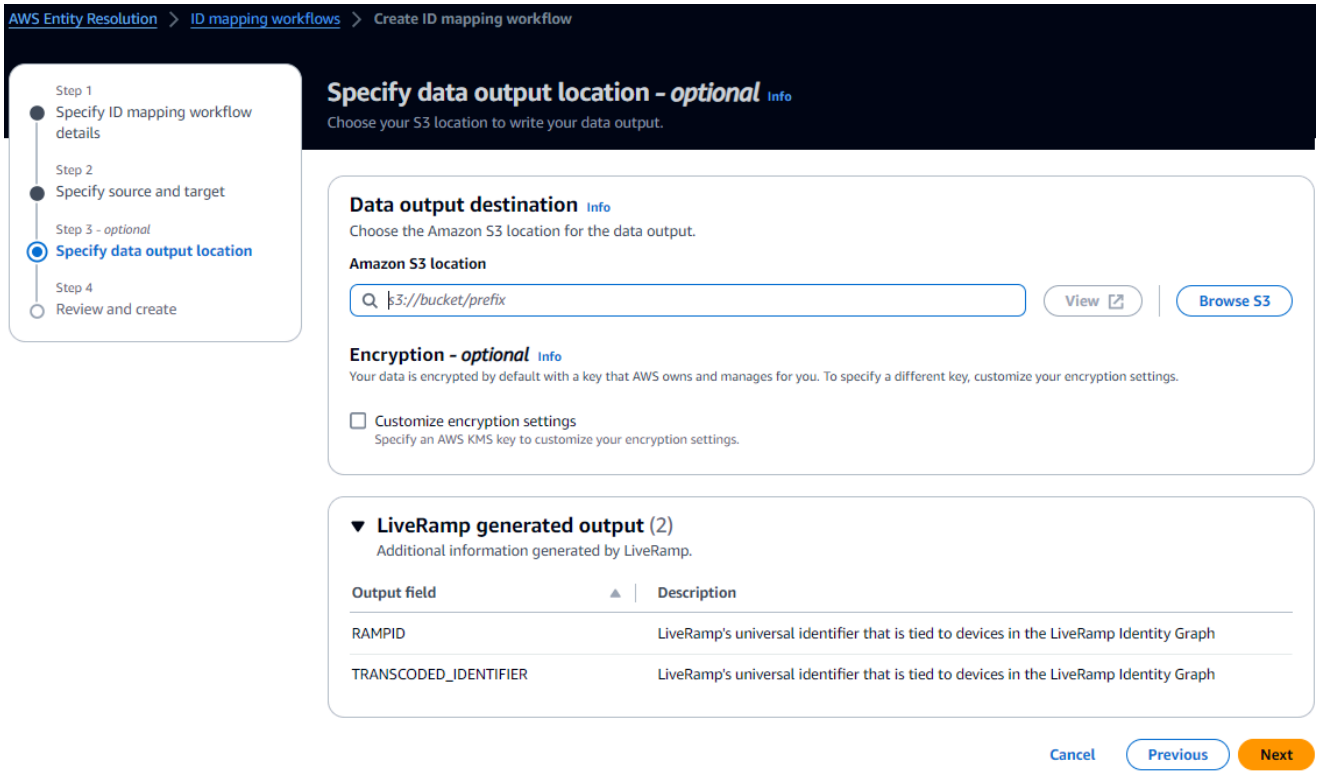
   c. Sehen Sie sich die LiveRamp generierte Ausgabe an.

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

   d. Sehen Sie sich für die Datenausgabe alle enthaltenen Felder an und legen Sie fest, ob Sie Felder einschließen, ausblenden oder maskieren möchten.

      > **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.

Wenn du möchtest...	Dann wähle...
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 (Zurückse tzen).



e. Wählen Sie Weiter aus.

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.

- Die generierten eindeutigen Match-IDs.
- 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.

Sie sind jetzt bereit für:

- Bearbeiten Sie einen Abgleichsworkflow
- Löschen Sie einen passenden Workflow

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 Einzel- und Haushalts-IDs bezeichnet werden. TransUnionermöglicht 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>durch Ihre 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 bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem 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 Datenbank aus der Dropdownliste aus, wählen Sie die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

      Sie können bis zu 20 Dateneingaben hinzufügen.

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

   d. Geben Sie die Dienstzugriffsberechtigungen an, indem Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden auswählen.

Wenn Sie wählen...	THEN
Eine neue Servicerolle erstellen und verwenden	• 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, können

Wenn Sie wählen...	THEN
	Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt auswählen und dann einen AWS KMS Schlüssel eingeben, der zur Entschlüsselung Ihrer Dateneingabe verwendet wird.

Wenn Sie wählen...	THEN
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtig t sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. Wenn es keine vorhandenen Servicerollen gibt, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenric htlinie 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 aus.

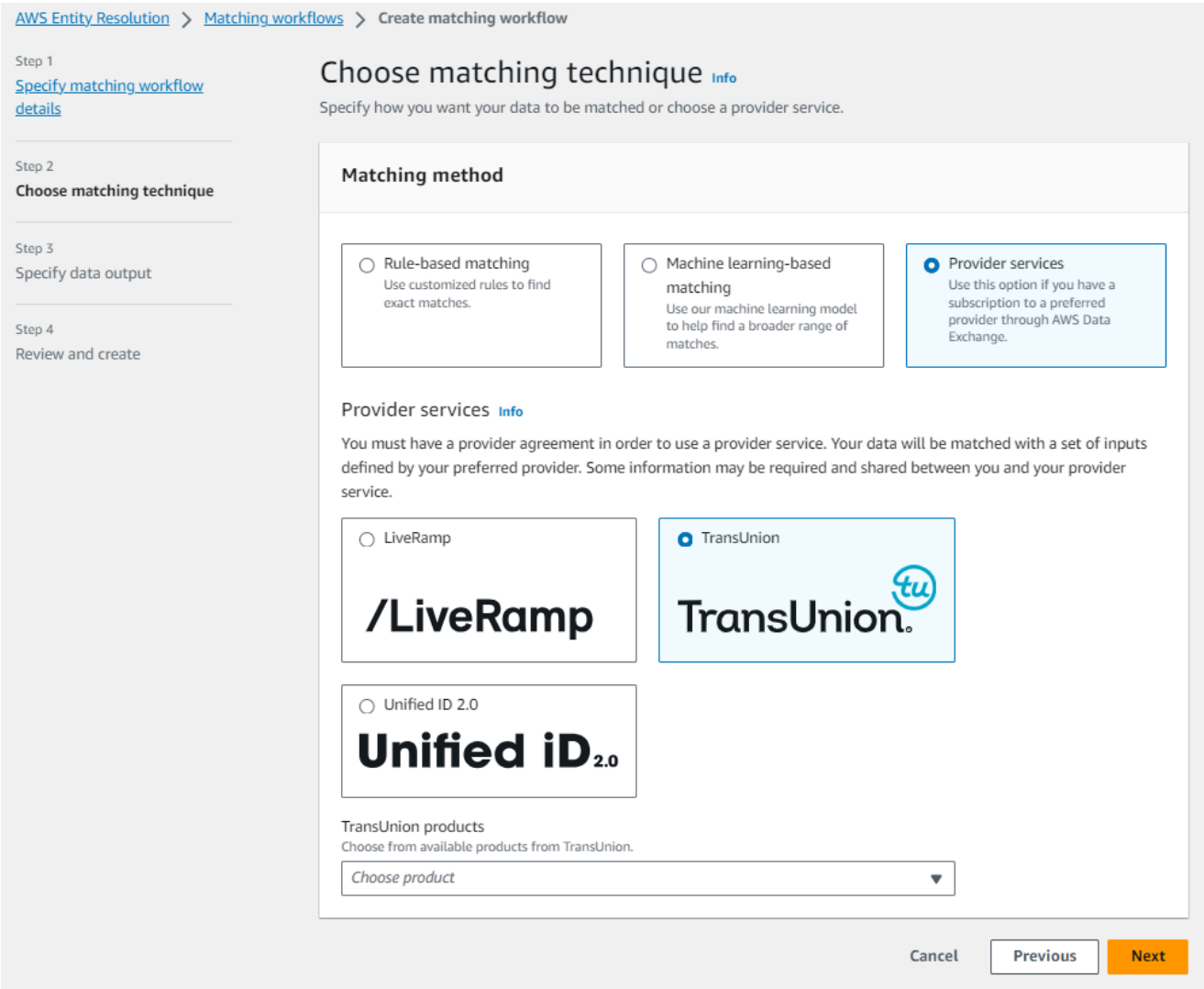
5. Für Schritt 2: Passende Technik wählen:

   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 “Erstellen Sie eine Workflow-Jobrolle für AWS Entity Resolution”.

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 unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel ARN ein.
   c. Sehen Sie sich die TransUnion generierte Ausgabe an.

      Dies sind die zusätzlichen Informationen, die von generiert wurden TransUnion.
   d. Sehen Sie sich für die Datenausgabe alle enthaltenen Felder an und legen Sie fest, ob Sie Felder einschließen, ausblenden oder maskieren möchten.

Wenn Sie möchten...	Dann wähle...
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 (Zurückse tzen).

   e. Sehen Sie sich für die vom System generierte Ausgabe alle enthaltenen Felder an.
   f. Wählen Sie Weiter aus.
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.
   - Die generierten eindeutigen Match-IDs.
   - 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.

Sie sind jetzt bereit für:

- Bearbeiten Sie einen Abgleichsworkflow
- Löschen Sie einen passenden Workflow

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 UID2-fähigen Teilnehmern im gesamten Werbeökosystem verlassen. Weitere Informationen finden Sie unter Überblick über Unified ID 2.0.

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

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

> **Note**
>
> Roh-UID2s werden durch das Hinzufügen von Salzen aus Salt-Buckets erzeugt, die ungefähr einmal pro Jahr rotiert werden. Dadurch wird auch die Roh-UID2 entsprechend rotiert. Es wird daher empfohlen, die Roh-UID2s täglich zu aktualisieren. Weitere Informationen finden Sie unter https://unifiedid.com/docs/getting-started/gs-faqs # 2 -incremental-updates how-often-should-uid s-be-refreshed-for

So erstellen Sie einen passenden Workflow mit UID 2.0:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem 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 Datenbank aus der Dropdownliste aus, wählen Sie die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

       Sie können bis zu 20 Dateneingaben hinzufügen.
    c. Lassen Sie die Option Daten normalisieren aktiviert, sodass Dateneingaben (**`Email Address`**oder**`Phone number`**) vor dem Abgleich normalisiert werden.

Weitere Informationen zur Normalisierung finden Sie unter **`Email Address`** 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 UID 2.0-Dokumentation.

d. Geben Sie die Dienstzugriffsberechtigungen an, indem Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden auswählen.

Wenn Sie wählen...	THEN
Eine neue Servicerolle erstellen und verwenden	• 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, können Sie die Option Diese Daten werden mit einem KMS-Schlüssel verschlüsselt auswählen und dann einen AWS KMS Schlüssel eingeben, der zur Entschlüsselung Ihrer Dateneingabe verwendet wird.

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

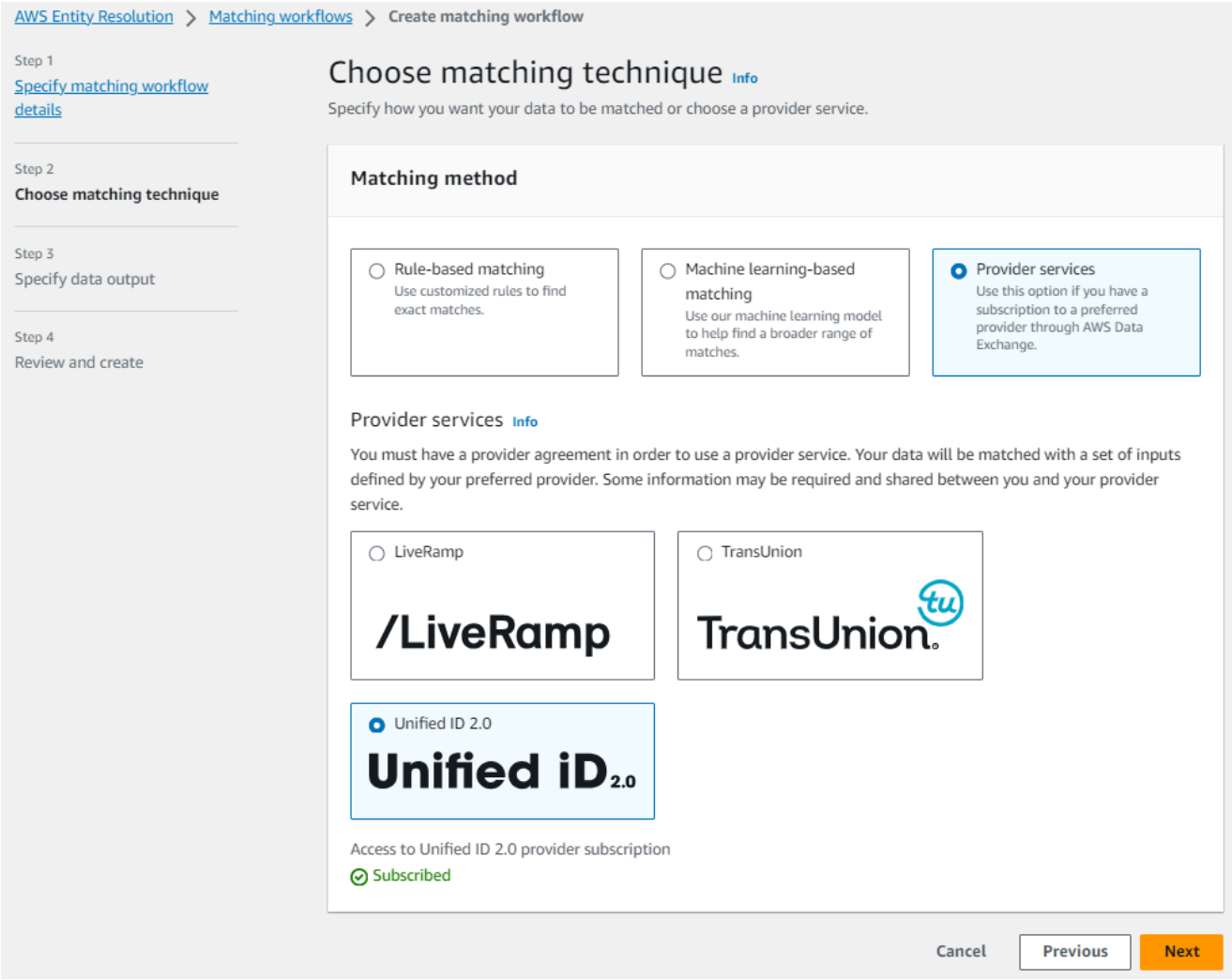
e. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.

f. Wählen Sie Weiter aus.

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 aus.

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 unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel ARN ein.

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

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

d. Sehen Sie sich für die Datenausgabe alle enthaltenen Felder an und legen Sie fest, ob Sie Felder einschließen, ausblenden oder maskieren möchten.

Wenn Sie möchten...	Dann wähle...
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 (Zurückse tzen).

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

f. Wählen Sie Weiter aus.

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.
   - Die generierten eindeutigen Match-IDs.
   - 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.

Sie sind jetzt bereit für:

- Bearbeiten Sie einen Abgleichsworkflow
- Löschen Sie einen passenden Workflow

Führen Sie einen passenden Workflow aus

Nachdem Sie einen regelbasierten Abgleichs-Workflow oder einen auf maschinellem Lernen basierenden Abgleichs-Workflow mit dem Verarbeitungstyp Manuell erstellt haben, können Sie einen Abgleichs-Workflow-Job ausführen.

> **Note**
>
> Wenn Sie einen passenden Workflow mit dem Verarbeitungstyp Automatisch erstellen, werden Ihre passenden Workflow-Jobs jedes Mal ausgeführt, wenn eine Dateneingabe aktualisiert wird.

AWS Entity Resolution liest Ihre Daten von der oder den angegebenen Speicherorten aus und findet eine Übereinstimmung zwischen zwei oder mehr Datensätzen in Ihren Daten. Anschließend wird den Datensätzen im abgeglichenen Datensatz eine Match-ID zugewiesen.

- Wenn Sie die regelbasierte Vergleichstechnik angegeben haben, AWS Entity Resolution wird auch die Regelnummer zugewiesen, die angewendet wurde, mit der der Treffer generiert wurde.
- Wenn Sie die auf maschinellem Lernen basierende Vergleichstechnik angegeben haben, AWS Entity Resolution wird auch das Konfidenzniveau der Treffer in Prozent zugewiesen.

AWS Entity Resolution schreibt dann Datenausgabedateien an einen von Ihnen ausgewählten Speicherort.

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

Die Datenausgabe enthält sowohl eine Datei für erfolgreiche Treffer als auch eine Datei für Fehler. Die Datenausgabe kann mehrere Felder enthalten. Die erfolgreichen Ergebnisse werden in einen `success` Ordner geschrieben, und der Ordner wird mehrere Dateien enthalten, von denen jede eine Teilmenge der erfolgreichen Datensätze enthält. Ebenso 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 unterWorkflows zur Fehlerbehebung.

So führen Sie einen passenden Workflow aus:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
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 Workflow ausführen aus.

   Es wird eine Meldung angezeigt, die darauf hinweist, dass der Job gestartet wurde.
5. Sehen Sie sich auf der Registerkarte Metriken unter Auftragsverlauf Folgendes an:

   - Der Status des passenden Workflow-Jobs: In Bearbeitung, Abgeschlossen, Fehlgeschlagen
   - Die Anzahl der verarbeiteten Datensätze.
   - Die Anzahl der gefundenen Treffer.
   - Die Anzahl der eindeutigen Datensätze.
   - Die Dauer des Jobs.
   - Die Job-ID.
6. 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.

Nächste Schritte

Sie sind jetzt bereit für:

- Bearbeiten Sie einen Abgleichsworkflow
- Löschen Sie einen passenden Workflow

Einen ID-Namespace erstellen

Ein ID-Namespace ist ein Wrapper für Ihre Datentabelle, mit dem Sie Metadaten bereitstellen, in denen Ihre Daten und Abgleichstechniken sowie deren Verwendung in einem ID-Mapping-Workflow erläutert werden.

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

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

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

Die folgenden Themen führen Sie durch eine Reihe von Schritten, um die Quell- und Ziel-ID-Namespaces zu erstellen und anschließend Ihre Datenausgabe in Amazon Simple Storage Service (Amazon S3) zu spezifizieren.

> **Note**
>
> AWS Entity Resolution bietet derzeit LiveRamp Transcodierung für die ID-Namespace-Methode an, wenn Sie einen ID-Namespace erstellen.

Themen

Erstellen Sie eine ID-Namespace-Quelle

In diesem Thema wird der Vorgang zum Erstellen einer ID-Namespace-Quelle auf der AWS Entity Resolution Konsole beschrieben. Dies ist die Quelle der Daten in einem ID-Zuordnungs-Workflow.

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

Um eine ID-Namespace-Quelle zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem 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 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. Sehen Sie sich die ID-Namespace-Methode an.

   > **Note**
   >
   > AWS Entity Resolution bietet derzeit den LiveRamp Provider-Service 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 unterAbonnieren Sie einen Anbieter-Service auf AWS Data Exchange.

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

   Sie können bis zu 20 Dateneingaben hinzufügen.
7. Um die Dienstzugriffsberechtigungen anzugeben, wählen Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden aus.

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

Wenn Sie wählen...	THEN
Verwenden Sie eine vorhandene Servicerolle	Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Wenn Sie berechtigt sind, Rollen aufzulisten, wird die Rollenliste angezeigt. 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. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderl ichen Berechtigungen hinzuzufü gen.

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“.

Erstellen Sie ein ID-Namespace-Ziel

In diesem Thema wird der Vorgang zum Erstellen eines ID-Namespace-Ziels auf der AWS Entity Resolution Konsole beschrieben. Dies ist das Ziel der Daten in einem ID-Zuordnungs-Workflow. Alle Quellen lösen sich auf das Ziel auf.

Um ein ID-Namespace-Ziel zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem 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 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. Sehen Sie sich die ID-Namespace-Methode an.

   > **Note**
   >
   > AWS Entity Resolution bietet derzeit den LiveRamp Provider-Service 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 unterAbonnieren Sie einen Anbieter-Service auf 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“.

Nachdem Sie die ID-Namespaces erstellt haben, die für einen ID-Mapping-Workflow mit zwei Komponenten erforderlich sind AWS-Konten, können Sie den ID-Zuordnungs-Workflow erstellen.

Einen ID-Mapping-Workflow erstellen

Der ID-Mapping-Workflow in AWS Entity Resolution ist derzeit in integriert LiveRamp. Wenn Sie ein Abonnement für den LiveRamp Dienst haben, können Sie einen ID-Mapping-Workflow erstellen, LiveRamp um die Transcodierung durchzuführen. Mit der LiveRamp Transcodierung können Sie eine Reihe von Quell-RampIDs in eine beliebige Ziel-RampID übersetzen. Indem Sie die RampID als Token zur Darstellung Ihrer Kunden verwenden, können Sie vermeiden, Kundendaten direkt an Werbeplattformen weiterzugeben.

Sie können die ID-Zuordnung zwischen zwei Datensätzen selbst AWS-Konto oder zwischen zwei verschiedenen Datensätzen durchführen. AWS-Konten Ihre Dateneingabequelle und Ihr Ziel hängen von der Art der ID-Zuordnung ab, die Sie durchführen möchten.

Weitere Informationen finden Sie auf der LiveRamp Dokumentationswebsite unter Perform Translation Through ADX.

Themen

Voraussetzung

Für diesen ID-Mapping-Workflow ist ein Daten-Staging-Bucket von Amazon Simple Storage Service (Amazon S3) erforderlich, in den Sie vorübergehend die Workflow-Ausgabe für die ID-Zuordnung schreiben möchten. Bevor Sie einen ID-Mapping-Workflow mit erstellen LiveRamp, fügen Sie die folgende Berechtigungsrichtlinie hinzu, mit der Sie auf den Daten-Staging-Bucket zugreifen können.

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

```
                "AWS": "arn:aws:iam::715724997226:root"

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

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

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

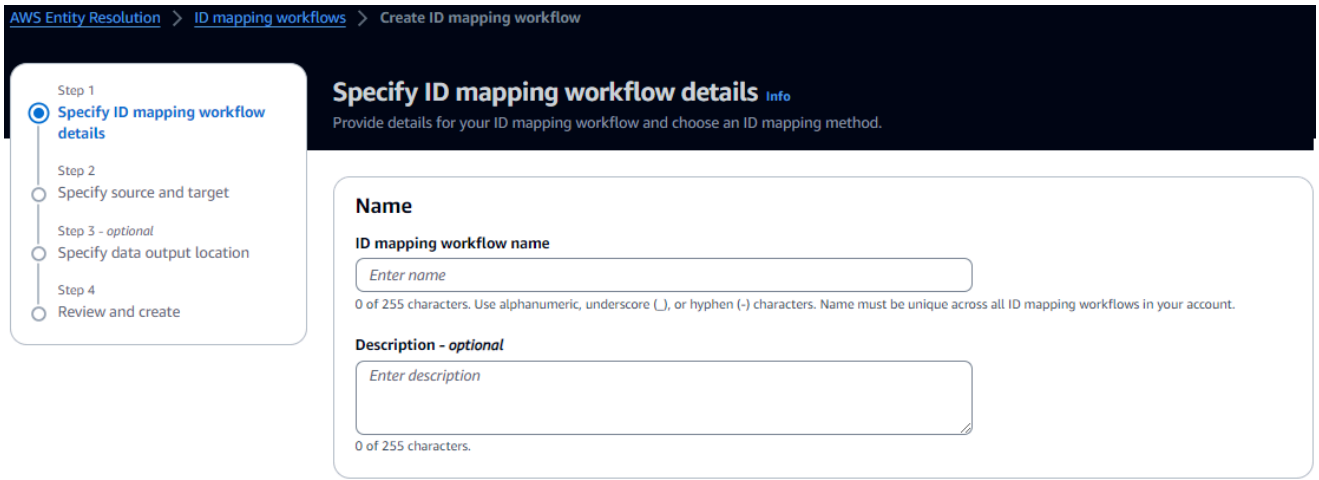
Einen ID-Mapping-Workflow für einen erstellen AWS-Konto

Nachdem Sie die Einrichtungsschritte abgeschlossen und ein Schema-Mapping erstellt haben, können Sie einen oder mehrere ID-Mapping-Workflows erstellen, um mithilfe von verwalteten oder abgeleiteten RampIDs einen Satz von Quell-RampIDs in einen anderen zu übersetzen.

Um einen ID-Mapping-Workflow für eine zu erstellen AWS-Konto

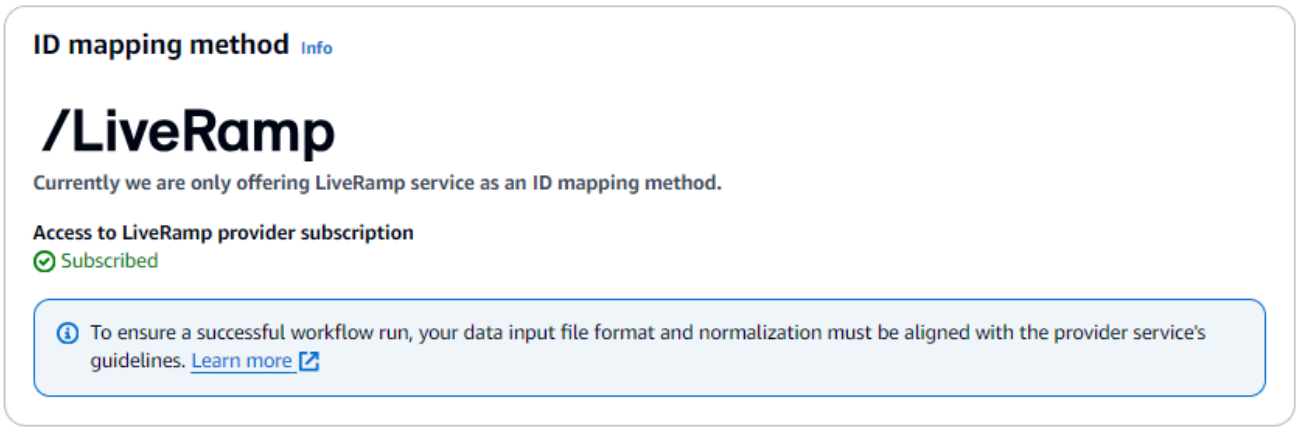
1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie auf der Seite mit den Workflows für die ID-Zuordnung in der oberen rechten Ecke die Option ID-Mapping-Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Workflow-Details für die ID-Zuordnung angeben wie folgt vor:

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



    b. Sehen Sie sich die Methode zur ID-Zuordnung an.

    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 unterAbonnieren Sie einen Anbieter-Service auf AWS Data Exchange.



> **Note**
>
> Stellen Sie sicher, dass das Format Ihrer Dateneingabedatei den Richtlinien des Dienstanbieters entspricht. Weitere Informationen zu den Richtlinien zur Formatierung LiveRamp von Eingabedateien finden Sie unter Perform Translation Through ADX auf der LiveRamp Dokumentationswebsite.

c. Geben Sie für die LiveRamp Konfiguration die folgenden Werte ein, die Folgendes LiveRamp bieten:

- Kunden-ID-Manager ARN
- Secret Manager ARN für Kunden

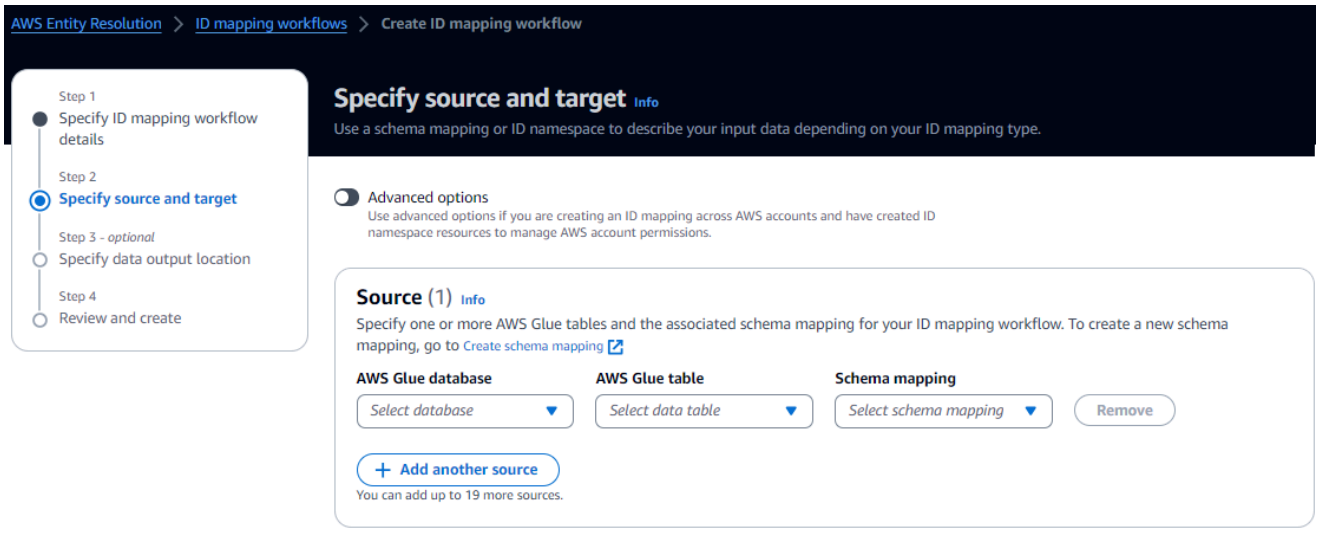
d. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

e. Wählen Sie Weiter aus.

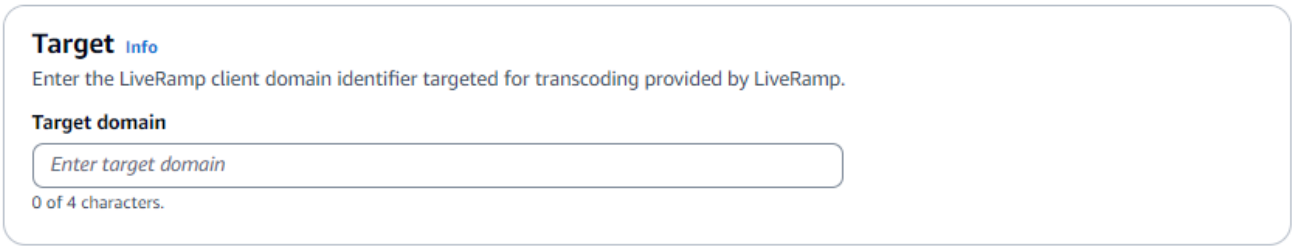
5. Gehen Sie für Schritt 2: Quelle und Ziel angeben wie folgt vor:

   a. Wählen Sie für Quelle eine AWS GlueDatenbank aus der Dropdownliste aus, wählen Sie die AWS Glue Tabelle und dann die entsprechende Schemazuordnung aus.

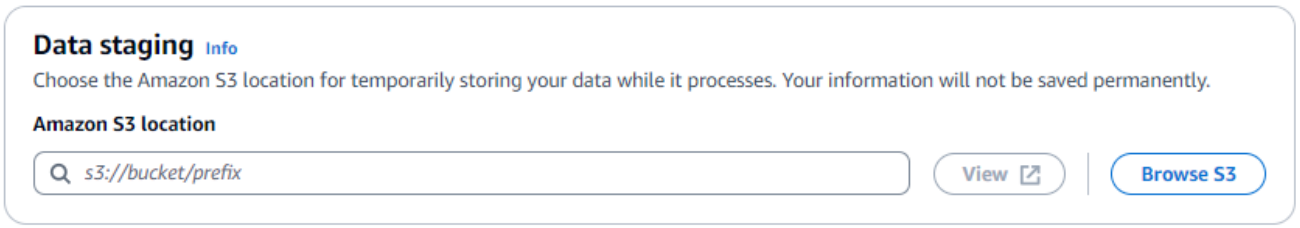
      Sie können bis zu 19 Dateneingaben hinzufügen.



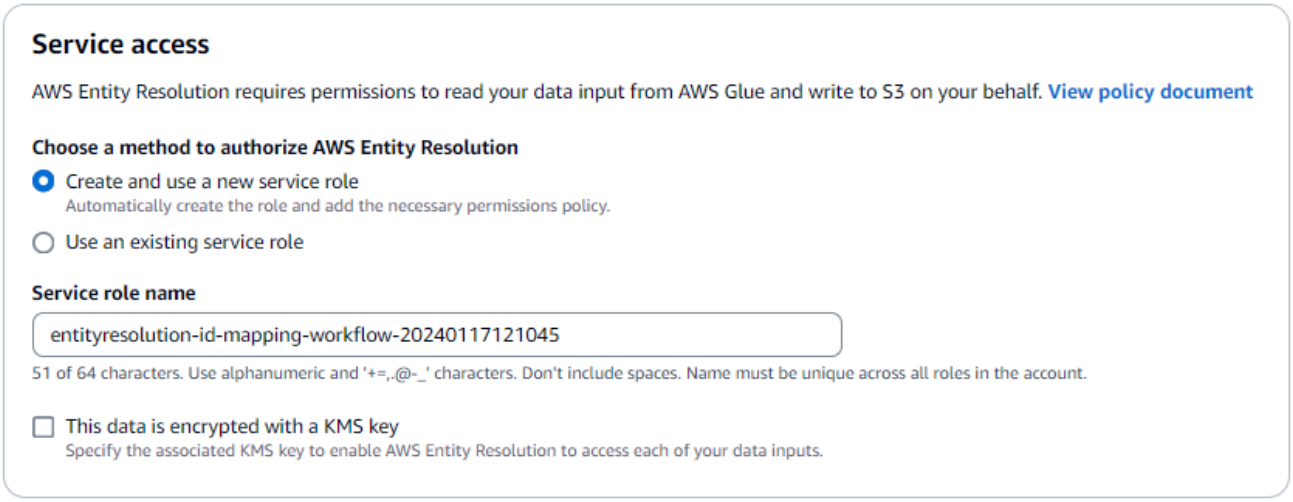
   b. Geben Sie für Target die LiveRamp Client-Domänen-ID ein, die für die Transcodierung vorgesehen ist und die Folgendes LiveRamp bietet:



   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 Service-Zugriffsberechtigungen anzugeben, wählen Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden.

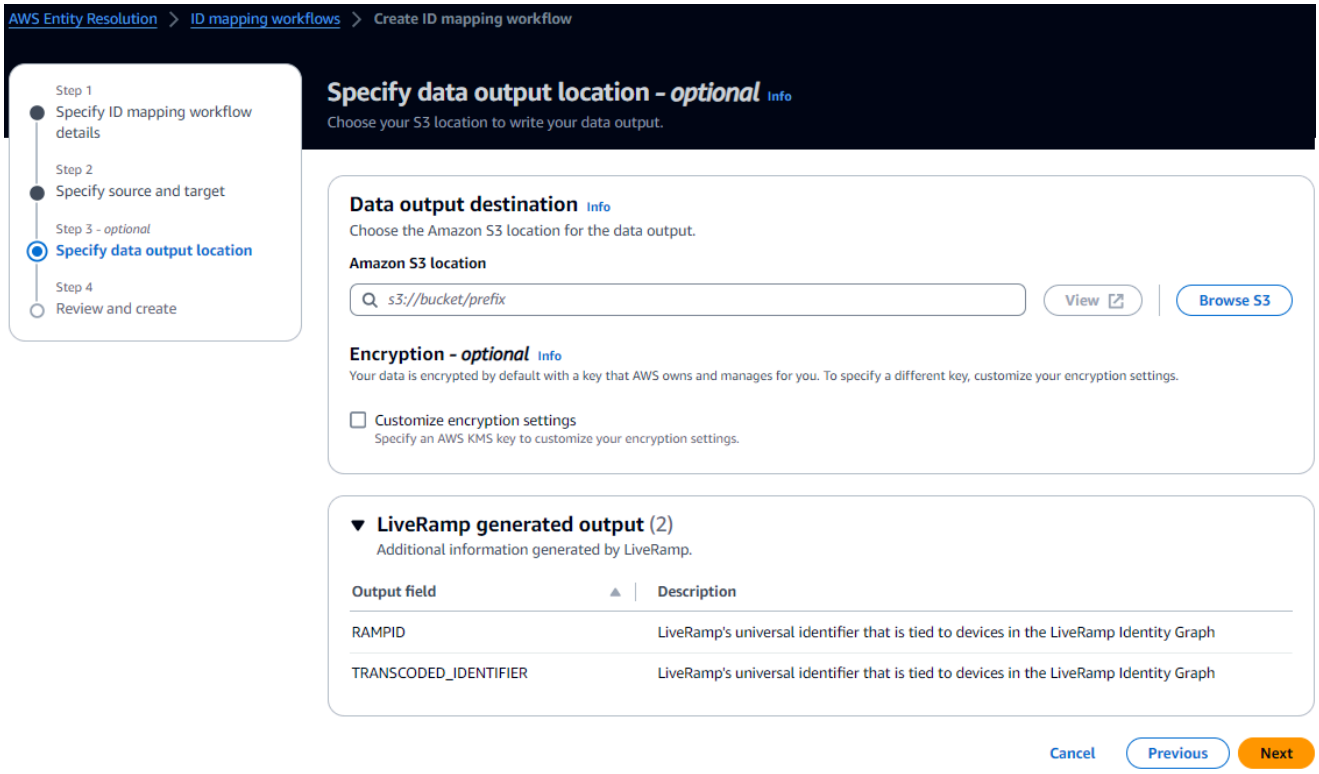


Wenn Sie wählen...	THEN
Eine neue Servicerolle erstellen und verwenden	AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. Der Standardname für die Dienstrolle lautet`entityresolution-id-mapping-workflow-<timestamp>` . Sie müssen über die erforderlichen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

Wenn Sie wählen...	THEN
Verwenden Sie eine vorhandene Servicerolle	Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Wenn Sie berechtigt sind, Rollen aufzulisten, wird die Rollenliste angezeigt. 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. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderl ichen Berechtigungen hinzuzufü gen.

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

c. Wählen Sie Weiter aus.



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

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

   b. Wählen Sie Erstellen.

      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, sind Sie bereit, einen ID-Zuordnungs-Workflow auszuführen

Erstellen eines Workflows zur ID-Zuordnung, der zwei Elemente umfasst AWS-Konten

Voraussetzung

Für die Erstellung eines Workflows zur ID-Zuordnung für zwei AWS-Konten Personen ist eine Zugriffsberechtigung für LiveRamp den S3-Bucket und den vom Kunden verwalteten Schlüssel AWS Key Management Service (AWS KMS) erforderlich. Bevor Sie einen ID-Mapping-Workflow für zwei AWS-Konten mit erstellen LiveRamp, fügen Sie die folgende Berechtigungsrichtlinie hinzu, die den LiveRamp Zugriff auf den S3-Bucket und den vom Kunden verwalteten Schlüssel ermöglicht.

```
{
    "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>durch Ihre eigenen Informationen.

<KMSKeyARN>	Der ARN eines vom AWS KMS Kunden verwalteten Schlüssels.

Erstellen Sie einen Workflow für die ID-Zuordnung

Bevor Sie einen Workflow für die ID-Zuordnung erstellen, der zwei AWS-Konten Elemente umfasst, müssen Sie zunächst die folgenden Schritte ausführen:

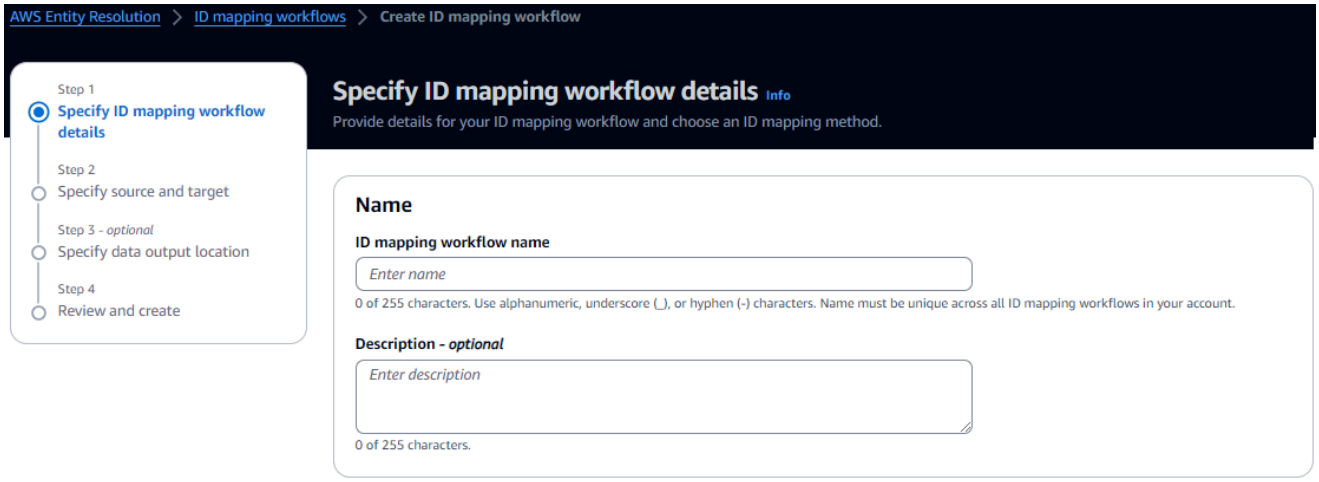
- Erfüllen Sie die Voraussetzungen, um dem vom Kunden verwalteten Schlüssel die Berechtigungen hinzuzufügen.
- Führen Sie die Aufgaben unter au Einrichten AWS Entity Resolution.
- Erstellen Sie eine ID-Namespace-Quelle.
- Erstellen Sie ein ID-Namespace-Ziel.

Nachdem Sie die zuvor aufgelisteten Aufgaben abgeschlossen haben, können Sie einen oder mehrere Workflows für die ID-Zuordnung erstellen, um eine Reihe von Quell-RampIDs mithilfe von verwalteten oder abgeleiteten RampIDs in eine andere zu übersetzen.

Um einen Workflow für die ID-Zuordnung zu erstellen, der zwei Elemente umfasst AWS-Konten

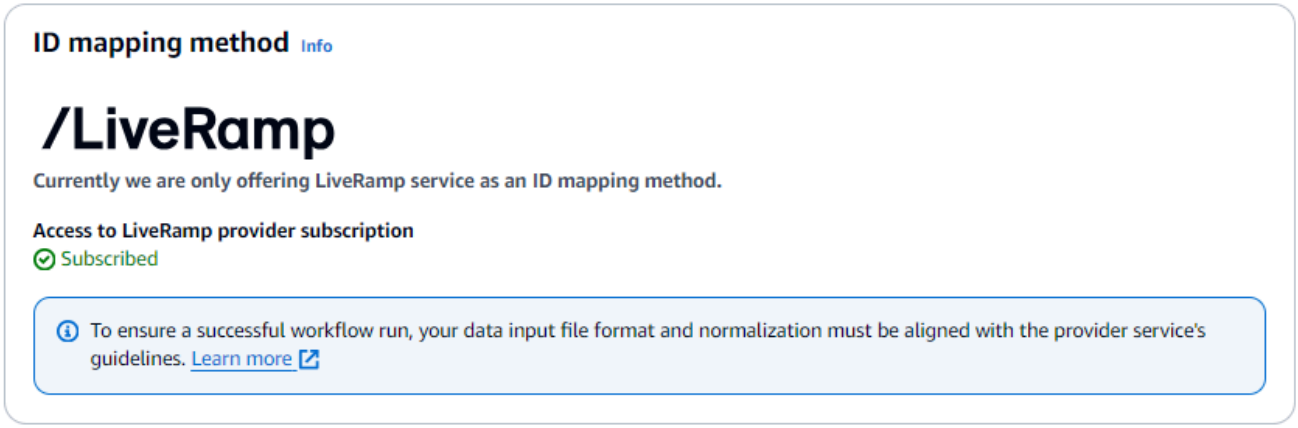
1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie auf der Seite mit den Workflows für die ID-Zuordnung in der oberen rechten Ecke die Option ID-Mapping-Workflow erstellen aus.
4. Gehen Sie für Schritt 1: Workflow-Details für die ID-Zuordnung angeben wie folgt vor:

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



b. Sehen Sie sich die Methode zur ID-Zuordnung an.

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 unter[Abonnieren Sie einen Anbieter-Service auf AWS Data Exchange](#).



> **Note**
>
> Stellen Sie sicher, dass das Format Ihrer Dateneingabedatei den Richtlinien des Dienstanbieters entspricht. Weitere Informationen zu den Richtlinien zur Formatierung LiveRamp von Eingabedateien finden Sie unter Perform Translation Through ADX auf der LiveRamp Dokumentationswebsite.

c. Geben Sie für die LiveRamp Konfiguration die folgenden Werte ein, die Folgendes LiveRamp bieten:

- Kunden-ID-Manager ARN
- Secret Manager ARN für Kunden

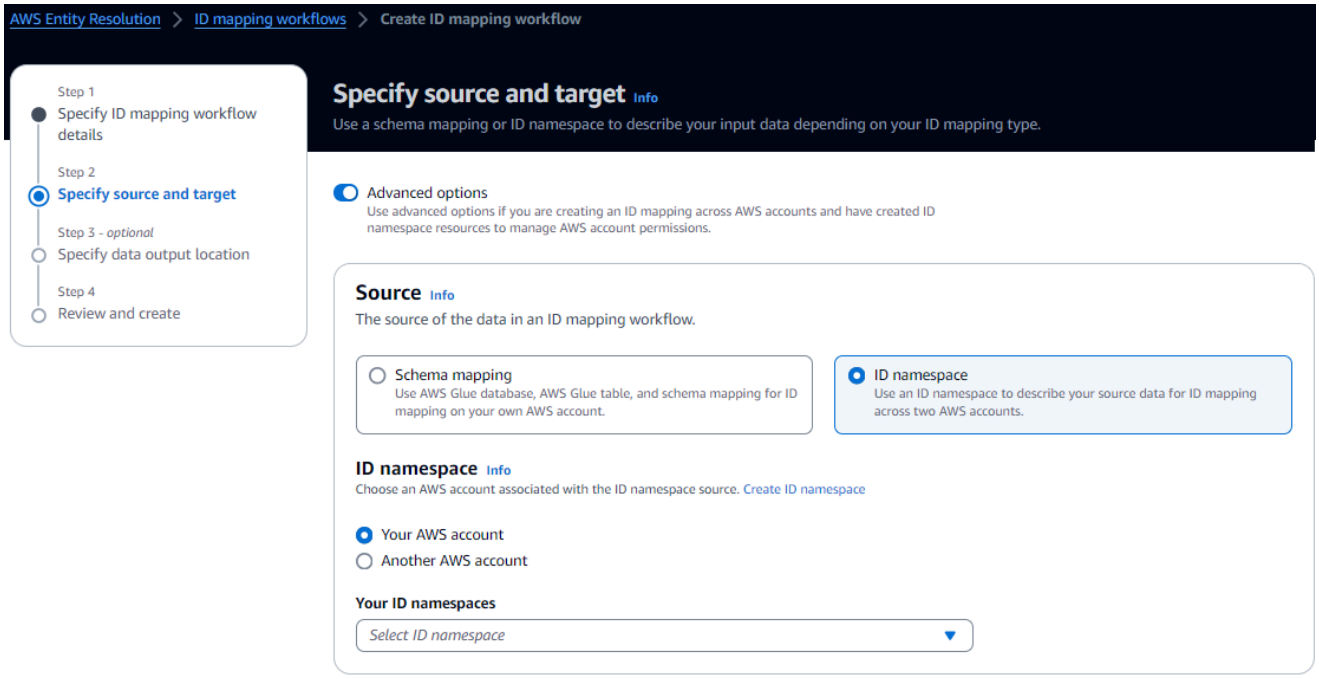
d. (Optional) Um Tags für die Ressource zu aktivieren, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

e. Wählen Sie Weiter aus.

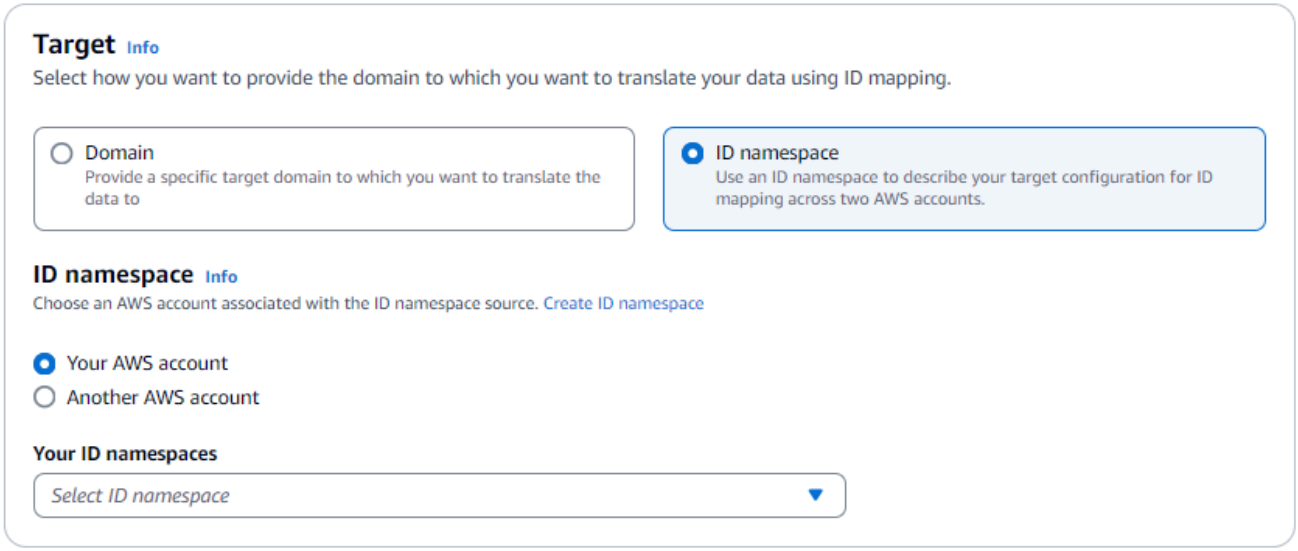
5. Gehen Sie für Schritt 2: Quelle und Ziel angeben wie folgt vor:

a. Aktivieren Sie „Erweiterte Optionen“.

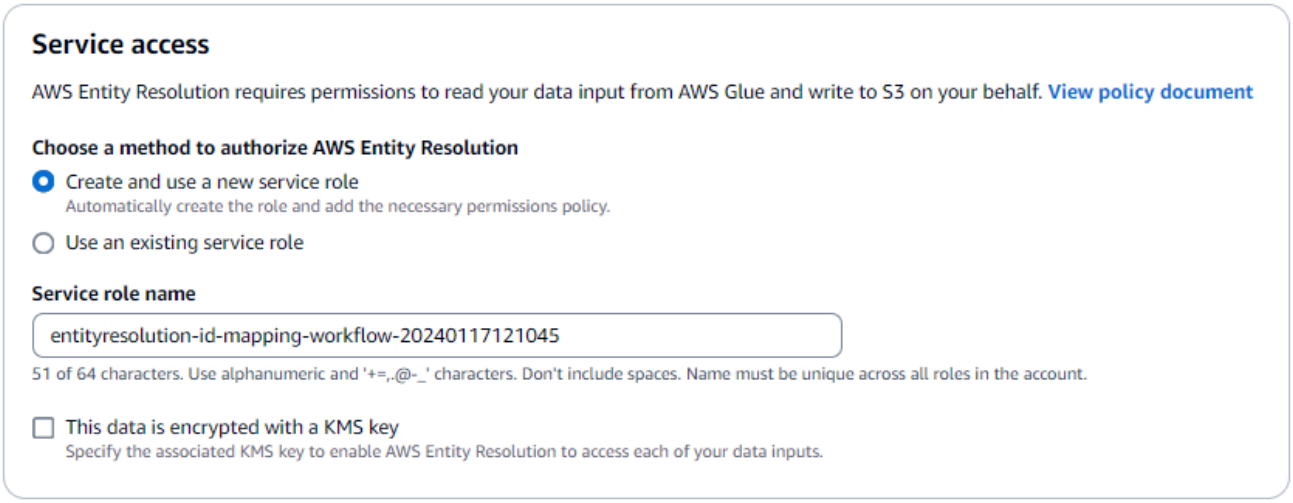
b. Wählen Sie als Quelle den ID-Namespace aus.



c. Wählen Sie für Target den ID-Namespace aus.



d. Um die Dienstzugriffsberechtigungen anzugeben, wählen Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden aus.

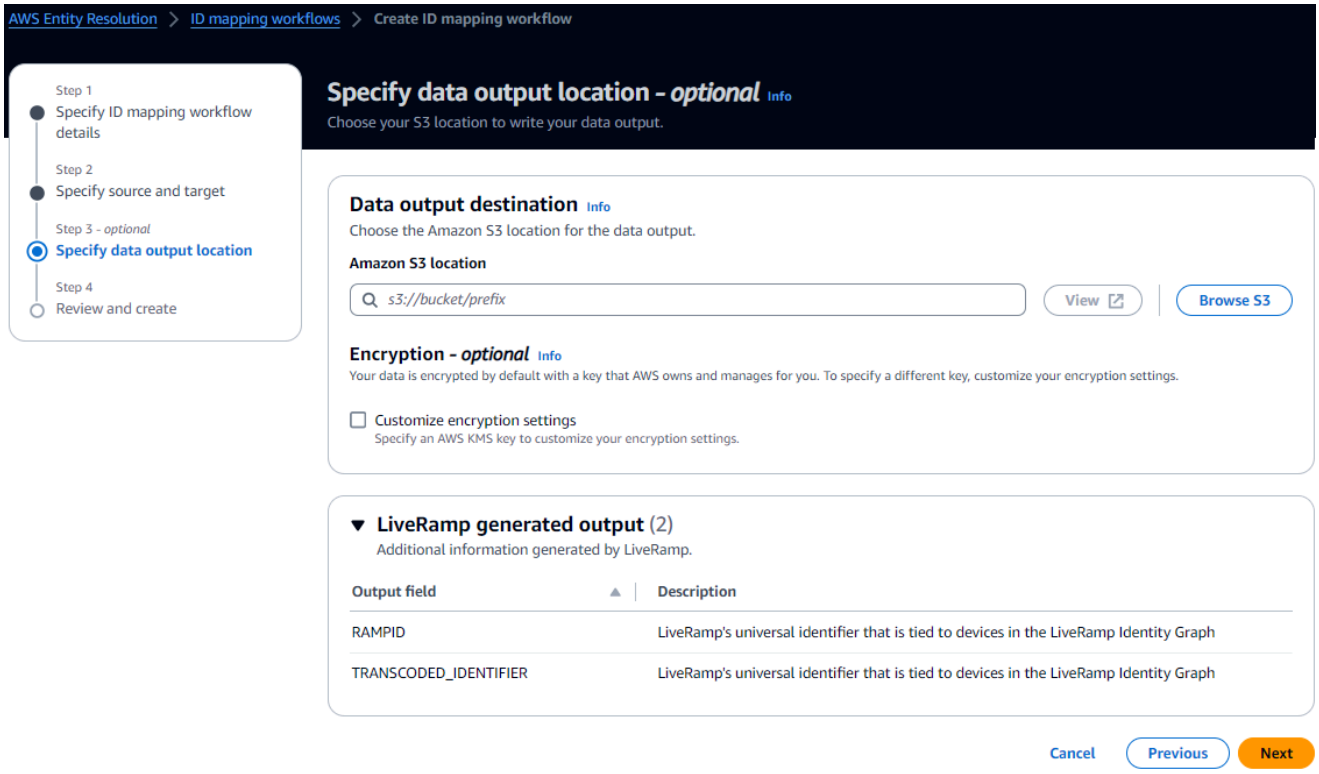


Wenn Sie wählen...	THEN
Eine neue Servicerolle erstellen und verwenden	AWS Entity Resolution erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. Der Standardname für die Dienstrolle lautet`entityresolution-id-mapping-workflow-<timestamp>` . Sie müssen über die erforderlichen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

Wenn Sie wählen...	THEN
Verwenden Sie eine vorhandene Servicerolle	Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Wenn Sie berechtigt sind, Rollen aufzulisten, wird die Rollenliste angezeigt. 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. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderl ichen Berechtigungen hinzuzufü gen.

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

c. Wählen Sie Weiter aus.



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

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

   b. Wählen Sie Erstellen.

      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 AWS-Konto oder einen ID-Zuordnungs-Workflow für zwei erstellt haben AWS-Konten, können Sie den ID-Zuordnungs-Workflow ausführen.

Um einen Workflow für die ID-Zuordnung auszuführen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den Workflow für die ID-Zuordnung aus.
4. Wählen Sie auf der Detailseite des ID-Mapping-Workflows in der oberen rechten Ecke die Option Ausführen aus.
5. Sehen Sie sich auf der Seite mit den entsprechenden Workflow-Details auf der Registerkarte Metriken unter Metriken für den letzten Job Folgendes an:

   - Die Job-ID
   - 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 der verbinden`TRANSCODED_ID`.

Ausführen eines Workflows zur ID-Zuordnung mit einem neuen Ausgabeziel

Nachdem Sie einen ID-Mapping-Workflow für einen AWS-Konto oder einen ID-Mapping-Workflow für zwei erstellt haben AWS-Konten, können Sie einen anderen S3-Speicherort für die Datenausgabe wählen.

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

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den Workflow für die ID-Zuordnung aus.
4. Wählen Sie auf der Detailseite des ID-Mapping-Workflows in der oberen rechten Ecke 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 unter Verschlüsselung die Verschlüsselungseinstellungen anpassen wählen, geben Sie den AWS KMS Schlüssel-ARN ein oder wählen Sie AWS KMS Schlüssel erstellen.
6. Um die Dienstzugriffsberechtigungen anzugeben, wählen Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden aus.

Wenn Sie wählen...	THEN
Eine neue Servicerolle erstellen und verwenden	AWS Entity Resolution erstellt eine Servicerolle mit der erforderl ichen Richtlinie für diese Tabelle. Der Standardname für die Dienstrolle lautet`entityres olution-id-mapping-workflow-<timestamp>` . Sie müssen über die erforderl ichen 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 verschlüs

Wenn Sie wählen...	THEN
	selt. Geben Sie dann einen AWS KMS Schlüssel ein, der zum Entschlüsseln Ihrer Dateneingabe verwendet wird.
Verwenden Sie eine vorhandene Servicerolle	Wählen Sie einen vorhanden en Servicerollennamen aus der Dropdownliste aus. Wenn Sie berechtigt sind, Rollen aufzulisten, wird die Rollenliste angezeigt. 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. Versucht standardmäßig AWS Entity Resolution nicht, die bestehende Rollenrichtlinie zu aktualisieren, um die erforderl ichen Berechtigungen hinzuzufü gen.

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 der verbinden`TRANSCODED_ID`.

Verwaltung AWS Entity Resolution

In den folgenden Themen wird erklärt, wie Workflows mithilfe der AWS Entity Resolution Konsole verwaltet werden.

Informationen zur Verwaltung AWS Entity Resolution mithilfe der AWS SDKs finden Sie in der AWS Entity Resolution API-Referenz.

Themen

Schemazuordnungen verwalten

In den folgenden Themen wird erklärt, wie Schemazuordnungen mithilfe der Konsole verwaltet werden. AWS Entity Resolution

Themen

Klonen Sie eine Schemazuordnung

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

So klonen Sie ein Schema-Mapping:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.

2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie die Schemazuordnung aus.
4. Klicken auf Clone.
5. Nehmen Sie auf der Seite Schemadetails angeben die erforderlichen Änderungen vor und wählen Sie dann Weiter.
6. Nehmen Sie auf der Seite Passende Technik auswählen die erforderlichen Änderungen vor und klicken Sie dann auf Weiter.
7. Nehmen Sie auf der Seite Map-Eingabefelder alle erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
8. Nehmen Sie auf der Seite Gruppendaten die erforderlichen Änderungen vor und wählen Sie dann Weiter.
9. Nehmen Sie auf der Seite Überprüfen und speichern die erforderlichen Änderungen vor und wählen Sie dann Schema-Mapping klonen aus.

Bearbeiten Sie eine Schemazuordnung

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 bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie die Schemazuordnung aus.
4. Wählen Sie Bearbeiten aus.
5. Nehmen Sie auf der Seite Schemadetails angeben die erforderlichen Änderungen vor und wählen Sie dann Weiter.
6. Nehmen Sie auf der Seite Passende Technik auswählen die erforderlichen Änderungen vor und klicken Sie dann auf Weiter.

7. Nehmen Sie auf der Seite Map-Eingabefelder alle erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
8. Nehmen Sie auf der Seite Gruppendaten die erforderlichen Änderungen vor und wählen Sie dann Weiter.
9. Nehmen Sie auf der Seite Überprüfen und speichern die erforderlichen Änderungen vor und wählen Sie dann Schemazuordnung bearbeiten aus.

Löschen Sie eine Schemazuordnung

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

Um eine Schemazuordnung zu löschen:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Datenvorbereitung die Option Schemazuordnungen aus.
3. Wählen Sie die Schemazuordnung aus.
4. Wählen Sie Löschen aus.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Verwaltung passender Workflows

Nachdem Sie einen regelbasierten Abgleichsworkflow, einen auf maschinellem Lernen basierenden Abgleich oder einen auf Anbieterdiensten basierenden Abgleichsworkflow erstellt haben, können Sie Abgleichs-Workflows auf folgende Weise verwalten.

Themen

Bearbeiten Sie einen Abgleichsworkflow

Um einen passenden Workflow zu bearbeiten:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
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.

Löschen Sie einen passenden Workflow

Um einen passenden Workflow zu löschen:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
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.

Suchen Sie eine Match-ID für einen regelbasierten Abgleichs-Workflow

Nachdem Sie einen regelbasierten Abgleichsworkflow 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 bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option Matching aus.
3. Wählen Sie den regelbasierten Abgleichs-Workflow, 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 Sie Datensätze aus einem regelbasierten oder ML-basierten Abgleichs-Workflow

Wenn Sie die 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 bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
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 Eindeutige IDs löschen aus.
5. Geben Sie die eindeutige ID, die Sie löschen möchten, im Abschnitt Eindeutige IDs ein.

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

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

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

ID-Namespaces verwalten

Sie können ID-Namespaces auf folgende Weise verwalten.

Themen

- Bearbeiten Sie einen ID-Namespace
- Löschen Sie einen ID-Namespace
- Fügen Sie eine Ressourcenrichtlinie hinzu oder aktualisieren Sie sie

Bearbeiten Sie einen ID-Namespace

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

So bearbeiten Sie einen ID-Namespace:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem 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 Bearbeiten aus.
5. Nehmen Sie auf der Seite ID-Namespace bearbeiten die erforderlichen Änderungen vor und wählen Sie dann Speichern.

Löschen Sie einen ID-Namespace

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

Um einen ID-Namespace zu löschen:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem 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 aus.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Fügen Sie eine Ressourcenrichtlinie hinzu oder aktualisieren Sie sie

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

Um eine Ressourcenrichtlinie hinzuzufügen oder zu aktualisieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Namespaces aus.
3. Wählen Sie den ID-Namespace aus.
4. Wählen Sie auf der Seite mit den ID-Namespace-Details die Registerkarte Berechtigungen aus.
5. Wählen Sie im Abschnitt Ressourcenrichtlinie die Option Bearbeiten aus.
6. Fügen Sie die Richtlinie im JSON-Editor hinzu oder aktualisieren Sie sie.
7. Wählen Sie Änderungen speichern aus.

Verwaltung von Workflows zur ID-Zuordnung

Sie können Workflows zur ID-Zuordnung auf folgende Weise verwalten.

Themen

Bearbeiten Sie einen Workflow für die ID-Zuordnung

So bearbeiten Sie einen Workflow für die ID-Zuordnung:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den Workflow für die ID-Zuordnung aus.
4. Wählen Sie auf der Detailseite des ID-Mapping-Workflows in der oberen rechten Ecke die Option Bearbeiten aus.

5. Nehmen Sie auf der Seite mit den Details zum Workflow „ID-Zuordnung angeben“ alle erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
6. Nehmen Sie auf der Seite „Datenausgabe angeben“ die erforderlichen Änderungen vor und wählen Sie dann Weiter aus.
7. Nehmen Sie auf der Seite Überprüfen und speichern die erforderlichen Änderungen vor und wählen Sie dann Speichern aus.

Löschen Sie einen Workflow für die ID-Zuordnung

So löschen Sie einen Workflow für die ID-Zuordnung:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den Workflow für die ID-Zuordnung aus.
4. Wählen Sie auf der Detailseite des ID-Mapping-Workflows in der oberen rechten Ecke die Option Löschen aus.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Fügen Sie eine Ressourcenrichtlinie hinzu oder aktualisieren Sie sie

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

Um eine Ressourcenrichtlinie hinzuzufügen oder zu aktualisieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Entity Resolution Konsole mit Ihrem AWS-Konto, falls Sie dies noch nicht getan haben.
2. Wählen Sie im linken Navigationsbereich unter Workflows die Option ID-Zuordnung aus.
3. Wählen Sie den Workflow für die ID-Zuordnung aus.
4. Wählen Sie auf der Detailseite des Workflows für die ID-Zuordnung die Registerkarte Berechtigungen aus.
5. Wählen Sie im Abschnitt Ressourcenrichtlinie die Option Bearbeiten aus.
6. Fügen Sie die Richtlinie im JSON-Editor hinzu oder aktualisieren Sie sie.

7. Wählen Sie Änderungen speichern aus.

Workflows zur Fehlerbehebung

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die beim Ausführen von Workflows auftreten können.

Ich habe eine Fehlerdatei erhalten.

Die Datensätze in der Fehlerdatei können 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
- Eines der Felder in der Schemazuordnung enthält einen reservierten Namen:
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - ID abgleichen
  - HashingProtocol
  - ConfidenceLevel
  - Quelle

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.

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 Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Entity Resolution. Wie in diesem Modell beschrieben, AWS ist verantwortlich

für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API AWS Entity Resolution oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung im Ruhezustand für AWS Entity Resolution

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

AWS-eigene Schlüssel — AWS Entity Resolution verwendet diese Schlüssel standardmäßig, um persönlich identifizierbare Daten automatisch zu verschlüsseln. Sie können AWS eigene Schlüssel nicht einsehen, verwalten oder verwenden oder deren Verwendung überprüfen. Sie müssen jedoch keine Maßnahmen ergreifen, um die Schlüssel zu schützen, mit denen Ihre Daten verschlüsselt werden. Weitere Informationen finden Sie unter AWS-eigene Schlüssel im AWS Key Management Service Entwicklerhandbuch.

Die standardmäßige Verschlüsselung von Daten im Ruhezustand trägt dazu bei, den betrieblichen Aufwand und die Komplexität zu reduzieren, die mit dem Schutz vertraulicher Daten verbunden sind. Gleichzeitig können Sie damit sichere Anwendungen erstellen, die strenge Verschlüsselungsvorschriften und regulatorische Anforderungen erfüllen.

Alternativ können Sie auch einen vom Kunden verwalteten KMS-Schlüssel für die Verschlüsselung angeben, wenn Sie Ihre passende Workflow-Ressource erstellen.

Vom Kunden verwaltete Schlüssel — AWS Entity Resolution unterstützt die Verwendung eines symmetrischen, vom Kunden verwalteten KMS-Schlüssels, den Sie selbst erstellen, besitzen und verwalten, um die Verschlüsselung Ihrer vertraulichen Daten zu ermöglichen. Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie beispielsweise folgende Aufgaben ausführen:

- Festlegung und Pflege wichtiger Richtlinien
- Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
- Aktivieren und Deaktivieren wichtiger Richtlinien
- Kryptographisches Material mit rotierendem Schlüssel
- Hinzufügen von Tags
- Erstellen von Schlüsselaliasen
- Schlüssel für das Löschen von Schlüsseln planen

Weitere Informationen finden Sie unter vom Kunden verwalteter Schlüssel im AWS Key Management Service Entwicklerhandbuch.

Weitere Informationen AWS KMS dazu finden Sie unter Was ist AWS Key Management Service?

Schlüsselverwaltung

Wie AWS Entity Resolution verwendet man Zuschüsse in AWS KMS

AWS Entity Resolution erfordert einen Zuschuss, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können. Wenn Sie einen passenden Workflow erstellen, der mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, AWS Entity Resolution erstellt in Ihrem Namen einen Zuschuss, indem es eine CreateGrantAnfrage an sendet AWS KMS. Grants in AWS KMS werden verwendet, um AWS Entity Resolution Zugriff auf einen KMS-Schlüssel in einem Kundenkonto zu gewähren. AWS Entity Resolution setzt voraus, dass der Zuschuss Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwendet:

- Senden Sie GenerateDataKeyAnfragen AWS KMS zur Generierung von Datenschlüsseln, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt sind.
- Senden Sie Entschlüsselungsanfragen an AWS KMS , um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie zur Verschlüsselung Ihrer Daten verwendet werden können.

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn Sie dies tun, können Sie auf AWS Entity Resolution keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise den Dienstzugriff auf Ihren Schlüssel durch die Gewährung entfernen und versuchen, einen Job für einen passenden Workflow zu starten, der mit einem Kundenschlüssel verschlüsselt ist, würde der Vorgang einen `AccessDeniedException` Fehler zurückgeben.

Einen vom Kunden verwalteten Schlüssel erstellen

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel mithilfe der AWS Management Console AWS KMS APIs oder erstellen.

Einen symmetrischen kundenverwalteten Schlüssel erstellen

AWS Entity Resolution unterstützt die Verschlüsselung mit symmetrischen KMS-Schlüsseln. Folgen Sie den Schritten zum Erstellen eines symmetrischen kundenverwalteten Schlüssels im Entwicklerhandbuch zum AWS Key Management Service .

Wichtige Richtlinienerklärung

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Verwaltung des Zugriffs auf vom Kunden verwaltete Schlüssel im AWS Key Management Service Entwicklerhandbuch.

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

- `kms:DescribeKey`— Stellt Informationen wie den Schlüssel-ARN, das Erstellungsdatum (und gegebenenfalls das Löschdatum), den Schlüsselstatus sowie das Herkunfts- und Ablaufdatum (falls vorhanden) des Schlüsselmaterials bereit. Es enthält Felder wie, die Ihnen helfen`KeySpec`, verschiedene Arten von KMS-Schlüsseln zu unterscheiden. Außerdem werden die Schlüsselverwendung (Verschlüsselung, Signierung oder Generierung und Überprüfung von MACs) und die Algorithmen angezeigt, die der KMS-Schlüssel unterstützt. AWS Entity Resolution bestätigt, dass das `KeySpec` ist und ist`SYMMETRIC_DEFAULT`. `KeyUsage` `ENCRYPT_DECRYPT`
- `kms:CreateGrant`: Fügt einem kundenverwalteten Schlüssel eine Erteilung hinzu. Gewährt Kontrollzugriff auf einen bestimmten KMS-Schlüssel, der den Zugriff für Grant-Operationen AWS Entity Resolution erfordert. Weitere Informationen zur Verwendung von Grants finden Sie im AWS Key Management Service Developer Guide.

Auf diese Weise können AWS Entity Resolution Sie Folgendes tun:

- `GenerateDataKey` aufrufen, um einen verschlüsselten Datenschlüssel zu generieren und zu speichern, da der Datenschlüssel nicht sofort zum Verschlüsseln verwendet wird.
- `Decrypt` aufrufen, um den gespeicherten verschlüsselten Datenschlüssel für den Zugriff auf verschlüsselte Daten zu verwenden.
- Richten Sie einen Principal ein, der in den Ruhestand geht, damit der Dienst dies tun `RetireGrant` kann.

Im Folgenden finden Sie Beispiele für Richtlinienerklärungen, für AWS Entity Resolution die Sie Folgendes hinzufügen können:

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

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

Berechtigungen für Benutzer

Wenn Sie einen KMS-Schlüssel als Standardschlüssel für die Verschlüsselung konfigurieren, ermöglicht die standardmäßige KMS-Schlüsselrichtlinie jedem Benutzer mit Zugriff auf die erforderlichen KMS-Aktionen, diesen KMS-Schlüssel zum Verschlüsseln oder Entschlüsseln von Ressourcen zu verwenden. Sie müssen Benutzern die Erlaubnis erteilen, die folgenden Aktionen aufzurufen, um die vom Kunden verwaltete KMS-Schlüsselverschlüsselung verwenden zu können:

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

Während einer `CreateMatchingWorkflow`Anfrage AWS Entity Resolution sendet ich in Ihrem Namen eine CreateGrantAnfrage DescribeKeyund eine Anfrage AWS KMS an. Dies setzt voraus, dass die IAM-Entität, die die `CreateMatchingWorkflow` Anfrage mit einem vom Kunden verwalteten KMS-Schlüssel stellt, über die `kms:DescribeKey` Berechtigungen für die KMS-Schlüsselrichtlinie verfügt.

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

Im Folgenden finden Sie Beispiele für Richtlinienerklärungen, die Sie für Anbieter hinzufügen können, um die Daten im AWS Entity Resolution Amazon S3 S3-Bucket zu entschlüsseln:

```
{
    "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 jede <user input placeholder>durch Ihre eigenen Informationen.

<KMSKeyARN>	AWS KMS Name der Amazon-Ressource.

Ebenso muss die IAM-Entität, die die `StartMatchingJob`API aufruft, über `kms:GenerateDataKey` Berechtigungen für den vom Kunden verwalteten KMS-Schlüssel verfügen`kms:Decrypt`, der im entsprechenden Workflow bereitgestellt wird.

Weitere Informationen zur Angabe von Berechtigungen in einer Richtlinie finden Sie im AWS Key Management Service Entwicklerhandbuch.

Weitere Informationen zur Problembehandlung beim Zugriff auf Schlüssel finden Sie im AWS Key Management Service Entwicklerhandbuch.

Angabe eines vom Kunden verwalteten Schlüssels für AWS Entity Resolution

Sie können einen vom Kunden verwalteten Schlüssel als zweite Verschlüsselungsebene für die folgenden Ressourcen festlegen:

Abgleichender Workflow — Wenn Sie eine passende Workflow-Ressource erstellen, können Sie den Datenschlüssel angeben, indem Sie einen KMSarn eingeben, der zur Verschlüsselung der von der Ressource gespeicherten identifizierbaren persönlichen Daten AWS Entity Resolution verwendet wird.

kmSARN — Geben Sie einen Schlüssel-ARN ein, der eine Schlüssel-ID für einen vom AWS KMS Kunden verwalteten Schlüssel ist.

Sie können einen vom Kunden verwalteten Schlüssel als zweite Verschlüsselungsebene für die folgenden Ressourcen angeben, wenn Sie einen ID-Zuordnungs-Workflow für zwei Ressourcen erstellen oder ausführen: AWS-Konten

ID-Zuordnungs-Workflow oder ID-Zuordnungs-Workflow starten — Wenn Sie eine Workflow-Ressource für die ID-Zuordnung erstellen oder einen Workflow-Job für die ID-Zuordnung starten, können Sie den Datenschlüssel angeben, indem Sie einen KMSarn eingeben, der zur Verschlüsselung der von der Ressource gespeicherten identifizierbaren personenbezogenen Daten AWS Entity Resolution verwendet wird.

kmSARN — Geben Sie einen Schlüssel-ARN ein, der eine Schlüssel-ID für einen vom AWS KMS Kunden verwalteten Schlüssel ist.

Überwachen Sie Ihre Verschlüsselungsschlüssel für den Service AWS Entity Resolution

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel mit Ihren AWS Entity Resolution Serviceressourcen verwenden, können Sie AWS CloudTrail oder Amazon CloudWatch Logs verwenden, um Anfragen zu verfolgen, die AWS Entity Resolution an gesendet AWS KMS werden.

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

Themen

- CreateGrant
- DescribeKey
- GenerateDataKey
- Decrypt

CreateGrant

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel verwenden, um Ihre passende Workflow-Ressource zu verschlüsseln, AWS Entity Resolution sendet in Ihrem Namen eine `CreateGrant` Anfrage für den Zugriff auf den KMS-Schlüssel in Ihrem AWS-Konto. Die gewährten Zuschüsse AWS Entity Resolution sind spezifisch für die Ressource, die dem vom AWS KMS Kunden verwalteten Schlüssel zugeordnet ist. AWS Entity Resolution Verwendet außerdem den `RetireGrant` Vorgang, um einen Zuschuss zu entfernen, wenn Sie eine Ressource löschen.

Das folgende Beispielereignis zeichnet den Vorgang `CreateGrant` auf:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "entityresolution.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
```

```
        "retiringPrincipal": "entityresolution.region.amazonaws.com",
        "operations": [
            "GenerateDataKey",
            "Decrypt",
        ],
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "granteePrincipal": "entityresolution.region.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

DescribeKey

AWS Entity Resolution verwendet den `DescribeKey` Vorgang, um zu überprüfen, ob der vom AWS KMS Kunden verwaltete Schlüssel, der Ihrer entsprechenden Ressource zugeordnet ist, im Konto und in der Region vorhanden ist.

Das folgende Beispielereignis zeichnet 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 einen vom AWS KMS Kunden verwalteten Schlüssel für Ihre passende Workflow-Ressource aktivieren, AWS Entity Resolution sendet eine `GenerateDataKey` Anfrage über Amazon Simple Storage Service (Amazon S3) an AWS KMS , in der der vom AWS KMS Kunden verwaltete Schlüssel für die Ressource angegeben ist.

Das folgende Beispielereignis zeichnet 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 einen vom AWS KMS Kunden verwalteten Schlüssel für Ihre passende Workflow-Ressource aktivieren, AWS Entity Resolution sendet eine `Decrypt` Anfrage über Amazon Simple Storage Service (Amazon S3) an AWS KMS , in der der vom AWS KMS Kunden verwaltete Schlüssel für die Ressource angegeben ist.

Das folgende Beispielereignis zeichnet 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 Developer Guide.

Weitere Informationen zu bewährten Sicherheitsmethoden für AWS Key Management Service finden Sie im AWS Key Management Service Developer Guide.

Zugriff AWS Entity Resolution über einen Schnittstellenendpunkt (AWS PrivateLink)

Sie können verwenden AWS PrivateLink , um eine private Verbindung zwischen Ihrer VPC und AWS Entity Resolution herzustellen. Sie können darauf zugreifen, AWS Entity Resolution als ob es in Ihrer VPC wäre, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung zu verwenden. Instances in Ihrer VPC benötigen für den Zugriff AWS Entity Resolution keine öffentlichen IP-Adressen.

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

Weitere Informationen finden Sie AWS PrivateLink im AWS PrivateLink Leitfaden unter Zugriff AWS-Services durch.

Überlegungen zu AWS Entity Resolution

Bevor Sie einen Schnittstellen-Endpunkt für einrichten AWS Entity Resolution, lesen Sie die Überlegungen im AWS PrivateLink Handbuch.

AWS Entity Resolution unterstützt Aufrufe aller API-Aktionen über den Schnittstellenendpunkt.

VPC-Endpunktrichtlinien werden für AWS Entity Resolution nicht unterstützt. Standardmäßig AWS Entity Resolution ist der vollständige Zugriff auf über den Schnittstellenendpunkt zulässig. Alternativ können Sie den Endpunkt-Netzwerkschnittstellen eine Sicherheitsgruppe zuordnen, um den Datenverkehr AWS Entity Resolution über den Schnittstellenendpunkt zu kontrollieren.

Erstellen Sie einen Schnittstellenendpunkt für AWS Entity Resolution

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

Erstellen Sie einen Schnittstellenendpunkt für die AWS Entity Resolution Verwendung des folgenden Servicenamens:

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

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

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-Endpunkt anfügen können. Die standardmäßige Endpunktrichtlinie ermöglicht den vollen Zugriff AWS Entity Resolution über den Schnittstellenendpunkt. Um den Zugriff zu kontrollieren, der AWS Entity Resolution von Ihrer VPC aus gewährt wird, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen).
- Aktionen, die ausgeführt werden können
- Die Ressourcen, auf denen die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Beispiel: VPC-Endpunktrichtlinie für Aktionen AWS Entity Resolution

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

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

Identitäts- und Zugriffsmanagement für AWS Entity Resolution

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Entity Resolution IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

> **Note**
>
> AWS Entity Resolution unterstützt kontoübergreifende Richtlinien. Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Art der Arbeit ab, in der Sie tätig sind. AWS Entity Resolution

Dienstbenutzer — Wenn Sie den AWS Entity Resolution Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS Entity Resolution Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Problembehandlung bei AWS Entity Resolution Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS Entity Resolution haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS Entity Resolution Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS Entity Resolution. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS Entity Resolution Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann AWS Entity Resolution, finden Sie unterWie AWS Entity Resolution funktioniert mit IAM.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS Entity Resolution verfassen können. Beispiele für AWS Entity Resolution identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Authentifizierung mit Identitäten

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

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

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, 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 Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, 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 unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

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

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. 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 Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges

Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe 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 einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten 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 Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- 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 unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, 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 -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch 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 unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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 IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie

ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, 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. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

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

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern,

welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

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 System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

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

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

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 ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen 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 über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (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 Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- 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 unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird,

ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS Entity Resolution funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren AWS Entity Resolution, mit welchen IAM-Funktionen Sie arbeiten können. AWS Entity Resolution

IAM-Funktionen, die Sie mit verwenden können AWS Entity Resolution

IAM-Feature	AWS Entity Resolution Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie AWS Entity Resolution und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für AWS Entity Resolution

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

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

Ressourcenbasierte Richtlinien finden Sie in AWS Entity Resolution

Unterstützt ressourcenbasierte Richtlinien	Ja

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. 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 Berechtigung zum Zugriff auf die Ressource erteilen. 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 unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für AWS Entity Resolution

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. 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.

Eine Liste der AWS Entity Resolution Aktionen finden Sie unter Definierte Aktionen von AWS Entity Resolution in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Entity Resolution verwendet:

```
entityresolution
```

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

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

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

Politische Ressourcen für AWS Entity Resolution

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. 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": "*"
```

Eine Liste der AWS Entity Resolution Ressourcentypen und ihrer ARNs finden Sie unter Resources Defined by AWS Entity Resolution in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Entity Resolution definierte Aktionen.

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

Bedingungsschlüssel für Richtlinien für AWS Entity Resolution

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff 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, wertet AWS diese mittels 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. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der AWS Entity Resolution Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Entity Resolution in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Definierte Aktionen von AWS Entity Resolution.

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

ACLs in AWS Entity Resolution

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS Entity Resolution

Unterstützt ABAC (Tags in Richtlinien)	Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam 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 ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS Entity Resolution

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

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

Zugriffssitzungen weiterleiten für AWS Entity Resolution

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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 IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS Entity Resolution Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, AWS Entity Resolution wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für AWS Entity Resolution

Unterstützt serviceverknüpfte Rollen	Nein

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS Entity Resolution

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS Entity Resolution -Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden AWS Entity Resolution, einschließlich des Formats der ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Entity Resolution in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden 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 AWS Entity Resolution Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie

können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der AWS Entity Resolution -Konsole

Um auf die AWS Entity Resolution Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Entity Resolution Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS Entity Resolution Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS Entity Resolution `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI AWS OR-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinien für AWS Entity Resolution

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie 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

Problembehandlung bei AWS Entity Resolution Identität und Zugriff

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

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Entity Resolution
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Entity Resolution Ressourcen ermöglichen

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

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `entityresolution:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `entityresolution:`*`GetWidget`* zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Entity Resolutionübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Entity Resolution auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Entity Resolution Ressourcen ermöglichen

Sie können eine Rolle erstellen, 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. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS Entity Resolution unterstützt werden, finden Sie unterWie AWS Entity Resolution funktioniert mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Kontenübergreifender Ressourcenzugriff in 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 Implementierung 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 HIPAA-fähige Anwendungen erstellen AWS können.

> **Note**
>
> AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- 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 den 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)) zugeordnet.
- 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 wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.

- 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.

Ausfallsicherheit in AWS Entity Resolution

Die globale AWS-Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz 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 über AWS-Regionen und Availability Zones finden Sie unter AWSGlobale Infrastruktur.

Zusätzlich zur globalen AWS-Infrastruktur stellt AWS Entity Resolution verschiedene Funktionen bereit, um Ihren Anforderungen in Bezug auf Ausfallsicherheit und Datensicherung zu erfüllen.

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.

Erstellen von AWS Entity Resolution-Ressourcen mit AWS CloudFormation

AWS Entity Resolution ist in einen Service integriert AWS CloudFormation, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt (z. B. AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace und AWS::EntityResolution::PolicyStatement) und diese Ressourcen für Sie 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.

AWS-Entitätsauflösung und AWS CloudFormation Vorlagen

Um Ressourcen für AWS Entity Resolution und verwandte Services bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation Vorlagen verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie AWS CloudFormation Designer verwenden, um Ihnen die ersten Schritte mit Vorlagen zu erleichtern. AWS CloudFormation Weitere Informationen finden Sie unter Was ist AWS CloudFormation -Designer? im AWS CloudFormation -Benutzerhandbuch.

AWS Entity Resolution unterstützt das Erstellen AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace und AWS::EntityResolution::PolicyStatement Eingeben AWS CloudFormation. Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace und AWS::EntityResolution::PolicyStatement, finden Sie in der AWS-Referenz zum Ressourcentyp „AWS Entity Resolution“ im AWS CloudFormation Benutzerhandbuch.

Die folgenden Vorlagen sind verfügbar:

- Passender Arbeitsablauf

  Erstellen Sie ein `MatchingWorkflow` Objekt, das die Konfiguration des auszuführenden Datenverarbeitungsjobs speichert.

  Weitere Informationen finden Sie unter den folgenden Themen:

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

  CreateMatchingWorkflow in der AWS Entity Resolution -API-Referenz

- Schemazuordnung

  Erstellen Sie eine Schemazuordnung, die das Schema der Eingabetabelle mit Kundendatensätzen definiert.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::EntityResolution::SchemaMapping im AWS CloudFormation -Benutzerhandbuch

  CreateSchemaMapping in der AWS Entity Resolution -API-Referenz

- Arbeitsablauf für die ID-Zuordnung

  Erstellen Sie ein `IdMappingWorkflow` Objekt, das die Konfiguration des auszuführenden Datenverarbeitungsauftrags speichert.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::EntityResolution::IdMappingWorkflow im AWS CloudFormation -Benutzerhandbuch

  CreateIdMappingWorkflow in der AWS Entity Resolution -API-Referenz

- ID-Namespace

  Erstellen Sie ein `IdNamespace` Objekt, das die Metadaten speichert, in denen der Datensatz und seine Verwendung erklärt werden.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::EntityResolution::IdNamespace im AWS CloudFormation -Benutzerhandbuch

  CreateIdNamespace in der AWS Entity Resolution -API-Referenz

- PolicyStatement

Erstellen Sie ein `PolicyStatement`-Objekt.

Weitere Informationen finden Sie unter den folgenden Themen:

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

AddPolicyStatement in der AWS Entity Resolution -API-Referenz

Erfahren Sie mehr über AWS CloudFormation

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

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- AWS CloudFormation API Referenz
- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Kontingente für AWS Entity Resolution

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden 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.

Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie den RSS-Feed abonnieren. Um RSS-Updates abonnieren zu können, muss für den von Ihnen verwendeten Browser ein RSS-Plug-In aktiviert sein.

Änderung	Beschreibung	Datum
Passender Workflow — 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
CloudFormation AWS-Ressourcen — Neue und aktualisierte Ressourcen	AWS Entity Resolution hat die folgenden Ressourcen hinzugefügt: `AWS::EntityResolution::IdNamespace` `AWS::EntityResolution::PolicyStatement` und die folgende Ressource aktualisiert:`AWS::EntityResolution::IdMappingWorkflow` .	2. April 2024

Finde die Match-ID	Kunden können jetzt die entsprechende Match-ID und die zugehörige Regel für einen verarbeiteten regelbasierten Workflow finden.	25. März 2024
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 PrivateLink , 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. ARNs sind erforderlich, wenn Sie eine Ressource in allen Bereichen eindeutig angeben müssen AWS Entity Resolution, z. B. in AWS Entity Resolution Richtlinien, Amazon Relational Database Service (Amazon RDS) -Tags und API-Aufrufen.

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 Datenwerte in Ihrer Ausgabe als Hashwert verwendet werden sollen.

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.

Arbeitsablauf für die ID-Zuordnung

Der Prozess, den Sie eingerichtet haben, um die Eingabedaten für die Übersetzung Ihrer IDs anzugeben und anzugeben, wie die ID-Zuordnung durchgeführt werden soll.

AWS Entity Resolution wird derzeit LiveRamp als ID-Mapping-Methode unterstützt. Sie müssen über ein Abonnement für LiveRamp bis verfügen, AWS Data Exchange um den ID-Zuordnungs-Workflow verwenden zu können.

Weitere Informationen finden Sie unter Abonnieren Sie einen Anbieter-Service auf AWS Data Exchange.

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.

Eingangsquelle 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 Name, der einem Match Key zugewiesen wurde.

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

- 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 Zeichen [a-zA-Z0-9] und [.@-] non-alpha-numeric

Phone

- TRIM = Kürzt führende und nachfolgende Leerzeichen
- 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]
- RAME_WORDS mit ADDRESS_RAME_WORD_MAP = Ersetze Wörter in der Adresszeichenfolge durch Wörter aus ADDRESS_RAME_WORD_MAP
- RAME_DELIMITERS mit ADDRESS_RAME_DELIMITER_MAP = ersetzt Trennzeichen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_RAME_DELIMITER_MAP
- RAME_DIRECTIONS mit ADDRESS_RAME_DIRECTION_MAP = ersetzt Trennzeichen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_RAME_DIRECTION_MAP
- RAME_NUMBERS mit ADDRESS_RAME_NUMBER_MAP = Ersetze Zahlen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_RAME_NUMBER_MAP
- RAME_SPECIAL_CHARS mit ADDRESS_RAME_SPECIAL_CHAR_MAP = ersetzt Sonderzeichen in der Adresszeichenfolge durch eine Zeichenfolge aus ADDRESS_RAME_SPECIAL_CHAR_MAP

ADDRESS_RENAME_WORD_MAP

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

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

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

ADDRESS_RENAME_DELIMITER_MAP

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

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

ADDRESS_RENAME_DIRECTION_MAP

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

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

ADDRESS_RENAME_NUMBER_MAP

Dies sind die 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, UND. `Record One mobile_phone = Record Two mobile_phone` `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
- UID 2.0

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.

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.