aws

Panduan Pengguna

Resolusi Entitas AWS

Resolusi Entitas AWS: Panduan Pengguna

Table of Contents

Apa itu Resolusi Entitas AWS?

Resolusi Entitas AWS adalah layanan yang membantu Anda mencocokkan, menautkan, dan meningkatkan catatan terkait yang disimpan di beberapa aplikasi, saluran, dan penyimpanan data. Anda dapat mulai menggunakan alur kerja resolusi entitas yang fleksibel, dapat diskalakan, dan dapat terhubung ke aplikasi dan penyedia layanan data yang ada.

Resolusi Entitas AWS menawarkan teknik pencocokan tingkat lanjut, seperti pencocokan berbasis aturan, pencocokan berbasis pembelajaran mesin (pencocokan ML), dan pencocokan yang dipimpin oleh penyedia layanan data. Teknik-teknik ini dapat membantu Anda lebih akurat menghubungkan dan meningkatkan catatan terkait informasi pelanggan, kode produk, atau kode data bisnis.

Anda dapat menggunakan Resolusi Entitas AWS untuk membuat tampilan terpadu interaksi pelanggan dengan menautkan peristiwa terbaru (seperti klik iklan, pengabaian keranjang, dan pembelian) dengan sinyal pseudonim dari penyedia layanan data Anda ke ID entitas unik. Anda juga dapat melacak produk dengan lebih baik yang menggunakan kode berbeda (misalnya,SKU,UPC) di seluruh toko Anda. Anda dapat menggunakan Resolusi Entitas AWS untuk mengontrol akurasi pencocokan dan melindungi keamanan data dengan lebih baik sambil meminimalkan pergerakan data.

Topik

Apakah Anda Resolusi Entitas AWS pengguna pertama kali?

Jika Anda adalah pengguna pertama kali Resolusi Entitas AWS, kami sarankan Anda mulai dengan membaca bagian berikut:

Fitur dari Resolusi Entitas AWS

Resolusi Entitas AWS termasuk fitur-fitur berikut:

- Persiapan data yang fleksibel dan dapat disesuaikan

  Resolusi Entitas AWS membaca data Anda dari AWS Glue untuk digunakan sebagai input untuk pemrosesan kecocokan. Anda dapat menentukan maksimum 20 input data. Resolusi Entitas AWS memproses setiap baris tabel input data sebagai catatan, dengan entitas unik yang berfungsi sebagai kunci utama. Resolusi Entitas AWS dapat beroperasi pada dataset terenkripsi. Pertama-tama tentukan pemetaan skema Resolusi Entitas AWS untuk memahami bidang input apa yang ingin Anda gunakan dalam alur kerja yang cocok. Anda dapat membawa skema data Anda sendiri, atau cetak biru, dari input data yang ada. AWS Glue Atau, Anda dapat membangun skema kustom Anda menggunakan antarmuka pengguna interaktif atau JSON editor. Secara default, Resolusi Entitas AWS juga menormalkan input data sebelum pencocokan untuk meningkatkan pemrosesan kecocokan, seperti menghapus karakter khusus dan spasi tambahan, dan memformat teks ke huruf kecil. Jika input data Anda sudah dinormalisasi, maka Anda dapat mematikan normalisasi. Kami juga menyediakan GitHub perpustakaan, yang dapat Anda gunakan untuk lebih menyesuaikan proses normalisasi data agar sesuai dengan kebutuhan Anda.
- Alur kerja pencocokan entitas yang dapat dikonfigurasi

  Alur kerja pencocokan entitas adalah urutan langkah yang Anda atur untuk memberi tahu Resolusi Entitas AWS cara mencocokkan input data Anda dan tempat menulis output data konsolidasi. Anda dapat menyiapkan satu atau beberapa alur kerja yang cocok untuk membandingkan input data yang berbeda dan menggunakan teknik pencocokan yang berbeda, seperti pencocokan berbasis aturan, pencocokan pembelajaran mesin, atau pencocokan yang dipimpin oleh penyedia layanan data tanpa resolusi entitas atau pengalaman ML. Anda juga dapat melihat status pekerjaan alur kerja dan metrik pencocokan yang ada, seperti nomor sumber daya, jumlah rekaman yang diproses, dan jumlah kecocokan yang ditemukan.

  - Pencocokan eady-to-use berbasis aturan R

    Teknik pencocokan ini mencakup seperangkat ready-to-use aturan dalam AWS Management Console or AWS Command Line Interface (AWS CLI). Anda dapat menggunakan aturan ini untuk menemukan catatan terkait berdasarkan bidang masukan Anda. Anda juga dapat menyesuaikan aturan dengan menambahkan atau menghapus kolom input untuk setiap aturan, menghapus aturan, mengatur ulang prioritas aturan, dan membuat aturan baru. Anda juga dapat mengatur ulang aturan untuk mengembalikannya ke konfigurasi aslinya. Output data di bucket

Amazon Simple Storage Service (Amazon S3) memiliki grup pencocokan Resolusi Entitas AWS yang dihasilkan menggunakan teknik pencocokan berbasis aturan. Setiap grup pertandingan memiliki nomor aturan yang digunakan untuk menghasilkan kecocokan yang terkait dengannya untuk membantu Anda memahami pertandingan. Misalnya, nomor aturan dapat menunjukkan ketepatan setiap grup pertandingan sehingga aturan satu lebih tepat daripada aturan dua.

- Pencocokan berbasis pembelajaran mesin yang telah dikonfigurasi sebelumnya (pencocokan ML)

  Teknik pencocokan ini mencakup model ML yang telah dikonfigurasi sebelumnya untuk menemukan kecocokan di semua input data Anda, terutama catatan berbasis konsumen. Model ini menggunakan semua bidang input yang terkait dengan nama, alamat email, nomor telepon, alamat, dan tipe data tanggal lahir. Model ini menghasilkan grup pertandingan dari catatan terkait dengan skor kepercayaan di setiap grup yang menjelaskan kualitas pertandingan relatif terhadap grup pertandingan lainnya. Model mempertimbangkan bidang input yang hilang dan menganalisis seluruh catatan bersama-sama untuk mewakili suatu entitas. Output data di bucket Amazon S3 Anda memiliki grup pencocokan yang Resolusi Entitas AWS dihasilkan menggunakan pencocokan ML. Di sinilah setiap grup pertandingan memiliki skor kepercayaan terkait 0,0—1,0, yang menunjukkan ketepatan pertandingan.

- Mencocokkan catatan dengan penyedia layanan data

  Dengan Resolusi Entitas AWS Anda dapat mencocokkan, menautkan, dan meningkatkan catatan Anda dengan vendor layanan data terkemuka dan kumpulan data berlisensi untuk memperluas kemampuan Anda memahami, menjangkau, dan melayani pelanggan Anda. Misalnya, Anda dapat menambahkan atribut ke data Anda untuk meningkatkan catatan Anda, atau Anda dapat meningkatkan interoperabilitas sistem dan platform tempat Anda bekerja untuk memenuhi tujuan bisnis Anda. Anda dapat menggunakan alur kerja yang cocok ini dengan beberapa klik, menghilangkan kebutuhan untuk membangun dan memelihara integrasi kepemilikan yang kompleks. Anda harus memiliki perjanjian lisensi dengan penyedia layanan data ini untuk memanfaatkan teknik pencocokan ini.

- Pemrosesan massal manual dan pemrosesan inkremental otomatis

  Anda dapat menggunakan pemrosesan data untuk membantu mengonversi input atau input data Anda menjadi tabel keluaran data terkonsolidasi dengan catatan serupa yang memiliki ID kecocokan umum yang dihasilkan menggunakan konfigurasi alur kerja pencocokan entitas. Dengan menggunakan API dan AWS Management Console atau AWS CLI, Anda dapat menjalankan pemrosesan massal manual sesuai permintaan, berdasarkan pipeline data ekstrak, transformasi, dan beban (ETL) yang ada, yang memproses ulang semua data untuk setiap

kecocokan dan pembaruan baru ke kecocokan yang ada. Selain itu, untuk skenario pencocokan berbasis aturan, Anda dapat memulai pemrosesan inkremental otomatis sehingga segera setelah data baru tersedia di bucket Amazon S3, layanan akan membaca catatan baru tersebut dan membandingkannya dengan catatan yang ada. Ini membuat kecocokan Anda tetap up to date dengan setiap perubahan dalam data Amazon S3.

- Dekat pencarian waktu nyata

  Mencari bidang entitas apa pun melalui Resolusi Entitas AWS GetMatchId APIoperasi membantu Anda mengambil ID kecocokan yang ada secara sinkron. Anda dapat menelepon Resolusi Entitas AWS dengan atribut informasi yang dapat diidentifikasi secara pribadi (PII) yang diperoleh melalui berbagai sumber dan saluran. Resolusi Entitas AWS hash atribut tersebut untuk perlindungan data dan mengambil ID kecocokan yang sesuai untuk menautkan dan mencocokkan pelanggan. Misalnya, Anda bisa mendapatkan pendaftaran web dengan nama, email, dan alamat surat terkait. Gunakan Resolusi Entitas AWS GetMatchId API operasi untuk mengetahui apakah pelanggan atau entitas ini sudah ada di hasil yang cocok yang disimpan di bucket S3, bersama dengan ID pencocokan entitas terkait yang terkait dengannya. Setelah mendapatkan ID pencocokan entitas, Anda dapat menemukan informasi transaksional yang terkait dengannya di aplikasi sumber Anda, seperti sistem manajemen hubungan pelanggan (CRM) atau platform data pelanggan (CDP) Anda.

- Perlindungan data dan Regionalisasi berdasarkan desain

  Resolusi Entitas AWS menawarkan kemampuan enkripsi default yang dapat membantu Anda melindungi data Anda, dan melengkapi Anda dengan kunci enkripsi untuk setiap input data ke dalam layanan. Misalnya, Resolusi Entitas AWS memberi Anda fleksibilitas untuk membawa data terenkripsi dan hash sisi server untuk menjalankan alur kerja pencocokan berbasis aturan. Resolusi Entitas AWS mendukung Regionalisasi, yang berarti alur kerja Anda yang cocok berjalan untuk memproses data Anda di tempat yang sama Wilayah AWS dari tempat Anda menggunakan layanan. Anda juga dapat mengenkripsi dan hash output data di Amazon S3 sebelum menggunakan data yang diselesaikan di aplikasi lain.

- Transcoding multi-pihak

  Resolusi Entitas AWS membantu Anda menentukan sumber data dan mencocokkan konfigurasi antara beberapa pihak yang ingin menggunakan kolaborasi data, seperti di AWS Clean Rooms.

Layanan terkait

Layanan AWS Berikut ini terkait dengan Resolusi Entitas AWS:

- Amazon S3

  Simpan data yang Anda bawa Resolusi Entitas AWS di Amazon S3.

  Untuk informasi selengkapnya, lihat Apa itu Amazon S3? di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

- AWS Glue

  Buat AWS Glue tabel dari data Anda di Amazon S3 untuk digunakan di. Resolusi Entitas AWS

  Untuk informasi lebih lanjut, lihat Apa itu AWS Glue? di Panduan AWS Glue Pengembang.

- AWS CloudTrail

  Gunakan Resolusi Entitas AWS dengan CloudTrail log untuk meningkatkan analisis Layanan AWS aktivitas Anda.

  Untuk informasi selengkapnya, lihat Logging panggilan Resolusi Entitas AWS API menggunakan AWS CloudTrail.

- AWS CloudFormation

  Buat sumber daya berikut di AWS CloudFormation: AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace dan AWS::EntityResolution::PolicyStatement

  Untuk informasi selengkapnya, lihat Buat sumber daya Resolusi AWS Entitas dengan AWS CloudFormation.

Mengakses Resolusi Entitas AWS

Anda dapat mengakses Resolusi Entitas AWS melalui opsi berikut:

- Langsung melalui Resolusi Entitas AWS konsol di https://console.aws.amazon.com/entityresolution/.
- Secara terprogram melalui. Resolusi Entitas AWS API Untuk informasi selengkapnya, lihat Resolusi Entitas AWS APIReferensi.
  - Jika Anda berencana untuk memanggil Resolusi Entitas AWS API in AWS Lambda Runtime, buat paket penyebaran Anda sendiri dan sertakan versi perpustakaan yang diinginkan. AWS SDK Untuk informasi selengkapnya, lihat contoh berikut di Panduan AWS Lambda Pengembang:

- Menyebarkan fungsi Java Lambda JAR dengan.zip atau arsip file
- Bekerja dengan arsip file.zip untuk fungsi Python Lambda

Harga untuk Resolusi Entitas AWS

Untuk informasi harga, lihat Harga Resolusi Entitas AWS.

Mengatur Resolusi Entitas AWS

Sebelum Anda menggunakan Resolusi Entitas AWS untuk pertama kalinya, daftar AWS dan buat pengguna administrator untuk membuat peran.

Mendaftar untuk AWS

Jika Anda sudah memiliki Akun AWS, lewati langkah ini.

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

Membuat pengguna administrator

Untuk membuat pengguna administrator, pilih salah satu opsi berikut.

Pilih salah satu cara untuk mengelola administrator Anda	Untuk	Oleh	Anda juga bisa
Di Pusat IAM Identitas (Direkomendasikan)	Gunakan kredensi jangka pendek untuk mengakses. AWS Ini sejalan dengan praktik terbaik keamanan. Untuk informasi tentang praktik terbaik, lihat Praktik terbaik keamanan IAM di Panduan IAM Pengguna.	Mengikuti petunjuk di Memulai di Panduan AWS IAM Identity Center Pengguna.	Konfigurasikan akses terprogram dengan Mengonfigurasi AWS CLI yang akan digunakan AWS IAM Identity Center dalam AWS Command Line Interface Panduan Pengguna.
Di IAM (Tidak direkomendasikan)	Gunakan kredensi jangka panjang untuk mengakses. AWS	Mengikuti petunjuk di Buat IAM pengguna untuk akses darurat di Panduan IAM Pengguna.	Konfigurasikan akses terprogram dengan Mengelola kunci akses untuk IAM pengguna di Panduan IAM Pengguna.

Membuat IAM peran untuk pengguna konsol

Selesaikan prosedur berikut jika Anda menggunakan Resolusi Entitas AWS konsol.

Untuk membuat IAM peran

1. Masuk ke IAM konsol (https://console.aws.amazon.com/iam/) dengan akun administrator Anda.

2. Di bawah Manajemen akses, pilih Peran.

   Anda dapat menggunakan Peran untuk membuat kredensi jangka pendek, yang direkomendasikan untuk meningkatkan keamanan. Anda juga dapat memilih Pengguna untuk membuat kredensi jangka panjang.

3. Pilih Buat peran.
4. Di wizard Buat peran, untuk jenis entitas Tepercaya, pilih Akun AWS.
5. Simpan opsi Akun ini dipilih, lalu pilih Berikutnya.
6. Untuk Menambahkan izin, pilih Buat Kebijakan.

   Tab baru terbuka.

   a. Pilih JSONtab, lalu tambahkan kebijakan tergantung pada kemampuan yang diberikan kepada pengguna konsol. Resolusi Entitas AWS menawarkan kebijakan terkelola berikut berdasarkan kasus penggunaan umum:

      - AWS kebijakan terkelola: AWSEntityResolutionConsoleFullAccess
      - AWS kebijakan terkelola: AWSEntityResolutionConsoleReadOnlyAccess

   b. Pilih Berikutnya: Tag, tambahkan tag (opsional), lalu pilih Berikutnya: Tinjau.
   c. Untuk kebijakan Tinjauan, masukkan Nama dan Deskripsi, dan tinjau Ringkasan.
   d. Pilih Buat kebijakan.

      Anda telah membuat kebijakan untuk anggota kolaborasi.

   e. Kembali ke tab asli Anda dan di bawah Tambahkan izin, masukkan nama kebijakan yang baru saja Anda buat. (Anda mungkin perlu memuat ulang halaman.)
   f. Pilih kotak centang di samping nama kebijakan yang Anda buat, lalu pilih Berikutnya.

7. Untuk Nama, tinjau, dan buat, masukkan nama Peran dan Deskripsi.

   a. Tinjau Pilih entitas tepercaya, masukkan Akun AWS untuk orang atau orang yang akan mengambil peran (jika perlu).
   b. Tinjau izin di Tambahkan izin, dan edit jika perlu.
   c. Tinjau Tag, dan tambahkan tag jika perlu.
   d. Pilih Buat peran.

Membuat peran pekerjaan alur kerja untuk Resolusi Entitas AWS

Resolusi Entitas AWS menggunakan peran pekerjaan alur kerja untuk menjalankan alur kerja. Anda dapat membuat peran ini menggunakan konsol jika Anda memiliki IAM izin yang diperlukan. Jika Anda tidak memiliki `CreateRole` izin, minta administrator Anda untuk membuat peran.

Untuk membuat peran pekerjaan alur kerja untuk Resolusi Entitas AWS

1. Masuk ke IAM konsol di https://console.aws.amazon.com/iam/dengan akun administrator Anda.
2. Di bawah Manajemen akses, pilih Peran.

   Anda dapat menggunakan Peran untuk membuat kredensi jangka pendek, yang direkomendasikan untuk meningkatkan keamanan. Anda juga dapat memilih Pengguna untuk membuat kredensi jangka panjang.
3. Pilih Buat peran.
4. Di wizard Buat peran, untuk jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus.
5. Salin dan tempel kebijakan kepercayaan khusus berikut ke JSON editor.

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

6. Pilih Berikutnya.
7. Untuk Menambahkan izin, pilih Buat Kebijakan.

   Tab baru muncul.

   a. Salin dan tempel kebijakan berikut ke JSON editor.

> **Note**
>
> Kebijakan contoh berikut mendukung izin yang diperlukan untuk membaca sumber daya data yang sesuai seperti Amazon AWS Glue S3 dan. Namun, Anda mungkin perlu mengubah kebijakan ini tergantung pada cara Anda menyiapkan sumber data. AWS Glue Sumber daya Anda dan sumber daya Amazon S3 yang mendasarinya harus sama Wilayah AWS dengan. Resolusi Entitas AWS
> Anda tidak perlu memberikan AWS KMS izin jika sumber data Anda tidak dienkripsi atau didekripsi.

```
{
    "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"
            ]
        }
    ]
}
```

Ganti masing-masing *{{user input placeholder}}* dengan informasi Anda sendiri.

aws-region	Wilayah AWS dari sumber daya Anda. AWS Glue Sumber daya Anda, sumber daya dan sumber daya Amazon S3 yang mendasari harus sama Wilayah AWS dengan AWS KMS sumber daya. `Resolusi Entitas AWS`
accountId	Akun AWS ID Anda.
input-buckets	Bucket Amazon S3 yang berisi objek data yang mendasari dari AWS Glue mana `Resolusi Entitas AWS` akan dibaca.
output-buckets	Bucket Amazon S3 di mana `Resolusi Entitas AWS` akan menghasilkan data output.
input-databases	AWS Glue database dari mana `Resolusi Entitas AWS` akan dibaca.

b. (Opsional) Jika bucket masukan Amazon S3 dienkripsi menggunakan KMS kunci pelanggan, tambahkan yang berikut ini:

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

Ganti masing-masing *{{user input placeholder}}* dengan informasi Anda sendiri.

aws-region	Wilayah AWS dari sumber daya Anda. AWS Glue Sumber daya Anda, sumber daya dan sumber daya Amazon S3 yang mendasari harus sama Wilayah AWS dengan AWS KMS sumber daya. `Resolusi Entitas AWS`
accountId	Akun AWS ID Anda.
inputKeys	Kunci terkelola di AWS Key Management Service. Jika sumber input Anda dienkripsi, `Resolusi Entitas AWS` harus mendekripsi data Anda menggunakan kunci Anda.

c. (Opsional) Jika data yang ditulis ke dalam bucket Amazon S3 keluaran perlu dienkripsi, tambahkan yang berikut ini:

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

Ganti masing-masing *{{user input placeholder}}* dengan informasi Anda sendiri.

aws-region	Wilayah AWS dari sumber daya Anda. AWS Glue Sumber daya Anda, sumber daya dan sumber daya Amazon S3 yang mendasari harus sama Wilayah AWS dengan AWS KMS sumber daya. `Resolusi Entitas AWS`

accountId	Akun AWS ID Anda.
outputKeys	Kunci terkelola di AWS Key Management Service. Jika Anda membutuhkan sumber output Anda untuk dienkripsi, `Resolusi Entitas AWS` harus mengenkripsi data output menggunakan kunci Anda.

d. (Opsional) Jika Anda memiliki langganan dengan layanan penyedia melalui AWS Data Exchange, dan ingin menggunakan peran yang ada untuk alur kerja berbasis layanan penyedia, tambahkan berikut ini:

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

Ganti masing-masing *{{user input placeholder}}* dengan informasi Anda sendiri.

aws-region	Di Wilayah AWS mana sumber daya penyedia diberikan. Anda dapat menemukan nilai ini di aset ARN di AWS Data Exchange konsol. Misalnya: `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
datasetId	ID kumpulan data, ditemukan di AWS Data Exchange konsol.

revisionId	Revisi dataset, ditemukan di konsol. AWS Data Exchange
assetId	ID aset, ditemukan di AWS Data Exchange konsol.

8. Kembali ke tab asli Anda dan di bawah Tambahkan izin, masukkan nama kebijakan yang baru saja Anda buat. (Anda mungkin perlu memuat ulang halaman.)
9. Pilih kotak centang di samping nama kebijakan yang Anda buat, lalu pilih Berikutnya.
10. Untuk Nama, tinjau, dan buat, masukkan nama Peran dan Deskripsi.

> **Note**
>
> Nama peran harus cocok dengan pola dalam `passRole` izin yang diberikan kepada anggota yang dapat meneruskan `workflow job role` untuk membuat alur kerja yang cocok.
> Misalnya, jika Anda menggunakan kebijakan `AWSEntityResolutionConsoleFullAccess` terkelola, ingatlah untuk memasukkan `entityresolution` ke dalam nama peran Anda.

    a. Tinjau Pilih entitas tepercaya, dan edit jika perlu.
    b. Tinjau izin di Tambahkan izin, dan edit jika perlu.
    c. Tinjau Tag, dan tambahkan tag jika perlu.
    d. Pilih Buat peran.

Peran pekerjaan alur kerja untuk Resolusi Entitas AWS telah dibuat.

Siapkan tabel data masukan

Masuk Resolusi Entitas AWS, setiap tabel data input Anda berisi catatan sumber. Catatan ini berisi pengidentifikasi konsumen seperti nama depan, nama belakang, alamat email, atau nomor telepon. Rekaman sumber ini dapat dicocokkan dengan catatan sumber lain yang Anda berikan dalam tabel data input yang sama atau lainnya. Setiap record harus memiliki Record ID (ID Unik) yang unik dan Anda harus mendefinisikannya sebagai kunci utama saat membuat pemetaan skema dalam Resolusi Entitas AWS.

Setiap tabel data input tersedia sebagai AWS Glue tabel yang didukung oleh Amazon S3. Anda dapat menggunakan data pihak pertama yang sudah ada dalam Amazon S3, atau mengimpor tabel data dari penyedia SaaS pihak ketiga lainnya ke Amazon S3. Setelah Anda mengunggah data ke Amazon S3, Anda dapat menggunakan AWS Glue crawler untuk membuat tabel data di AWS Glue Data Catalog. Anda kemudian dapat menggunakan tabel data sebagai masukan untuk Resolusi Entitas AWS.

Bagian berikut menjelaskan cara menyiapkan data pihak pertama dan data pihak ketiga.

Topik

Mempersiapkan data masukan pihak pertama

Langkah-langkah berikut menjelaskan cara menyiapkan data pihak pertama untuk digunakan dalam alur kerja pencocokan berbasis aturan, alur kerja pencocokan berbasis pembelajaran mesin, atau alurkerja pemetaan ID.

Langkah 1: Simpan tabel data input Anda dalam format data yang didukung

Jika Anda telah menyimpan data input pihak pertama dalam format data yang didukung, Anda dapat melewati langkah ini.

Untuk menggunakan Resolusi Entitas AWS, data input harus dalam format yang Resolusi Entitas AWS mendukung. Resolusi Entitas AWS mendukung format data berikut:

- nilai dipisahkan koma () CSV

- Parquet

Langkah 2: Unggah tabel data input Anda ke Amazon S3

Jika Anda sudah memiliki tabel data pihak pertama di Amazon S3, Anda dapat melewati langkah ini.

> **Note**
>
> Data input harus disimpan di Amazon Simple Storage Service (Amazon S3) di tempat yang sama Akun AWS and Wilayah AWS di mana Anda ingin menjalankan alur kerja yang cocok.

Untuk mengunggah tabel data input Anda ke Amazon S3

1. Masuk ke AWS Management Console dan buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Pilih Bucket, lalu pilih bucket untuk menyimpan tabel data Anda.
3. Pilih Unggah, lalu ikuti petunjuknya.
4. Pilih tab Objek untuk melihat awalan tempat data Anda disimpan. Catat nama folder.

   Anda dapat memilih folder untuk melihat tabel data.

Langkah 3: Buat AWS Glue tabel

Data masukan di Amazon S3 harus dikatalogkan AWS Glue dan direpresentasikan sebagai AWS Glue meja. Untuk informasi lebih lanjut tentang cara membuat AWS Glue tabel dengan Amazon S3 sebagai input, lihat Bekerja dengan crawler di AWS Glue konsol di AWS Glue Panduan Pengembang.

> **Note**
>
> Resolusi Entitas AWS tidak mendukung tabel yang dipartisi.

Pada langkah ini, Anda mengatur crawler di AWS Glue yang merayapi semua file di bucket S3 Anda dan membuat AWS Glue meja.

> **Note**
>
> Resolusi Entitas AWS saat ini tidak mendukung lokasi Amazon S3 yang terdaftar di AWS Lake Formation.

Untuk membuat AWS Glue tabel

1. Masuk ke AWS Management Console dan buka AWS Glue konsol di https://console.aws.amazon.com/glue/.
2. Dari bilah navigasi, pilih Crawler.
3. Pilih bucket S3 Anda dari daftar, lalu pilih Tambahkan crawler.
4. Pada halaman Add crawler, masukkan nama Crawler lalu pilih Next.
5. Lanjutkan melalui halaman Add crawler, tentukan detailnya.
6. Pada halaman Pilih IAM peran, pilih Pilih IAM peran yang ada, lalu pilih Berikutnya.

   Anda juga dapat memilih Buat IAM peran atau minta administrator membuat IAM peran jika diperlukan.
7. Untuk Buat jadwal untuk crawler ini, pertahankan default Frekuensi (Jalankan sesuai permintaan) dan kemudian pilih Berikutnya.
8. Untuk Mengkonfigurasi output crawler, masukkan AWS Glue Database dan kemudian pilih Next.
9. Tinjau semua detail, lalu pilih Selesai.
10. Pada halaman Crawler, pilih kotak centang di samping bucket S3, lalu pilih Run crawler.
11. Setelah crawler selesai berjalan, pada AWS Glue bilah navigasi, pilih Database, lalu pilih nama database Anda.
12. Pada halaman Database, pilih Tabel di {nama database Anda}.
    a. Lihat tabel di AWS Glue basis data.
    b. Untuk melihat skema tabel, pilih tabel tertentu.
    c. Buat catatan tentang AWS Glue nama database dan AWS Glue nama meja.

Anda sekarang siap untuk membuat pemetaan skema. Untuk informasi selengkapnya, lihat Membuat pemetaan skema.

Mempersiapkan data input pihak ketiga

Layanan data pihak ketiga menyediakan pengidentifikasi yang dapat dicocokkan dengan pengidentifikasi Anda yang dikenal.

Resolusi Entitas AWS saat ini mendukung layanan penyedia data pihak ketiga berikut:

Layanan penyedia data

Nama perusahaan	Tersedia Wilayah AWS	Pengidentifikasi
LiveRamp	AS Timur (Virginia N.) (us-timur-1), AS Timur (Ohio) (us-timur-2), dan AS Barat (Oregon) (us-barat-2)	ID Ramp
TransUnion	AS Timur (Virginia N.) (us-timur-1), AS Timur (Ohio) (us-timur-2), dan AS Barat (Oregon) (us-barat-2)	TransUnion Individu dan Rumah Tangga IDs
ID Terpadu 2.0	AS Timur (Virginia N.) (us-timur-1), AS Timur (Ohio) (us-timur-2), dan AS Barat (Oregon) (us-barat-2)	mentah UID 2

Langkah-langkah berikut menjelaskan cara menyiapkan data pihak ketiga untuk menggunakan alur kerja pencocokan berbasis layanan penyedia atau alur kerja pemetaan ID berbasis layanan penyedia.

Topik

Langkah 1: Berlangganan layanan penyedia di AWS Data Exchange

Jika Anda memiliki langganan dengan layanan penyedia melalui AWS Data Exchange, Anda dapat menjalankan alur kerja yang cocok dengan salah satu layanan penyedia berikut untuk mencocokkan pengenal Anda yang dikenal dengan penyedia pilihan Anda. Data Anda akan dicocokkan dengan serangkaian input yang ditentukan oleh penyedia pilihan Anda.

Untuk berlangganan layanan penyedia di AWS Data Exchange

1. Lihat daftar penyedia di AWS Data Exchange. Daftar penyedia berikut tersedia:
   - LiveRamp
     - LiveRampResolusi Identitas
     - LiveRampTranscoding
   - TransUnion
     - TransUnion TruAudience Resolusi & Pengayaan Identitas Tanpa Transfer
     - TransUnion TruAudience Resolusi Identitas Tanpa Transfer
   - ID Terpadu 2.0
     - Resolusi Identitas ID 2.0 Terpadu
2. Selesaikan salah satu langkah berikut, tergantung pada jenis penawaran Anda.
   - Penawaran pribadi — Jika Anda memiliki hubungan yang sudah ada dengan penyedia, ikuti prosedur produk dan penawaran Pribadi di AWS Data Exchange Panduan Pengguna untuk menerima penawaran pribadi AWS Data Exchange.
   - Bawa langganan Anda sendiri — Jika Anda sudah memiliki langganan data yang ada dengan penyedia, ikuti prosedur penawaran Bawa Langganan Anda Sendiri (BYOS) di AWS Data Exchange Panduan Pengguna untuk menerima BYOS penawaran AWS Data Exchange.
3. Setelah Anda berlangganan layanan penyedia di AWS Data Exchange, Anda kemudian dapat membuat alur kerja yang cocok atau alur kerja pemetaan ID dengan layanan penyedia tersebut.

Untuk informasi selengkapnya tentang cara mengakses produk penyedia yang berisiAPIs, lihat Mengakses API produk di dalam AWS Data Exchange Panduan Pengguna.

Langkah 2: Siapkan tabel data pihak ketiga

Setiap layanan pihak ketiga memiliki serangkaian rekomendasi dan pedoman yang berbeda untuk membantu memastikan alur kerja pencocokan yang berhasil.

Untuk menyiapkan tabel data pihak ketiga, lihat tabel berikut:

Pedoman layanan penyedia data

Layanan penyedia	Diperlukan ID unik?	Tindakan
LiveRamp	Ya	Pastikan yang berikut ini: • ID Unik dapat berupa pengidentifikasi pseudonim Anda sendiri atau ID baris. • Format file input data dan normalisasi Anda selaras dengan pedoman. LiveRamp Untuk informasi selengkapnya tentang pedoman pemformatan file input untuk alur kerja yang cocok, lihat Melakukan Resolusi Identitas Melalui ADX dalam dokumentasi. LiveRamp Untuk informasi selengkapnya tentang pedoman pemformatan file masukan untuk alur kerja pemetaan ID, lihat Melakukan Transcoding Melalui ADX dalam dokumenta si. LiveRamp
TransUnion	Ya	Pastikan yang berikut ini: • ID Unik ada untuk Pengayaan TransUnion Data. **Note** Atribut pass along diizinkan untuk bertahan dalam input dan output ke

Layanan penyedia	Diperlukan ID unik?	Tindakan

		TransUnion. Kunci E rumah tangga dan HHID khusus untuk namespace klien.
		• **`Phone number`**harus 10 digit, tanpa karakter khusus seperti spasi atau tanda hubung.
		• **`Addresses`** harus dipecah menjadi
		  • satu baris alamat (gabungkan baris alamat 1 & 2, jika ada)
		  • kota
		  • zip (atau zip plus4), tanpa karakter khusus seperti spasi atau tanda hubung
		  • negara, ditentukan sebagai 2 kode huruf 3
		• **`Email addresses`** harus dalam plaintext.
		• **`First Name`**bisa lebih rendah atau huruf besar, nama panggilan didukung, tetapi judul dan sufiks harus dikecualikan.
		• **`Last Name`**dapat berupa huruf kecil atau besar, inisiasi tengah untuk dikecualikan.

Layanan penyedia	Diperlukan ID unik?	Tindakan
ID Terpadu 2.0	Ya	Pastikan yang berikut ini: • ID Unik tidak bisa berupa hash. • UID2mendukung email dan nomor telepon untuk UID2 generasi. Namun, jika kedua nilai hadir dalam pemetaan skema, alur kerja menduplikasi setiap catatan dalam output. Satu catatan menggunakan email untuk UID2 pembuatan dan catatan kedua menggunakan nomor telepon. Jika data Anda menyertakan campuran email dan nomor telepon dan Anda tidak ingin duplikasi catatan ini dalam output, pendekatan terbaik adalah membuat alur kerja terpisah untuk masing-masing, dengan pemetaan skema terpisah. Dalam skenario ini, lakukan langkah-langkah dua kali—buat satu alur kerja untuk email dan yang terpisah untuk nomor telepon. **Note** Email atau nomor telepon tertentu, pada waktu tertentu, menghasil kan UID2 nilai mentah yang sama, tidak peduli siapa yang mengajukan permintaan. Mentah UID2s dibuat dengan menambahkan garam dari ember garam yang diputar kira-kira setahun sekali, UID2 menyebabkan bahan mentah juga diputar dengannya. Ember garam yang berbeda berputar

Layanan penyedia	Diperlukan ID unik?	Tindakan
		pada waktu yang berbeda sepanjang tahun. Resolusi Entitas AWS saat ini tidak melacak ember garam berputar dan mentahUID2s, jadi disaranka n agar Anda meregenerasi mentah setiap hari. UID2s Untuk informasi selengkapnya, lihat Seberapa sering UID2s harus di-refresh untuk pembaruan tambahan? dalam dokumentasi UID 2.0.

Langkah 3: Simpan tabel data input Anda dalam format data yang didukung

Jika Anda telah menyimpan data input pihak ketiga dalam format data yang didukung, Anda dapat melewati langkah ini.

Untuk menggunakan Resolusi Entitas AWS, data input harus dalam format yang Resolusi Entitas AWS mendukung. Resolusi Entitas AWS mendukung format data berikut:

- nilai dipisahkan koma () CSV

> **Note**
>
> LiveRamp hanya mendukung CSV file.

- Parquet

Langkah 4: Unggah tabel data input Anda ke Amazon S3

Jika Anda sudah memiliki tabel data pihak ketiga di Amazon S3, Anda dapat melewati langkah ini.

> **Note**
>
> Data input harus disimpan di Amazon Simple Storage Service (Amazon S3) di tempat yang sama Akun AWS and Wilayah AWS di mana Anda ingin menjalankan alur kerja yang cocok.

Untuk mengunggah tabel data input Anda ke Amazon S3

1. Masuk ke AWS Management Console dan buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Pilih Bucket, lalu pilih bucket untuk menyimpan tabel data Anda.
3. Pilih Unggah, lalu ikuti petunjuknya.
4. Pilih tab Objek untuk melihat awalan tempat data Anda disimpan. Catat nama folder.

   Anda dapat memilih folder untuk melihat tabel data.

Langkah 5: Buat AWS Glue tabel

Data masukan di Amazon S3 harus dikatalogkan AWS Glue dan direpresentasikan sebagai AWS Glue meja. Untuk informasi lebih lanjut tentang cara membuat AWS Glue tabel dengan Amazon S3 sebagai input, lihat Bekerja dengan crawler di AWS Glue konsol di AWS Glue Panduan Pengembang.

> **Note**
>
> Resolusi Entitas AWS tidak mendukung tabel yang dipartisi.

Pada langkah ini, Anda mengatur crawler di AWS Glue yang merayapi semua file di bucket S3 Anda dan membuat AWS Glue meja.

> **Note**
>
> Resolusi Entitas AWS saat ini tidak mendukung lokasi Amazon S3 yang terdaftar di AWS Lake Formation.

Untuk membuat AWS Glue tabel

1. Masuk ke AWS Management Console dan buka AWS Glue konsol di https://console.aws.amazon.com/glue/.
2. Dari bilah navigasi, pilih Crawler.
3. Pilih bucket S3 Anda dari daftar, lalu pilih Tambahkan crawler.
4. Pada halaman Add crawler, masukkan nama Crawler lalu pilih Next.
5. Lanjutkan melalui halaman Add crawler, tentukan detailnya.
6. Pada halaman Pilih IAM peran, pilih Pilih IAM peran yang ada, lalu pilih Berikutnya.

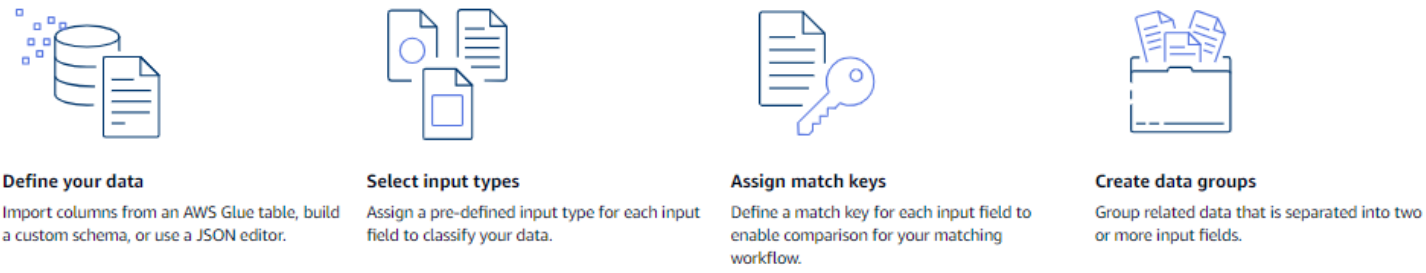
   Anda juga dapat memilih Buat IAM peran atau minta administrator membuat IAM peran jika diperlukan.
7. Untuk Buat jadwal untuk crawler ini, pertahankan default Frekuensi (Jalankan sesuai permintaan) dan kemudian pilih Berikutnya.
8. Untuk Mengkonfigurasi output crawler, masukkan AWS Glue Database dan kemudian pilih Next.
9. Tinjau semua detail, lalu pilih Selesai.
10. Pada halaman Crawler, pilih kotak centang di samping bucket S3 Anda, lalu pilih Jalankan crawler.
11. Setelah crawler selesai berjalan, pada AWS Glue bilah navigasi, pilih Database, lalu pilih nama database Anda.
12. Pada halaman Database, pilih Tabel di {nama database Anda}.

    a. Lihat tabel di AWS Glue basis data.
    b. Untuk melihat skema tabel, pilih tabel tertentu.
    c. Buat catatan tentang AWS Glue nama database dan AWS Glue nama meja.

Tentukan data input menggunakan pemetaan skema

Pemetaan skema mendefinisikan data masukan yang ingin Anda selesaikan. Ini juga menyediakan metadata tentang data input, seperti jenis atribut kolom (tipe input) dan kolom mana yang cocok.

Saat membuat pemetaan skema, pertama-tama Anda menentukan bidang masukan dan jenis masukan, lalu tentukan kunci pencocokan dan data terkait grup. Diagram berikut merangkum cara membuat pemetaan skema.



Sebelum Anda membuat pemetaan skema, Anda harus terlebih dahulu mengatur Resolusi Entitas AWS dan siapkan tabel data Anda. Untuk informasi selengkapnya, silakan lihat Mengatur Resolusi Entitas AWS dan Siapkan tabel data masukan.

Setelah Anda membuat pemetaan skema, Anda dapat melakukan salah satu hal berikut:

- Buat alur kerja yang cocok untuk menemukan kecocokan antara input data yang berbeda.
- Buat sumber namespace ID yang dapat Anda gunakan dalam alur kerja pemetaan ID untuk menerjemahkan data dari sumber ke target.
- Buat alur kerja pemetaan ID dalam hal yang sama Akun AWSmenggunakan pemetaan skema Anda sebagai sumbernya.

Topik

- Membuat pemetaan skema
- Mengkloning pemetaan skema
- Mengedit pemetaan skema
- Menghapus pemetaan skema

Membuat pemetaan skema

Prosedur ini menjelaskan proses pembuatan pemetaan skema menggunakan Resolusi Entitas AWS konsol.

Ada tiga cara untuk membuat pemetaan skema:

- Impor data masukan yang ada menggunakan Impor dari AWS Glueopsi - Gunakan metode pembuatan ini untuk menentukan bidang masukan yang dimulai dengan kolom yang telah diisi sebelumnya dari sebuah AWS Glue tabel menggunakan aliran terpandu.
- Mendefinisikan data input secara manual menggunakan opsi Build custom schema — Gunakan metode pembuatan ini untuk menentukan kolom input secara manual menggunakan alur terpandu.
- Buat secara manual menggunakan opsi Gunakan JSON editor - Gunakan JSON editor untuk membuat, menggunakan sampel, atau mengimpor data input yang ada secara manual.

> **Note**
>
> Kolom Unik ID dan Input tidak tersedia dengan opsi ini.

Import from AWS Glue

Untuk membuat pemetaan skema dengan mengimpor data input yang ada dari AWS Glue

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih Pemetaan skema.
3. Pada halaman pemetaan Skema, di sudut kanan atas, pilih Buat pemetaan skema.
4. Untuk Langkah 1: Tentukan detail skema, lakukan hal berikut:
    a. Untuk Nama dan metode pembuatan, masukkan nama pemetaan Skema dan Deskripsi opsional.
    b. Untuk metode Pembuatan, pilih Impor dari AWS Glue.
    c. Pilih AWS Glue database dari dropdown, dan kemudian pilih AWS Glue tabel dari dropdown.

Untuk membuat tabel baru, buka AWS Glue konsol https://console.aws.amazon.com/glue/. Untuk informasi selengkapnya, silakan lihat AWS Glue tabel di AWS Glue Panduan Pengguna.

d. Untuk ID Unik, tentukan kolom yang secara jelas mereferensikan setiap baris data Anda.

   Example

   Misalnya: **`Primary_key`**, **`Row_ID`**, atau **`Record_ID`**.

   > **Note**
   >
   > Kolom ID Unik diperlukan. ID Unik harus berupa pengidentifikasi unik dalam satu tabel. Namun, di berbagai tabel, ID Unik dapat memiliki nilai duplikat. Jika ID Unik tidak ditentukan, tidak unik dalam sumber yang sama, atau tumpang tindih dalam hal nama atribut di seluruh sumber, Resolusi Entitas AWS menolak catatan saat alur kerja yang cocok dijalankan. Jika Anda menggunakan pemetaan skema ini dalam alur kerja pencocokan berbasis aturan, ID Unik tidak boleh melebihi 38 karakter.

e. Untuk bidang Input, pilih kolom yang ingin Anda gunakan untuk pencocokan dan untuk opsional melewati.

   Anda dapat memilih maksimal 34 kolom total untuk pencocokan dan melewati.

   i. Di bawah Pencocokan, pilih kolom yang akan Anda gunakan sebagai bidang input untuk pencocokan.

      Anda dapat memilih maksimal 24 kolom total untuk pencocokan.

   ii. Pilih Tambahkan kolom untuk dilewati jika Anda ingin menentukan kolom yang tidak digunakan untuk pencocokan.

   iii. (Opsional) Di bawah Lewati, pilih kolom yang akan disertakan sebagai kolom pass through.

f. (Opsional) Jika Anda ingin mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

g. Pilih Berikutnya.

5. Untuk Langkah 2: Petakan bidang input, tentukan bidang input yang ingin Anda gunakan untuk pencocokan dan untuk lolos opsional.

a. Untuk bidang Input yang cocok, untuk setiap bidang Input, tentukan tipe Input, kunci Match, dan status Hashing.

   Tipe Input membantu Anda mengklasifikasikan data. Tombol Match memungkinkan perbandingan bidang input dengan alur kerja yang cocok. Status Hashing menunjukkan apakah nilai kolom untuk bidang input tersebut di-hash atau cleartext.

   > **Note**
   >
   > Jika Anda membuat pemetaan skema untuk digunakan dengan teknik pencocokan berbasis layanan LiveRamp penyedia, Anda dapat:
   >
   > - Tentukan tipe Input sebagai LiveRampID.
   > - Tentukan bidang nama sebagai beberapa bidang (seperti**`first_name`**,**`last_name`**) atau dalam satu bidang.
   > - Tentukan bidang alamat jalan sebagai beberapa bidang (seperti**`address1`**,**`address2`**) atau dalam satu bidang.
   >
   >   Jika cocok dengan alamat, kode pos diperlukan.
   > - Sertakan email atau telepon dengan nama, dan bidang tersebut dapat cocok dengan alamat jalan.

   > **Note**
   >
   > Jika Anda membuat pemetaan skema untuk digunakan dengan alur kerja pencocokan berbasis pembelajaran mesin, kumpulan data Anda harus berisi setidaknya satu dari atribut berikut:,,,,, atau. **`phonenumber`** **`emailaddress`** **`fullname`** **`addresses`** **`birthdate`**
   > Jangan tentukan tipe Input untuk salah satu atribut ini sebagai string Kustom.

b. (Opsional) Untuk field Input untuk dilewati, tambahkan field input yang tidak akan cocok dan status Hashing yang sesuai.

   Status Hashing menunjukkan apakah nilai kolom untuk bidang input tersebut di-hash atau cleartext.

c. Pilih Berikutnya.

6. Untuk Langkah 3: Kelompokkan data, lakukan hal berikut:

   a. Pilih bidang Nama terkait, lalu masukkan Nama grup dan tombol Cocokkan.

      Example

      Misalnya, pilih bidang input**`First name`**,**`Middle name`**, dan**`Last name`**. Kemudian masukkan nama Grup yang disebut "**`Full name`**" dan tombol Match yang disebut "**`Full name`**" untuk mengaktifkan perbandingan.

   b. Pilih bidang Alamat terkait, lalu masukkan Nama grup dan tombol Cocokkan.

      Example

      Misalnya, pilih bidang input**`Home street address 1`**,**`Home street address 2`**, dan**`Home city`**. Kemudian masukkan nama Grup yang disebut "**`Shipping address`**" dan tombol Match yang disebut "**`Shipping address`**" untuk mengaktifkan perbandingan.

   c. Pilih bidang Nomor telepon terkait, lalu masukkan nama grup dan tombol Cocokkan.

      Example

      Misalnya, pilih bidang input**`Home phone 1`**,**`Home phone 2`**, dan**`Cell phone`**. Kemudian masukkan nama Grup yang disebut "**`Shipping phone number`**" dan tombol Match yang disebut "**`Shipping phone number`**" untuk mengaktifkan perbandingan.

      Jika Anda memiliki lebih dari satu jenis data, Anda dapat menambahkan lebih banyak grup.

   d. Pilih Berikutnya.

7. Untuk Langkah 4: Tinjau dan buat, lakukan hal berikut:

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat pemetaan skema.

> **Note**
>
> Anda tidak dapat memodifikasi pemetaan skema setelah Anda mengaitkannya ke alur kerja. Anda dapat mengkloning pemetaan skema jika Anda ingin menggunakan konfigurasi yang ada untuk membuat pemetaan skema baru.

Setelah membuat pemetaan skema, Anda siap membuat alur kerja yang cocok atau membuat namespace ID.

Build custom schema

Untuk membuat pemetaan skema menggunakan opsi Build custom schema

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih Pemetaan skema.
3. Pada halaman pemetaan Skema, di sudut kanan atas, pilih Buat pemetaan skema.
4. Untuk Langkah 1: Tentukan detail skema, lakukan hal berikut:
   a. Untuk nama dan metode pembuatan, masukkan nama pemetaan Skema dan Deskripsi opsional.
   b. Untuk metode Creation, pilih Build custom schema.
   c. Untuk ID Unik, masukkan ID unik untuk mengidentifikasi setiap baris data Anda.

      Example

      Misalnya: **`Primary_key`**, **`Row_ID`**, atau **`Record_ID`**.

      > **Note**
      >
      > Kolom ID Unik diperlukan. ID Unik harus berupa pengidentifikasi unik dalam satu tabel. Namun, di berbagai tabel, ID Unik dapat memiliki nilai duplikat. Jika ID Unik tidak ditentukan, tidak unik dalam sumber yang sama, atau tumpang tindih dalam hal nama atribut di seluruh sumber, Resolusi Entitas AWS menolak catatan saat alur kerja yang cocok dijalankan. Jika Anda menggunakan

pemetaan skema ini dalam alur kerja pencocokan berbasis aturan, ID Unik tidak boleh melebihi 38 karakter.

d. (Opsional) Jika Anda ingin mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

e. Pilih Berikutnya.

5. Untuk Langkah 2: Petakan bidang input, tentukan bidang input yang ingin Anda gunakan untuk pencocokan dan untuk lolos opsional.

   Anda dapat menentukan maksimum 34 kolom total untuk pencocokan dan melewati.

   a. Untuk bidang Input yang cocok, tambahkan kolom Input, dan jenis Input yang sesuai, kunci Match, dan status Hashing.

      Anda dapat menambahkan maksimal 24 kolom input total untuk pencocokan.

      Tipe Input membantu Anda mengklasifikasikan data. Tombol Match memungkinkan perbandingan bidang input dengan alur kerja yang cocok. Status Hashing menunjukkan apakah nilai kolom untuk bidang input tersebut di-hash atau cleartext.

      > **Note**
      >
      > Jika Anda membuat pemetaan skema untuk digunakan dengan teknik pencocokan berbasis layanan LiveRamp penyedia, Anda dapat menentukan tipe Input sebagai ID. LiveRamp Jika Anda ingin memasukkan PII data dalam output, maka Anda harus menentukan Jenis input sebagai String khusus.

      > **Note**
      >
      > Jika Anda membuat pemetaan skema untuk digunakan dengan alur kerja pencocokan berbasis pembelajaran mesin, kumpulan data Anda harus berisi setidaknya satu dari atribut berikut:,,,,, atau. **`phonenumber`** **`emailaddress`** **`fullname`** **`addresses`** **`birthdate`**
      > Jangan tentukan tipe Input untuk salah satu atribut ini sebagai string Kustom.

   b. (Opsional) Untuk bidang Input untuk dilewati, tambahkan kolom input yang tidak akan cocok dan status Hashing yang sesuai.

c. Pilih Berikutnya.

6. Untuk Langkah 3: Data grup:

   a. Pilih bidang Nama terkait, lalu masukkan Nama grup dan tombol Cocokkan.

      Example

      Misalnya, pilih bidang input**`First name`**,**`Middle name`**, dan**`Last name`**. Kemudian masukkan nama Grup yang disebut "**`Full name`**" dan tombol Match yang disebut "**`Full name`**" untuk mengaktifkan perbandingan.

   b. Pilih bidang Alamat terkait, lalu masukkan Nama grup dan tombol Cocokkan.

      Example

      Misalnya, pilih bidang input**`Home street address 1`**,**`Home street address 2`**, dan**`Home city`**. Kemudian masukkan nama Grup yang disebut "**`Shipping address`**" dan tombol Match yang disebut "**`Shipping address`**" untuk mengaktifkan perbandingan.

   c. Pilih bidang Nomor telepon terkait, lalu masukkan nama grup dan tombol Cocokkan.

      Example

      Misalnya, pilih bidang input**`Home phone 1`**,**`Home phone 2`**, dan**`Cell phone`**. Kemudian masukkan nama Grup yang disebut "**`Shipping phone number`**" dan tombol Match yang disebut "**`Shipping phone number`**" untuk mengaktifkan perbandingan.

      Jika Anda memiliki lebih dari satu jenis data, Anda dapat menambahkan lebih banyak grup.

   d. Pilih Berikutnya.

7. Untuk Langkah 4: Tinjau dan buat, lakukan hal berikut:

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat pemetaan skema.

> **Note**
>
> Anda tidak dapat mengubah pemetaan skema setelah Anda mengaitkannya dengan alur kerja. Anda dapat mengkloning pemetaan skema jika Anda ingin menggunakan konfigurasi yang ada untuk membuat pemetaan skema baru.

Setelah membuat pemetaan skema, Anda siap membuat alur kerja yang cocok atau membuat namespace ID.

Use JSON editor

Untuk membuat pemetaan skema dengan menggunakan editor JSON

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih Pemetaan skema.
3. Pada halaman pemetaan Skema, di sudut kanan atas, pilih Buat pemetaan skema.
4. Untuk Langkah 1: Tentukan detail skema, lakukan hal berikut:
   a. Untuk nama dan metode pembuatan, masukkan nama pemetaan Skema dan Deskripsi opsional.
   b. Untuk metode pembuatan, pilih Gunakan JSON editor.
   c. (Opsional) Jika Anda ingin mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.
   d. Pilih Berikutnya.
5. Untuk Langkah 2: Tentukan pemetaan:
   a. Mulai buat skema di JSON editor atau pilih salah satu opsi berikut berdasarkan tujuan Anda:

Tujuan Anda	Opsi yang disarankan
Mulai membangun pemetaan skema Anda	Masukkan sampel JSON dan kemudian edit informasi seperluny a.

Tujuan Anda	Opsi yang disarankan
Gunakan JSON file yang sudah ada	Impor dari file

b. Pilih Berikutnya.

6. Untuk Langkah 3: Tinjau dan buat:

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat pemetaan skema.

> **Note**
>
> Anda tidak dapat mengubah pemetaan skema setelah Anda mengaitkannya dengan alur kerja. Anda dapat mengkloning pemetaan skema jika Anda ingin menggunakan konfigurasi yang ada untuk membuat pemetaan skema baru.

Setelah membuat pemetaan skema, Anda siap membuat alur kerja yang cocok atau membuat namespace ID.

Mengkloning pemetaan skema

Anda dapat mengkloning pemetaan skema jika Anda ingin menggunakan konfigurasi yang ada untuk membuat pemetaan skema baru.

Untuk mengkloning pemetaan skema:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih Pemetaan skema.
3. Pilih pemetaan skema.
4. Pilih Klon.
5. Pada halaman Tentukan detail skema, buat perubahan yang diperlukan lalu pilih Berikutnya.
6. Pada halaman Pilih teknik pencocokan, buat perubahan yang diperlukan dan kemudian pilih Berikutnya.

7. Pada halaman kolom masukan Peta, buat perubahan yang diperlukan lalu pilih Berikutnya.
8. Pada halaman Data grup, buat perubahan yang diperlukan lalu pilih Berikutnya.
9. Pada halaman Tinjau dan simpan, buat perubahan yang diperlukan lalu pilih Pemetaan skema klon.

Mengedit pemetaan skema

Anda hanya dapat mengedit pemetaan skema sebelum mengaitkannya ke alur kerja. Setelah mengaitkan pemetaan skema ke alur kerja, Anda tidak dapat mengeditnya. Anda dapat mengkloning pemetaan skema jika Anda ingin menggunakan konfigurasi yang ada untuk membuat pemetaan skema baru.

Untuk mengedit pemetaan skema:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih Pemetaan skema.
3. Pilih pemetaan skema.
4. Pilih Edit.
5. Pada halaman Tentukan detail skema, buat perubahan yang diperlukan lalu pilih Berikutnya.
6. Pada halaman Pilih teknik pencocokan, buat perubahan yang diperlukan dan kemudian pilih Berikutnya.
7. Pada halaman kolom masukan Peta, buat perubahan yang diperlukan lalu pilih Berikutnya.
8. Pada halaman Data grup, buat perubahan yang diperlukan lalu pilih Berikutnya.
9. Pada halaman Tinjau dan simpan, buat perubahan yang diperlukan lalu pilih Edit pemetaan skema.

Menghapus pemetaan skema

Anda tidak dapat menghapus pemetaan skema saat dikaitkan dengan alur kerja yang cocok. Anda harus terlebih dahulu menghapus pemetaan skema dari semua alur kerja pencocokan terkait sebelum Anda dapat menghapusnya.

Untuk menghapus pemetaan skema:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih Pemetaan skema.
3. Pilih pemetaan skema.
4. Pilih Hapus.
5. Konfirmasikan penghapusan dan kemudian pilih Hapus.

Tentukan data input menggunakan namespace ID

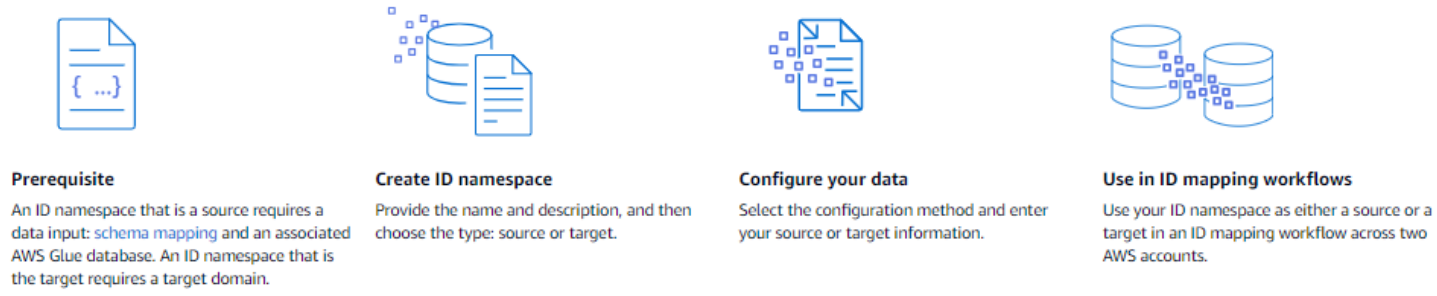
Namespace ID adalah pembungkus di sekitar tabel data input Anda. Anda menggunakan namespace ID untuk menyediakan metadata yang menjelaskan data masukan dan teknik pencocokan serta cara menggunakannya dalam alur kerja pemetaan ID.

Ada dua jenis ruang nama ID: Sumber dan Target.

- Sumber berisi konfigurasi untuk data sumber yang Resolusi Entitas AWS proses dalam alur kerja pemetaan ID.
- Target berisi konfigurasi data target yang diselesaikan oleh semua sumber.

Anda dapat menentukan data masukan yang ingin Anda selesaikan di dua Akun AWS dalam alur kerja pemetaan ID. Satu peserta membuat sumber namespace ID dan peserta lain membuat target namespace ID. Setelah peserta membuat sumber dan target, Anda dapat menjalankan alur kerja pemetaan ID untuk menerjemahkan data dari sumber ke target.

Diagram berikut merangkum cara membuat namespace ID untuk digunakan dalam alur kerja pemetaan ID.



Bagian berikut menjelaskan cara membuat sumber namespace ID dan target namespace ID.

Topik

- Sumber namespace ID
- Target namespace ID
- Mengedit namespace ID
- Menghapus namespace ID
- Menambahkan atau memperbarui kebijakan sumber daya untuk namespace ID

Sumber namespace ID

Sumber namespace ID adalah sumber data dalam alur kerja pemetaan ID.

Sebelum membuat sumber namespace ID, Anda harus terlebih dahulu membuat pemetaan skema atau alur kerja yang cocok, tergantung pada kasus penggunaan Anda. Untuk informasi selengkapnya, silakan lihat Membuat pemetaan skema dan Cocokkan data input menggunakan alur kerja yang cocok.

Setelah membuat sumber namespace ID, Anda dapat menggunakannya bersama dengan target namespace ID dalam alur kerja pemetaan ID. Untuk informasi selengkapnya, lihat Memetakan data masukan menggunakan alur kerja pemetaan ID.

Ada dua cara untuk membuat sumber namespace ID di Resolusi Entitas AWS konsol: metode berbasis aturan atau metode layanan penyedia.

Topik

- Membuat sumber namespace ID (berbasis aturan)
- Membuat sumber namespace ID (layanan penyedia)

Membuat sumber namespace ID (berbasis aturan)

Topik ini menjelaskan proses pembuatan sumber namespace ID menggunakan metode berbasis aturan. Metode ini menggunakan aturan pencocokan untuk menerjemahkan data pihak pertama dari sumber ke target dalam alur kerja pemetaan ID.

> **Note**
>
> Jika data input adalah sumbernya, maka harus memiliki pemetaan skema dan yang terkait AWS Glue basis data.

Untuk membuat sumber namespace ID (berbasis aturan)

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih ruang nama ID.

3. Pada halaman ruang nama ID, di sudut kanan atas, pilih Buat namespace ID.
4. Untuk Detailnya, lakukan hal berikut:
   a. Untuk nama namespace ID, masukkan nama unik.
   b. (Opsional) Untuk Deskripsi, masukkan deskripsi opsional.
   c. Untuk jenis namespace ID, pilih Sumber.
5. Untuk metode namespace ID, pilih Rule based.
6. Untuk input Data, pilih jenis input yang ingin Anda gunakan dan kemudian lakukan tindakan yang disarankan.

Layanan penyedia	Tindakan yang disarankan
Pemetaan skema yang ada	1. Pilih pemetaan Skema. 2. Pilih AWS Glue database, AWS Glue tabel, dan pemetaan Skema dari daftar dropdown. Anda dapat menambahkan hingga 20 input data.
Alur kerja pencocokan yang ada	1. Pilih alur kerja Pencocokan. 2. Pilih akun yang terkait dengan namespace ID: salah satu akun Anda Akun AWSatau Lainnya Akun AWS. 3. Bergantung pada jenis akun, pilih nama alur kerja yang cocok atau masukkan alur kerja ARN Pencocokan.

7. Untuk parameter Aturan, lakukan hal berikut.
   a. Tentukan kontrol Aturan dengan memilih salah satu opsi berikut berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Izinkan aturan dari sumber dan target	Tidak ada preferensi

Tujuan Anda	Opsi yang disarankan
Pilih apakah sumber, target, atau keduanya dapat memberikan aturan dalam alur kerja pemetaan ID	Aturan terbatas

Kontrol aturan harus kompatibel antara sumber dan target yang akan digunakan dalam alur kerja pemetaan ID. Misalnya, jika namespace ID sumber membatasi aturan ke target tetapi namespace ID target membatasi aturan ke sumber, ini menghasilkan kesalahan.

b. Tentukan aturan Pencocokan dengan memilih salah satu opsi berikut berdasarkan jenis input data Anda.

Jenis masukan data	Tindakan yang disarankan
Pemetaan skema	Pilih Tambahkan aturan lain untuk menambahkan aturan yang cocok. Anda dapat menerapkan hingga 25 aturan Pencocokan untuk menentukan kriteria kecocokan Anda.
Alur kerja yang cocok	Pilih salah satu Gunakan aturan dari alur kerja yang cocok atau Berikan aturan baru untuk menentukan aturan Pencocokan Anda.

8. Untuk parameter Perbandingan dan pencocokan, lakukan hal berikut.

a. Tentukan tipe Perbandingan dengan memilih salah satu opsi berikut berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Izinkan jenis perbandingan apa pun digunakan saat Anda membuat alur kerja pemetaan ID.	Tidak ada preferensi

Tujuan Anda	Opsi yang disarankan
Temukan kombinasi kecocokan di seluruh data yang disimpan di beberapa bidang input, terlepas dari apakah data berada di bidang input yang sama atau berbeda.	Beberapa bidang masukan
Batasi perbandingan dalam satu bidang input, ketika data serupa yang disimpan di beberapa bidang input tidak boleh dicocokkan.	Bidang masukan tunggal

b. Tentukan jenis pencocokan Rekam dengan memilih salah satu opsi berikut berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Izinkan jenis perbandingan apa pun digunakan saat Anda membuat alur kerja pemetaan ID.	Tidak ada preferensi
Batasi jenis pencocokan rekaman untuk menyimpan hanya satu catatan yang cocok di sumber untuk setiap rekaman yang cocok dalam target saat Anda membuat alur kerja pemetaan ID.	Pencocokan catatan terbatas and Satu sumber untuk satu target
Batasi jenis pencocokan rekaman untuk menyimpan semua catatan yang cocok di sumber untuk setiap rekaman yang cocok dalam target saat Anda membuat alur kerja pemetaan ID.	Pencocokan catatan terbatas and Banyak sumber untuk satu target

> **Note**
>
> Anda harus menentukan batasan yang kompatibel untuk ruang nama ID sumber dan target. Misalnya, jika namespace ID sumber membatasi aturan ke target tetapi namespace ID target membatasi aturan ke sumber, ini menghasilkan kesalahan.

9. Tentukan izin akses Layanan dengan memilih nama peran Layanan yang ada dari daftar tarik-turun.
10. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.
11. Pilih Buat namespace ID.

Sumber namespace ID dibuat. Anda sekarang siap untuk membuat target namespace ID.

Membuat sumber namespace ID (layanan penyedia)

Topik ini menjelaskan proses pembuatan sumber namespace ID menggunakan metode layanan Penyedia. Metode ini menggunakan layanan penyedia yang disebut LiveRamp. LiveRamp menerjemahkan data pihak ketiga yang dikodekan dari sumber ke target selama alur kerja pemetaan ID.

> **Note**
>
> Jika data input adalah sumbernya, maka harus memiliki pemetaan skema dan yang terkait AWS Glue basis data.

Untuk membuat sumber namespace ID (layanan penyedia)

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih ruang nama ID.
3. Pada halaman ruang nama ID, di sudut kanan atas, pilih Buat namespace ID.
4. Untuk Detailnya, lakukan hal berikut:

    a. Untuk nama namespace ID, masukkan nama unik.

b. (Opsional) Untuk Deskripsi, masukkan deskripsi opsional.

c. Untuk jenis namespace ID, pilih Sumber.

5. Untuk metode namespace ID, pilih Layanan penyedia.

> **Note**
>
> Resolusi Entitas AWS saat ini menawarkan layanan LiveRamp penyedia sebagai metode namespace ID. Jika Anda memiliki langganan LiveRamp, maka status akan muncul sebagai Berlangganan. Untuk informasi selengkapnya tentang cara berlangganan LiveRamp, lihatLangkah 1: Berlangganan layanan penyedia di AWS Data Exchange.

6. Untuk input Data, pilih AWS Glue database, AWS Glue tabel, dan pemetaan Skema dari daftar dropdown.

   Anda dapat menambahkan hingga 20 input data.

7. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.

Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-id-mapping-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun.

Opsi	Tindakan yang disarankan
	Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

8. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.
9. Pilih Buat namespace ID.

Sumber namespace ID dibuat. Anda sekarang siap untuk membuat target namespace ID.

Target namespace ID

Target namespace ID adalah target data dalam alur kerja pemetaan ID. Semua sumber menyelesaikan target.

Sebelum membuat target namespace ID, Anda harus terlebih dahulu membuat alur kerja yang cocok atau berlangganan layanan penyedia (LiveRamp), tergantung pada kasus penggunaan Anda. Untuk informasi selengkapnya, silakan lihat Cocokkan data input menggunakan alur kerja yang cocok dan Langkah 1: Berlangganan layanan penyedia di AWS Data Exchange.

Setelah membuat target namespace ID, Anda dapat menggunakannya bersama dengan sumber namespace ID dalam alur kerja pemetaan ID. Untuk informasi selengkapnya, lihat Memetakan data masukan menggunakan alur kerja pemetaan ID.

Ada dua cara untuk membuat target namespace ID di Resolusi Entitas AWS konsol: metode berbasis aturan atau metode layanan penyedia.

Topik

- Membuat target namespace ID (metode berbasis aturan)
- Membuat target namespace ID (metode layanan penyedia)

Membuat target namespace ID (metode berbasis aturan)

Topik ini menjelaskan proses pembuatan target namespace ID menggunakan metode berbasis aturan. Metode ini menggunakan aturan pencocokan untuk menerjemahkan data pihak pertama dari sumber ke target selama alur kerja pemetaan ID.

Untuk membuat target namespace ID (berbasis aturan)

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih ruang nama ID.
3. Pada halaman ruang nama ID, di sudut kanan atas, pilih Buat namespace ID.
4. Untuk Detailnya, lakukan hal berikut:
    a. Untuk nama namespace ID, masukkan nama unik.
    b. (Opsional) Untuk Deskripsi, masukkan deskripsi opsional.
    c. Untuk jenis namespace ID, pilih Target.
5. Untuk metode namespace ID, pilih Rule based.
6. Untuk input Data, di bawah Alur kerja yang cocok, lakukan hal berikut.
    a. Pilih akun yang terkait dengan namespace ID: salah satu akun Anda Akun AWSatau Lainnya Akun AWS.
    b. Bergantung pada jenis akun, pilih nama alur kerja yang cocok atau masukkan alur kerja ARN Pencocokan.
7. Untuk parameter Aturan, lakukan hal berikut.

a. Tentukan kontrol Aturan dengan memilih salah satu opsi berikut berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Izinkan aturan dari sumber dan target	Tidak ada preferensi
Pilih apakah sumber, target, atau keduanya dapat memberikan aturan dalam alur kerja pemetaan ID	Aturan terbatas

Kontrol aturan harus kompatibel antara sumber dan target yang akan digunakan dalam alur kerja pemetaan ID. Misalnya, jika namespace ID sumber membatasi aturan ke target tetapi namespace ID target membatasi aturan ke sumber, ini menghasilkan kesalahan.

b. Untuk aturan Pencocokan, Resolusi Entitas AWS secara otomatis menambahkan aturan dari alur kerja yang cocok.

8. Untuk parameter Perbandingan dan pencocokan, lakukan hal berikut.

a. Tentukan tipe Perbandingan dengan memilih salah satu opsi berikut berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Izinkan jenis perbandingan apa pun digunakan saat Anda membuat alur kerja pemetaan ID.	Tidak ada preferensi
Temukan kombinasi kecocokan di seluruh data yang disimpan di beberapa bidang input, terlepas dari apakah data berada di bidang input yang sama atau berbeda.	Beberapa bidang masukan
Batasi perbandingan dalam satu bidang input, ketika data serupa yang disimpan di beberapa bidang input tidak boleh dicocokkan.	Bidang masukan tunggal

b. Tentukan jenis pencocokan Rekam dengan memilih salah satu opsi berikut berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Izinkan jenis perbandingan apa pun digunakan saat Anda membuat alur kerja pemetaan ID.	Tidak ada preferensi
Batasi jenis pencocokan rekaman untuk menyimpan hanya satu catatan yang cocok di sumber untuk setiap rekaman yang cocok dalam target saat Anda membuat alur kerja pemetaan ID.	Pencocokan catatan terbatas and Satu sumber untuk satu target
Batasi jenis pencocokan rekaman untuk menyimpan semua catatan yang cocok di sumber untuk setiap rekaman yang cocok dalam target saat Anda membuat alur kerja pemetaan ID.	Pencocokan catatan terbatas and Banyak sumber untuk satu target

> **Note**
>
> Anda harus menentukan batasan yang kompatibel untuk ruang nama ID sumber dan target. Misalnya, jika namespace ID sumber membatasi aturan ke target tetapi namespace ID target membatasi aturan ke sumber, ini menghasilkan kesalahan.

9. Tentukan izin akses Layanan dengan memilih nama peran Layanan yang ada dari daftar tarik-turun.
10. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.
11. Pilih Buat namespace ID.

Target namespace ID dibuat. Setelah membuat ruang nama ID (sumber dan target) yang diperlukan untuk alur kerja pemetaan ID, Anda siap membuat alur kerja pemetaan ID.

Membuat target namespace ID (metode layanan penyedia)

Topik ini menjelaskan proses pembuatan target namespace ID menggunakan metode layanan Penyedia. Metode ini menggunakan layanan penyedia yang disebut LiveRamp. LiveRamp menerjemahkan data pihak ketiga yang dikodekan dari sumber ke target selama alur kerja pemetaan ID.

Untuk membuat target namespace ID (layanan penyedia)

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Persiapan data, pilih ruang nama ID.
3. Pada halaman ruang nama ID, di sudut kanan atas, pilih Buat namespace ID.
4. Untuk Detailnya, lakukan hal berikut:
   a. Untuk nama namespace ID, masukkan nama unik.
   b. (Opsional) Untuk Deskripsi, masukkan deskripsi opsional.
   c. Untuk jenis namespace ID, pilih Target.
5. Untuk metode namespace ID, pilih Layanan penyedia.

> **Note**
>
> Resolusi Entitas AWS saat ini menawarkan layanan LiveRamp penyedia sebagai metode namespace ID.
> Jika Anda memiliki langganan LiveRamp, maka status akan muncul sebagai Berlangganan.
> Untuk informasi selengkapnya tentang cara berlangganan LiveRamp, lihatLangkah 1: Berlangganan layanan penyedia di AWS Data Exchange.

6. Untuk domain Target, masukkan pengenal domain LiveRamp klien yang ditargetkan untuk transcoding yang LiveRamp menyediakan.
7. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.
8. Pilih Buat namespace ID.

Target namespace ID dibuat. Setelah Anda membuat ruang nama ID (sumber dan target) yang diperlukan untuk alur kerja pemetaan ID, Anda siap untuk Membuat alur kerja pemetaan ID.

Mengedit namespace ID

Anda hanya dapat mengedit namespace ID sebelum mengaitkannya ke alur kerja pemetaan ID. Setelah mengaitkan namespace ID ke alur kerja pemetaan ID, Anda tidak dapat mengeditnya.

Untuk mengedit namespace ID:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, di bawah Persiapan data, pilih ruang nama ID.
3. Pilih namespace ID.
4. Pilih Edit.
5. Pada halaman Namespace Edit ID, buat perubahan yang diperlukan lalu pilih Simpan.

Menghapus namespace ID

Anda tidak dapat menghapus namespace ID saat dikaitkan dengan alur kerja pemetaan ID. Anda harus terlebih dahulu menghapus pemetaan skema dari semua alur kerja pemetaan ID terkait sebelum Anda dapat menghapusnya.

Untuk menghapus namespace ID:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, di bawah Persiapan data, pilih ruang nama ID.
3. Pilih namespace ID.
4. Pilih Hapus.
5. Konfirmasikan penghapusan dan kemudian pilih Hapus.

Menambahkan atau memperbarui kebijakan sumber daya untuk namespace ID

Kebijakan sumber daya memungkinkan pembuat sumber daya pemetaan ID mengakses sumber daya namespace ID Anda.

Untuk menambah atau memperbarui kebijakan sumber daya

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih ruang nama ID.
3. Pilih namespace ID.
4. Pada halaman detail namespace ID, pilih tab Izin.
5. Di bagian Kebijakan sumber daya, pilih Edit.
6. Tambahkan atau perbarui kebijakan di JSON editor.
7. Pilih Simpan perubahan.

Cocokkan data input menggunakan alur kerja yang cocok

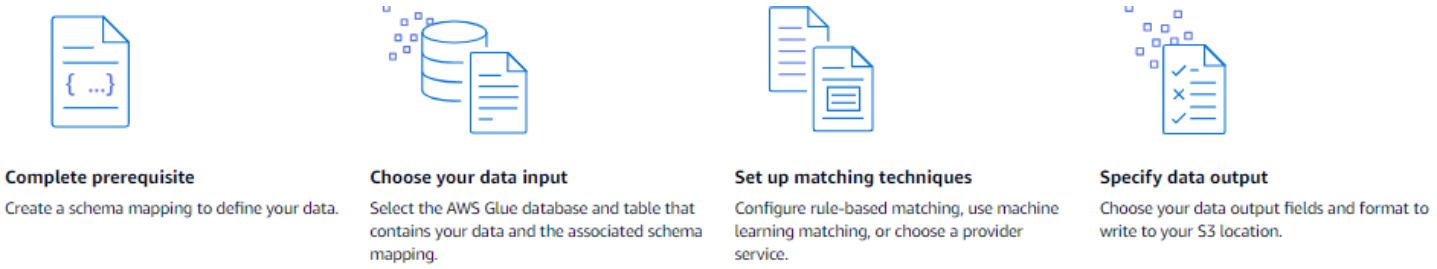
Alur kerja yang cocok adalah pekerjaan pemrosesan data yang menggabungkan dan membandingkan data dari sumber input yang berbeda dan menentukan mana yang cocok berdasarkan teknik pencocokan yang berbeda. Ini menghasilkan tabel output data.

Saat Anda membuat alur kerja yang cocok, pertama-tama Anda menentukan input data, langkah normalisasi, dan kemudian memilih teknik pencocokan dan output data yang Anda inginkan. Resolusi Entitas AWS membaca data Anda dari lokasi atau lokasi tertentu dan menemukan kecocokan antara dua atau lebih catatan dalam data Anda. Kemudian menetapkan ID Pencocokan ke catatan dalam kumpulan data yang cocok. Resolusi Entitas AWS kemudian menulis file keluaran data ke lokasi yang Anda pilih. Anda dapat menggunakan Resolusi Entitas AWS untuk hash data output jika diinginkan - membantu Anda mempertahankan kontrol atas data Anda.

Alur kerja yang cocok dapat memiliki beberapa proses dan hasilnya (keberhasilan atau kesalahan) ditulis ke folder dengan nama `jobId` sebagai.

Output data berisi file untuk kecocokan yang berhasil dan file untuk kesalahan. Output data dapat berisi beberapa bidang. Hasil yang berhasil ditulis ke `success` folder yang berisi banyak file, dan setiap file berisi subset dari catatan yang berhasil. Demikian pula, kesalahan ditulis ke `error` folder dengan beberapa bidang, dengan masing-masing berisi subset dari catatan kesalahan. Untuk informasi selengkapnya tentang kesalahan pemecahan masalah, lihat. Memecahkan masalah alur kerja yang cocok

Diagram berikut merangkum cara membuat alur kerja yang cocok.



Sebelum membuat alur kerja yang cocok, Anda harus terlebih dahulu membuat pemetaan skema. Untuk informasi selengkapnya, lihat Membuat pemetaan skema.

Ada tiga cara untuk membuat alur kerja yang cocok, berdasarkan teknik pencocokan: berbasis aturan, berbasispembelajaran mesin, atau berbasis layanan penyedia.

Setelah Anda membuat dan menjalankan alur kerja yang cocok, Anda dapat melakukan hal berikut:

- Lihat hasilnya di lokasi S3 yang Anda tentukan. Alur kerja yang cocok dihasilkan IDs setelah data diindeks.
- Gunakan output pencocokan berbasis aturan atau pencocokan pembelajaran mesin (ML) sebagai masukan untuk pencocokan berbasis layanan penyedia atau sebaliknya untuk memenuhi kebutuhan bisnis Anda.

Misalnya, untuk menghemat biaya berlangganan penyedia, Anda dapat menjalankan pencocokan berbasis aturan terlebih dahulu untuk menemukan kecocokan pada data Anda. Kemudian, Anda dapat mengirim subset catatan yang tak tertandingi ke pencocokan berbasis layanan penyedia.

Topik

Membuat alur kerja pencocokan berbasis aturan

Pencocokan berbasis aturan adalah seperangkat hierarkis aturan pencocokan air terjun, disarankan oleh Resolusi Entitas AWS, berdasarkan data yang Anda masukkan dan sepenuhnya dapat dikonfigurasi oleh Anda. Alur kerja pencocokan berbasis aturan memungkinkan Anda membandingkan cleartext atau data hash untuk menemukan kecocokan yang tepat berdasarkan kriteria yang Anda sesuaikan.

Ketika Resolusi Entitas AWS menemukan kecocokan antara dua atau lebih catatan dalam data Anda, ia menetapkan:

- ID Pencocokan dengan catatan dalam kumpulan data yang cocok
- Aturan Pertandingan yang menghasilkan pertandingan.

Untuk membuat alur kerja pencocokan berbasis aturan

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, di bawah Alur Kerja, pilih Pencocokan.
3. Pada halaman Pencocokan alur kerja, di sudut kanan atas, pilih Buat alur kerja yang cocok.
4. Untuk Langkah 1: Tentukan detail alur kerja yang cocok, lakukan hal berikut:

   a. Masukkan nama alur kerja yang cocok dan deskripsi opsional.

   b. Untuk input Data, pilih AWS Glue database dari dropdown, pilih AWS Glue tabel, dan kemudian pemetaan Skema yang sesuai.

      Anda dapat menambahkan hingga 19 input data.

   c. Opsi Normalisasi data dipilih secara default, sehingga input data dinormalisasi sebelum pencocokan. Jika Anda tidak ingin menormalkan data, batalkan pilihan opsi Normalisasi data.

   d. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.

Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-matching-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.

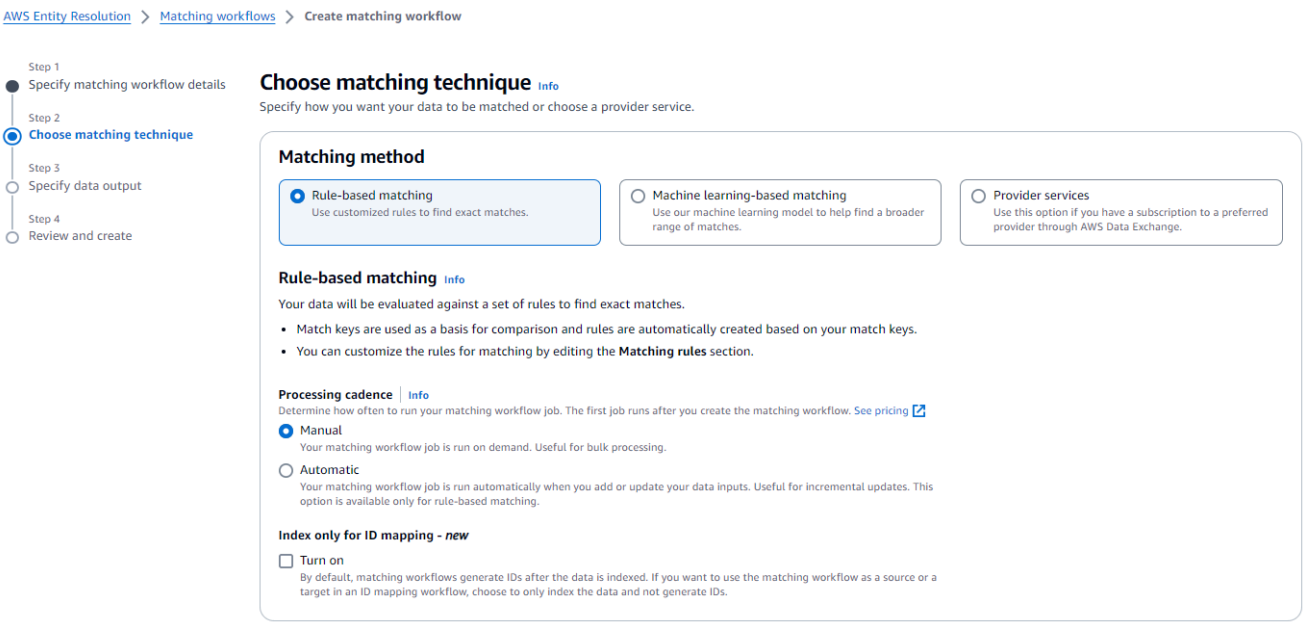
Opsi	Tindakan yang disarankan
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

e. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

f. Pilih Berikutnya.

5. Untuk Langkah 2: Pilih teknik pencocokan:

   a. Untuk metode Pencocokan, pilih Pencocokan berbasis aturan.



b. Untuk Memproses irama, pilih salah satu opsi berikut berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Jalankan alur kerja sesuai permintaan untuk pembaruan massal	Manual
Jalankan alur kerja segera setelah data baru ada di bucket S3 Anda	Otomatis

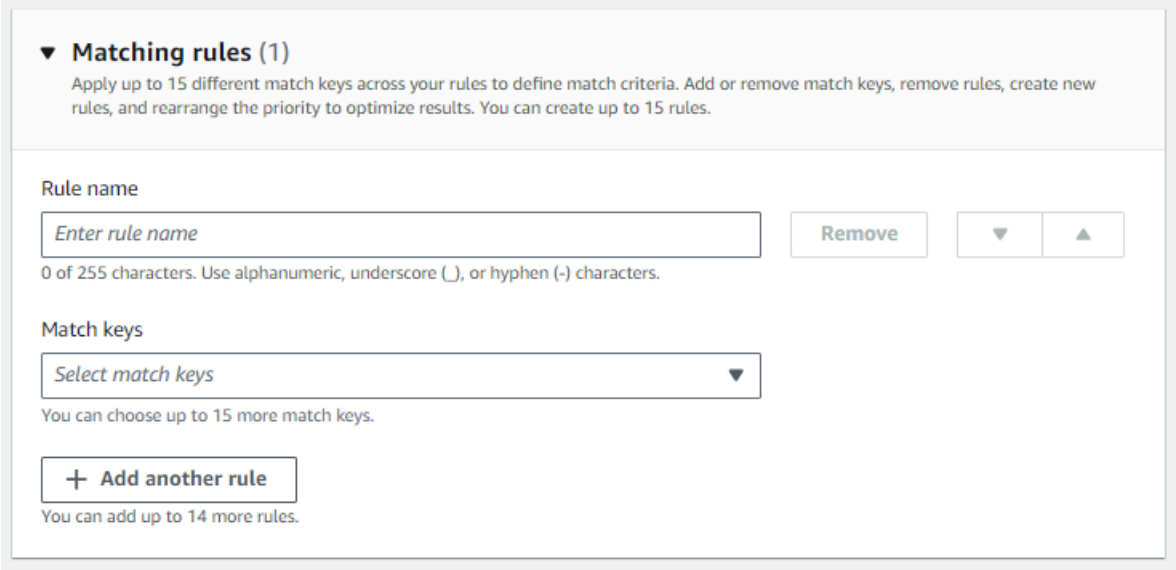
> **Note**
>
> Jika Anda memilih Otomatis, pastikan EventBridge notifikasi Amazon diaktifkan untuk bucket S3 Anda. Untuk petunjuk cara mengaktifkan Amazon EventBridge menggunakan konsol S3, lihat Mengaktifkan Amazon di Panduan EventBridge Pengguna Amazon S3.

c. (Opsional) Untuk Indeks hanya untuk pemetaan ID, Anda dapat memilih untuk Mengaktifkan kemampuan untuk hanya mengindeks data dan tidak menghasilkanIDs.

   Secara default, alur kerja yang cocok dihasilkan IDs setelah data diindeks.

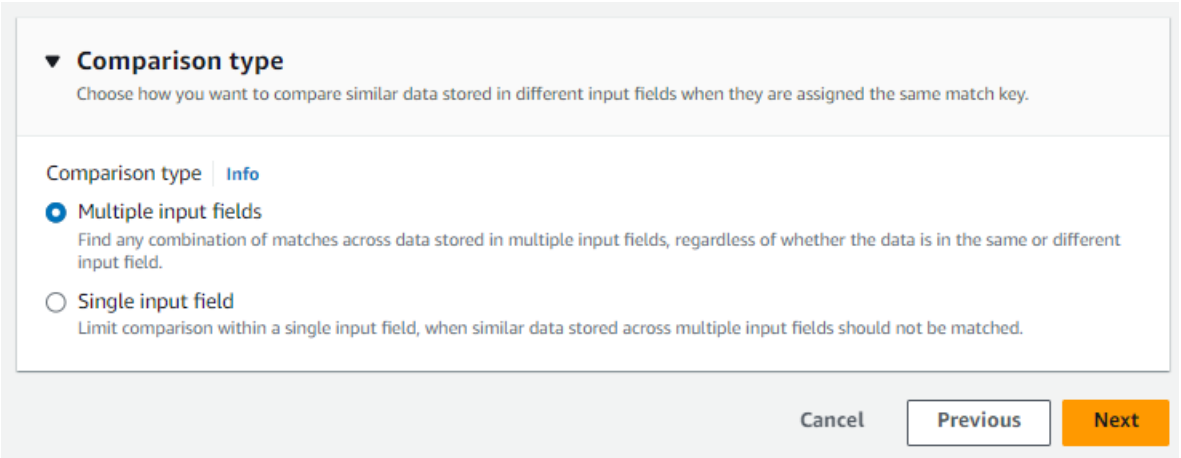
d. Untuk aturan Pencocokan, masukkan nama Aturan dan kemudian pilih tombol Cocokkan untuk aturan itu.

Anda dapat membuat hingga 15 aturan dan Anda dapat menerapkan hingga 15 kunci pencocokan yang berbeda di seluruh aturan Anda untuk menentukan kriteria kecocokan.



e. Untuk tipe Perbandingan, pilih salah satu opsi berikut berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Temukan kombinasi kecocokan di seluruh data yang disimpan di beberapa bidang input	Beberapa bidang masukan
Batasi perbandingan dengan satu bidang input	Bidang masukan tunggal



f. Pilih Berikutnya.

6. Untuk Langkah 3: Tentukan output dan format data:

   a. Untuk tujuan dan format keluaran Data, pilih lokasi Amazon S3 untuk output data dan apakah format Data akan menjadi Data yang dinormalisasi atau Data asli.

   b. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, masukkan AWS KMS kuncinyaARN.

   c. Lihat output yang dihasilkan Sistem.

   d. Untuk keluaran Data, tentukan bidang mana yang ingin Anda sertakan, sembunyikan, atau tutupi, lalu lakukan tindakan yang disarankan berdasarkan sasaran Anda.

Tujuan Anda	Opsi yang disarankan
Sertakan bidang	Pertahankan status output sebagai Termasuk.
Sembunyikan bidang (kecualikan dari output)	Pilih bidang Output, lalu pilih Sembunyikan.
Bidang topeng	Pilih bidang Output, dan kemudian pilih output Hash.
Setel ulang pengaturan sebelumnya	Pilih Reset.

   e. Pilih Berikutnya.

7. Untuk Langkah 4: Tinjau dan buat:

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat dan jalankan.

      Sebuah pesan muncul, menunjukkan bahwa alur kerja yang cocok telah dibuat dan bahwa pekerjaan telah dimulai.

8. Pada halaman detail alur kerja yang cocok, pada tab Metrik, lihat yang berikut ini di bawah Metrik pekerjaan terakhir:

   - ID Job.
   - Status pekerjaan alur kerja yang cocok: Antrian, Sedang berlangsung, Selesai, Gagal

- Waktu selesai untuk pekerjaan alur kerja.
- Jumlah Rekaman yang diproses.
- Jumlah Rekaman yang tidak diproses.
- Pertandingan Unik IDs yang dihasilkan.
- Jumlah catatan Input.

Anda juga dapat melihat metrik pekerjaan untuk mencocokkan pekerjaan alur kerja yang sebelumnya telah dijalankan di bawah riwayat Job.

9. Setelah pekerjaan alur kerja yang cocok selesai (Status Selesai), Anda dapat pergi ke tab Output data dan kemudian pilih lokasi Amazon S3 Anda untuk melihat hasilnya.
10. (Hanya jenis pemrosesan manual) Jika Anda telah membuat alur kerja pencocokan berbasis Aturan dengan jenis pemrosesan Manual, Anda dapat menjalankan alur kerja yang cocok kapan saja dengan memilih Jalankan alur kerja pada halaman detail alur kerja yang cocok.

Membuat alur kerja pencocokan berbasis pembelajaran mesin

Pencocokan berbasis pembelajaran mesin adalah proses preset yang mencoba mencocokkan catatan di semua data yang Anda masukkan. Alur kerja pencocokan berbasis pembelajaran mesin memungkinkan Anda membandingkan data cleartext untuk menemukan berbagai kecocokan menggunakan model pembelajaran mesin.

> **Note**
>
> Model pembelajaran mesin tidak mendukung perbandingan data hash.

Ketika Resolusi Entitas AWS menemukan kecocokan antara dua atau lebih catatan dalam data Anda, ia menetapkan:

- ID Pencocokan dengan catatan dalam kumpulan data yang cocok
- Persentase tingkat kepercayaan pertandingan.

Anda dapat menggunakan output alur kerja pencocokan berbasis ML sebagai masukan untuk pencocokan penyedia layanan data, atau sebaliknya untuk memenuhi tujuan spesifik Anda. Misalnya, Anda dapat menjalankan pencocokan berbasis ML untuk menemukan kecocokan di seluruh sumber

data pada catatan Anda sendiri terlebih dahulu. Jika subset tidak cocok, Anda dapat menjalankan pencocokan berbasis layanan penyedia untuk menemukan kecocokan tambahan.

Untuk membuat alur kerja pencocokan berbasis ML:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, di bawah Alur Kerja, pilih Pencocokan.
3. Pada halaman Pencocokan alur kerja, di sudut kanan atas, pilih Buat alur kerja yang cocok.
4. Untuk Langkah 1: Tentukan detail alur kerja yang cocok, lakukan hal berikut:

   a. Masukkan nama alur kerja yang cocok dan deskripsi opsional.

   b. Untuk input Data, pilih AWS Glue database dari dropdown, pilih AWS Glue tabel, dan kemudian pemetaan Skema yang sesuai.

      Anda dapat menambahkan hingga 20 input data.

   c. Opsi Normalisasi data dipilih secara default, sehingga input data dinormalisasi sebelum pencocokan. Jika Anda tidak ingin menormalkan data, batalkan pilihan opsi Normalisasi data.

      Pencocokan berbasis pembelajaran mesin hanya menormalkanNama,, Telepon dan. Email

   d. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.

Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-matching-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS

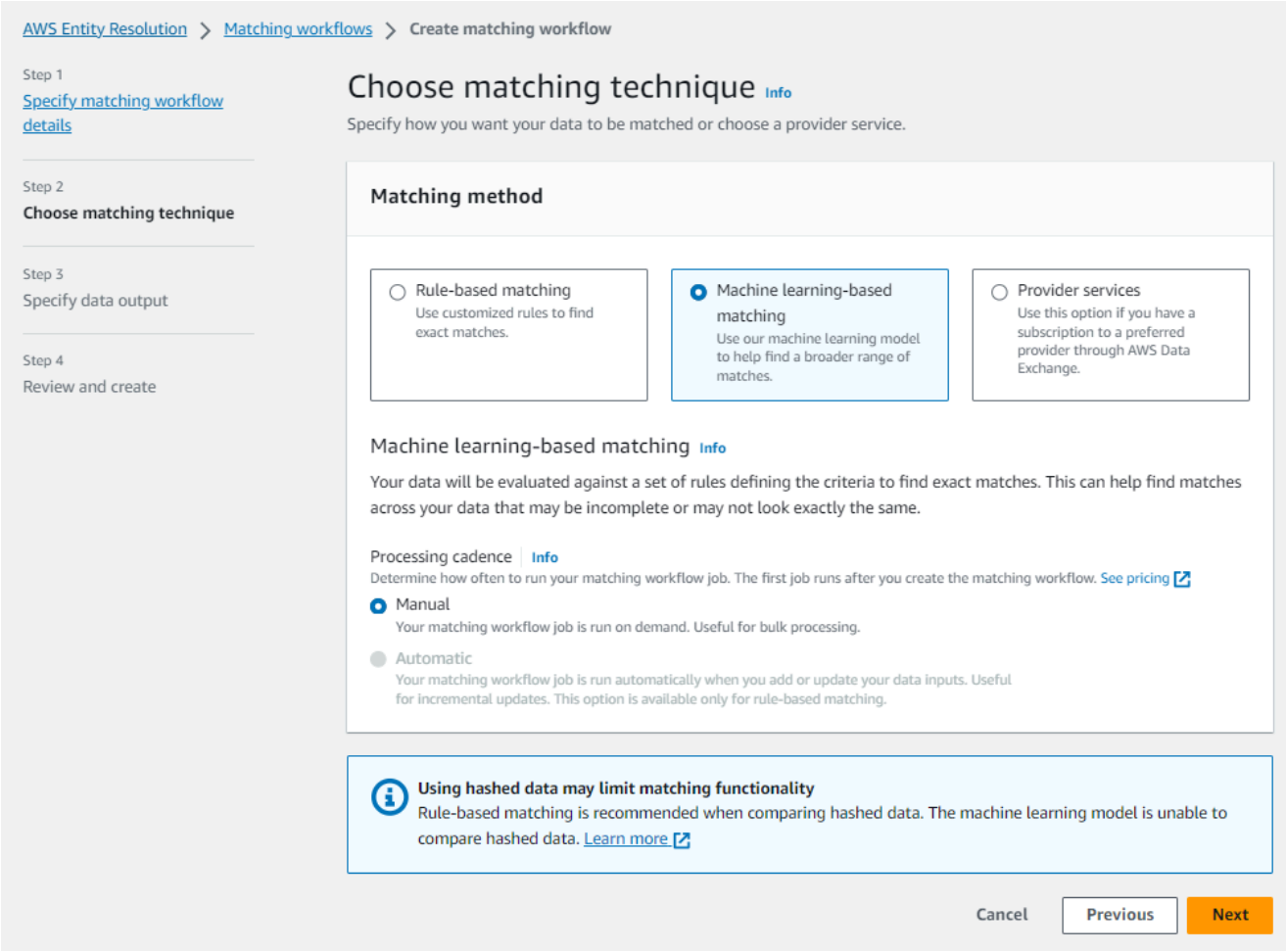
Opsi	Tindakan yang disarankan
	Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

e. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

f. Pilih Berikutnya.

5. Untuk Langkah 2: Pilih teknik pencocokan:

   a. Untuk metode Pencocokan, pilih Pencocokan berbasis pembelajaran mesin.



b. Untuk irama Pemrosesan, opsi Manual dipilih.

   Opsi ini memungkinkan Anda menjalankan alur kerja sesuai permintaan untuk pembaruan massal.

c. Pilih Berikutnya.

6. Untuk Langkah 3: Tentukan output dan format data:

   a. Untuk tujuan dan format keluaran Data, pilih lokasi Amazon S3 untuk output data dan apakah format Data akan menjadi Data yang dinormalisasi atau Data asli.

   b. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, masukkan AWS KMS kuncinyaARN.

   c. Lihat output yang dihasilkan Sistem.

   d. Untuk keluaran Data, tentukan bidang mana yang ingin Anda sertakan, sembunyikan, atau tutupi, lalu lakukan tindakan yang disarankan berdasarkan sasaran Anda.

Tujuan Anda	Opsi yang disarankan
Sertakan bidang	Pertahankan status output sebagai Termasuk.
Sembunyikan bidang (kecualikan dari output)	Pilih bidang Output, lalu pilih Sembunyikan.
Bidang topeng	Pilih bidang Output, dan kemudian pilih output Hash.
Setel ulang pengaturan sebelumnya	Pilih Reset.

e. Pilih Berikutnya.

7. Untuk Langkah 4: Tinjau dan buat:

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat dan jalankan.

      Sebuah pesan muncul, menunjukkan bahwa alur kerja yang cocok telah dibuat dan bahwa pekerjaan telah dimulai.

8. Pada halaman detail alur kerja yang cocok, pada tab Metrik, lihat yang berikut ini di bawah Metrik pekerjaan terakhir:

   - ID Job.
   - Status pekerjaan alur kerja yang cocok: Antrian, Sedang berlangsung, Selesai, Gagal
   - Waktu selesai untuk pekerjaan alur kerja.
   - Jumlah Rekaman yang diproses.
   - Jumlah Rekaman yang tidak diproses.
   - Pertandingan Unik IDs yang dihasilkan.
   - Jumlah catatan Input.

   Anda juga dapat melihat metrik pekerjaan untuk mencocokkan pekerjaan alur kerja yang sebelumnya telah dijalankan di bawah riwayat Job.

9. Setelah pekerjaan alur kerja yang cocok selesai (Status Selesai), Anda dapat pergi ke tab Output data dan kemudian pilih lokasi Amazon S3 Anda untuk melihat hasilnya.
10. (Hanya jenis pemrosesan manual) Jika Anda telah membuat alur kerja pencocokan berbasis pembelajaran Mesin dengan jenis pemrosesan Manual, Anda dapat menjalankan alur kerja yang cocok kapan saja dengan memilih Jalankan alur kerja pada halaman detail alur kerja yang cocok.

Membuat alur kerja pencocokan berbasis layanan penyedia

Pencocokan berbasis layanan penyedia memungkinkan Anda mencocokkan pengenal yang dikenal dengan penyedia layanan data pilihan Anda.

Resolusi Entitas AWS saat ini mendukung layanan penyedia data berikut:

- LiveRamp
- TransUnion
- ID Terpadu 2.0

Untuk informasi selengkapnya tentang layanan penyedia yang didukung, lihatMempersiapkan data input pihak ketiga.

Anda dapat menggunakan langganan publik untuk penyedia ini AWS Data Exchange atau menegosiasikan penawaran pribadi langsung dengan penyedia data. Untuk informasi selengkapnya tentang membuat langganan baru atau menggunakan kembali langganan yang sudah ada ke layanan penyedia, lihatLangkah 1: Berlangganan layanan penyedia di AWS Data Exchange.

Bagian berikut menjelaskan cara membuat alur kerja pencocokan berbasis penyedia.

Topik

- Membuat alur kerja yang cocok dengan LiveRamp
- Membuat alur kerja yang cocok dengan TransUnion
- Membuat alur kerja yang cocok dengan 2.0 UID

Membuat alur kerja yang cocok dengan LiveRamp

Jika Anda memiliki langganan ke LiveRamp layanan, Anda dapat membuat alur kerja yang cocok dengan LiveRamp layanan untuk melakukan resolusi identitas.

LiveRamp Layanan ini menyediakan pengenal yang disebut rampID. RampID adalah salah satu yang paling umum digunakan IDs dalam platform sisi permintaan untuk menciptakan audiens untuk kampanye iklan. Dengan menggunakan alur kerja yang cocok LiveRamp, Anda dapat menyelesaikan alamat email yang di-hash. RAMPIDs

> **Note**
>
> Resolusi Entitas AWS mendukung PII penugasan rampID berbasis.

Alur kerja ini memerlukan bucket pementasan data Amazon S3 tempat Anda ingin output alur kerja yang cocok ditulis sementara. Sebelum membuat alur kerja pemetaan ID dengan LiveRamp, tambahkan izin berikut ke bucket pementasan data.

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

Ganti masing-masing *<user input placeholder>* dengan informasi Anda sendiri.

staging-bucket	Bucket Amazon S3 yang menyimpan sementara data Anda saat menjalankan alur kerja berbasis layanan penyedia.

Untuk membuat alur kerja yang cocok dengan LiveRamp:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, di bawah Alur Kerja, pilih Pencocokan.
3. Pada halaman Pencocokan alur kerja, di sudut kanan atas, pilih Buat alur kerja yang cocok.
4. Untuk Langkah 1: Tentukan detail alur kerja yang cocok, lakukan hal berikut:

    a. Masukkan nama alur kerja yang cocok dan deskripsi opsional.

    b. Untuk input Data, pilih AWS Glue database dari dropdown, pilih AWS Glue tabel, lalu pilih pemetaan Skema yang sesuai.

    Anda dapat menambahkan hingga 20 input data.

    c. Opsi Normalisasi data dipilih secara default, sehingga input data dinormalisasi sebelum pencocokan.

Jika Anda menggunakan proses resolusi email saja, batalkan pilihan Normalisasi data opsi, karena hanya email hash yang digunakan untuk memasukkan data.

d. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.

Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-matching-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.

Opsi	Tindakan yang disarankan
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

e. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

f. Pilih Berikutnya.

5. Untuk Langkah 2: Pilih teknik pencocokan:

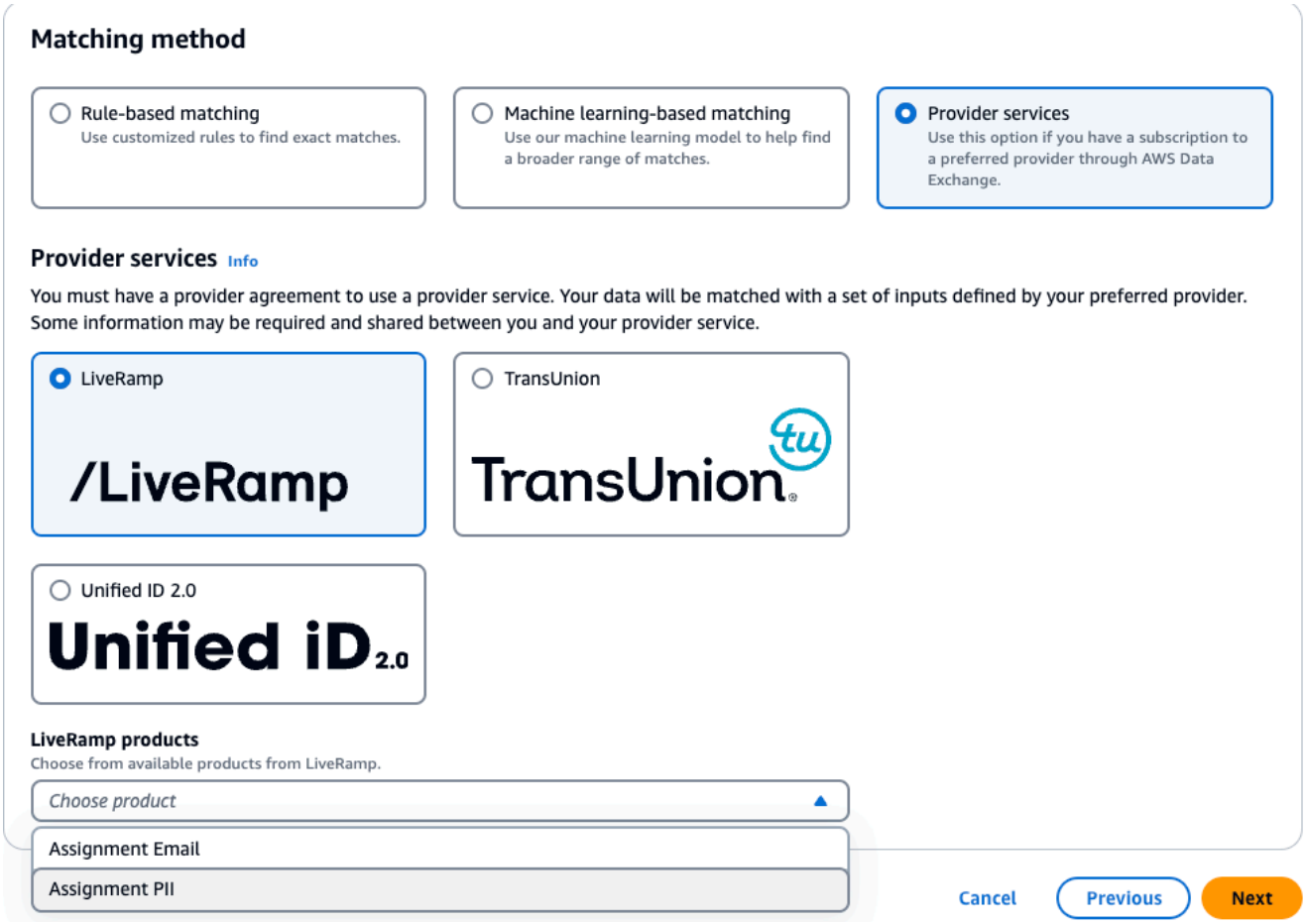
a. Untuk metode Pencocokan, pilih Layanan penyedia.

b. Untuk layanan Penyedia, pilih LiveRamp.

> **Note**
>
> Pastikan format file input data dan normalisasi selaras dengan pedoman layanan penyedia.

Untuk informasi selengkapnya tentang pedoman pemformatan file masukan untuk alur kerja yang cocok, lihat Melakukan Resolusi Identitas Melalui ADX dalam dokumentasi. LiveRamp

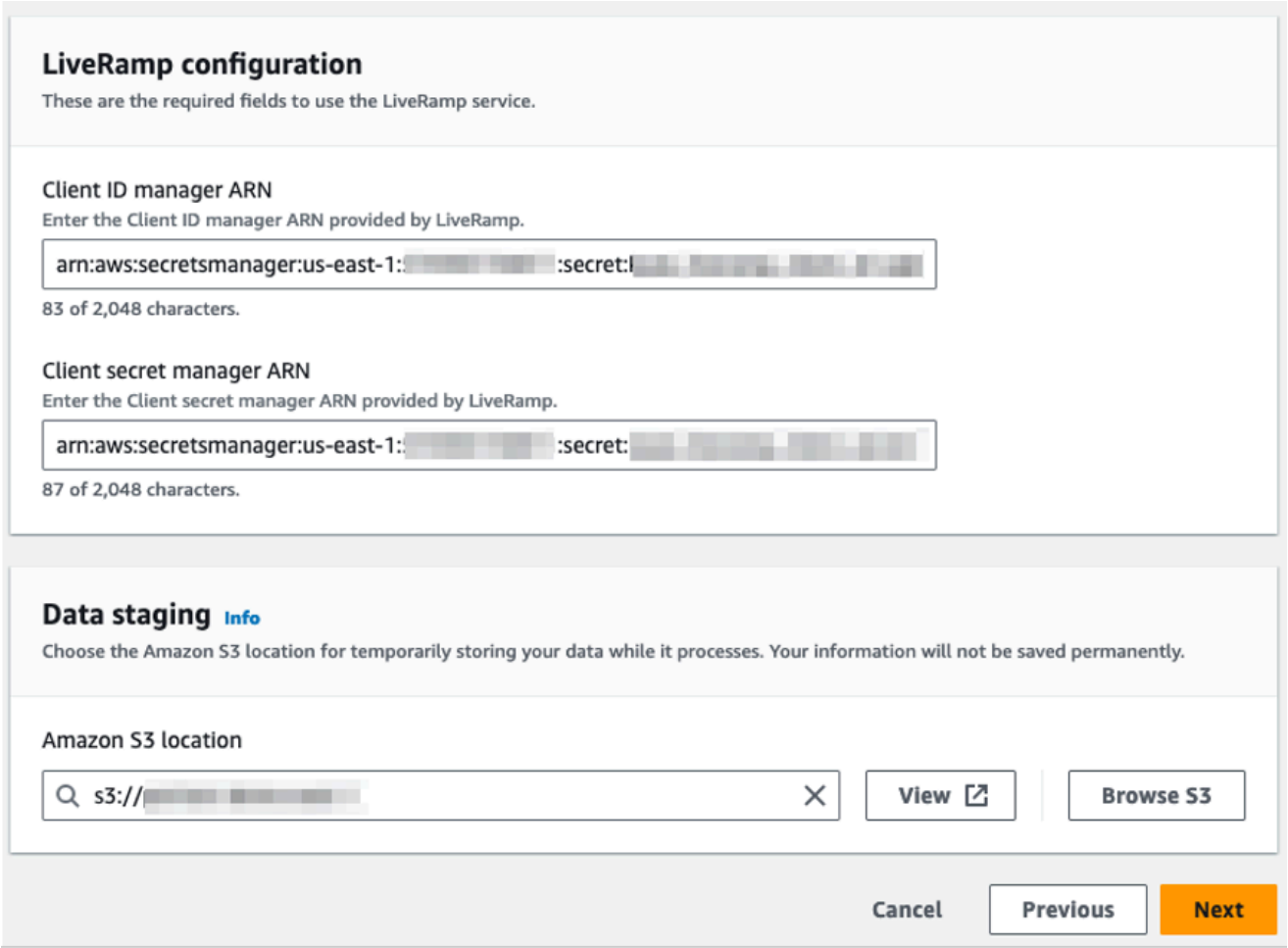
c. Untuk LiveRamp produk, pilih produk dari daftar dropdown.



Note

Jika Anda memilih PenugasanPII, maka Anda harus menyediakan setidaknya satu kolom non-pengenal saat melakukan resolusi entitas. Misalnya,GENDER.

d. Untuk LiveRamp konfigurasi, masukkan manajer ID Klien ARN dan manajer rahasia Klien ARN.



e. Untuk pementasan Data, pilih lokasi Amazon S3 untuk penyimpanan sementara data Anda saat diproses.

   Anda harus memiliki izin untuk pementasan data lokasi Amazon S3. Untuk informasi selengkapnya, lihat Membuat peran pekerjaan alur kerja untuk Resolusi Entitas AWS.

f. Pilih Berikutnya.

6. Untuk Langkah 3: Tentukan output data:

   a. Untuk tujuan dan format keluaran Data, pilih lokasi Amazon S3 untuk output data dan apakah format Data akan menjadi Data yang dinormalisasi atau Data asli.

   b. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, masukkan AWS KMS kuncinyaARN.

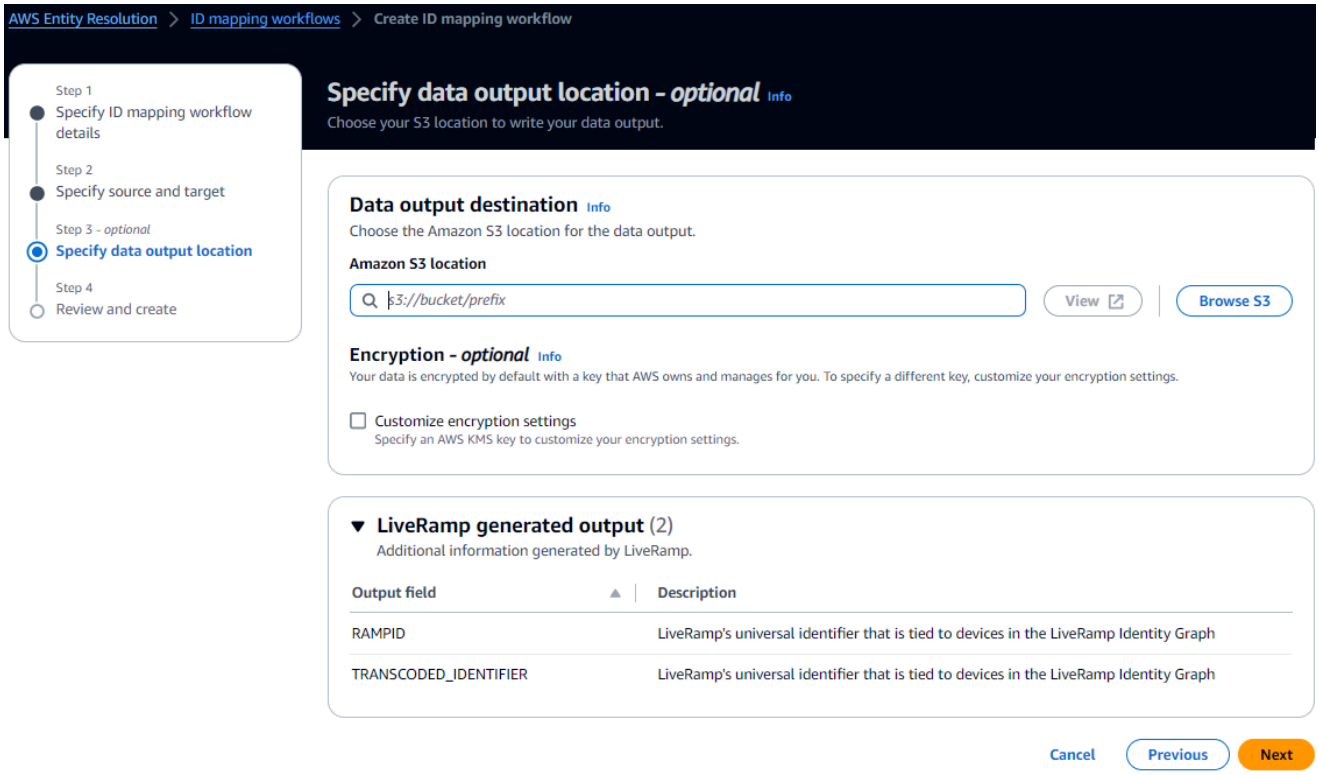
   c. Lihat output LiveRamp yang dihasilkan.

      Ini adalah informasi tambahan yang dihasilkan oleh LiveRamp.

d. Untuk keluaran Data, tentukan bidang mana yang ingin Anda sertakan, sembunyikan, atau tutupi, lalu lakukan tindakan yang disarankan berdasarkan sasaran Anda.

> **Note**
>
> Jika Anda telah memilih LiveRamp, karena filter LiveRamp privasi yang menghapus Informasi Identifikasi Pribadi (PII), beberapa bidang akan menampilkan status Keluaran Tidak Tersedia.

Tujuan Anda	Opsi yang disarankan
Sertakan bidang	Pertahankan status output sebagai Termasuk.
Sembunyikan bidang (kecualikan dari output)	Pilih bidang Output, lalu pilih Sembunyikan.
Bidang topeng	Pilih bidang Output, dan kemudian pilih output Hash.
Setel ulang pengaturan sebelumnya	Pilih Reset.



e. Pilih Berikutnya.

7. Untuk Langkah 4: Tinjau dan buat:

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat dan jalankan.

      Sebuah pesan muncul, menunjukkan bahwa alur kerja yang cocok telah dibuat dan bahwa pekerjaan telah dimulai.

8. Pada halaman detail alur kerja yang cocok, pada tab Metrik, lihat yang berikut ini di bawah Metrik pekerjaan terakhir:

   - ID Job.
   - Status pekerjaan alur kerja yang cocok: Antrian, Sedang berlangsung, Selesai, Gagal
   - Waktu selesai untuk pekerjaan alur kerja.
   - Jumlah Rekaman yang diproses.
   - Jumlah Rekaman yang tidak diproses.
   - Pertandingan Unik IDs yang dihasilkan.
   - Jumlah catatan Input.

Anda juga dapat melihat metrik pekerjaan untuk mencocokkan pekerjaan alur kerja yang sebelumnya telah dijalankan di bawah riwayat Job.

9. Setelah pekerjaan alur kerja yang cocok selesai (Status Selesai), Anda dapat pergi ke tab Output data dan kemudian pilih lokasi Amazon S3 Anda untuk melihat hasilnya.

Membuat alur kerja yang cocok dengan TransUnion

Jika Anda berlangganan TransUnion layanan, Anda dapat meningkatkan pemahaman pelanggan dengan menautkan, mencocokkan, dan meningkatkan catatan terkait pelanggan yang disimpan di saluran yang berbeda dengan TransUnion Person and Household E Keys dan lebih dari 200 atribut data.

TransUnion Layanan ini menyediakan pengidentifikasi yang dikenal sebagai TransUnion Individu dan Rumah TanggaIDs. TransUnion memberikan penugasan ID (juga dikenal sebagai pengkodean) pengidentifikasi yang dikenal seperti nama, alamat, nomor telepon, dan alamat email.

Alur kerja ini memerlukan bucket pementasan data Amazon S3 tempat Anda ingin output alur kerja yang cocok ditulis sementara. Sebelum membuat alur kerja yang cocok dengan TransUnion, tambahkan izin berikut ke bucket pementasan data.

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

Ganti masing-masing *<user input placeholder>* dengan informasi Anda sendiri.

staging-bucket	Bucket Amazon S3 yang menyimpan sementara data Anda saat menjalankan alur kerja berbasis layanan penyedia.

Untuk membuat alur kerja yang cocok dengan TransUnion:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, di bawah Alur Kerja, pilih Pencocokan.
3. Pada halaman Pencocokan alur kerja, di sudut kanan atas, pilih Buat alur kerja yang cocok.
4. Untuk Langkah 1: Tentukan detail alur kerja yang cocok, lakukan hal berikut:
    a. Masukkan nama alur kerja yang cocok dan deskripsi opsional.
    b. Untuk input Data, pilih AWS Glue database dari dropdown, pilih AWS Glue tabel, lalu pilih pemetaan Skema yang sesuai.

Anda dapat menambahkan hingga 20 input data.

c. Opsi Normalisasi data dipilih secara default, sehingga input data dinormalisasi sebelum pencocokan. Jika Anda tidak ingin menormalkan data, batalkan pilihan opsi Normalisasi data.

d. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.

Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-matching-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.

Opsi	Tindakan yang disarankan
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

e. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

f. Pilih Berikutnya.

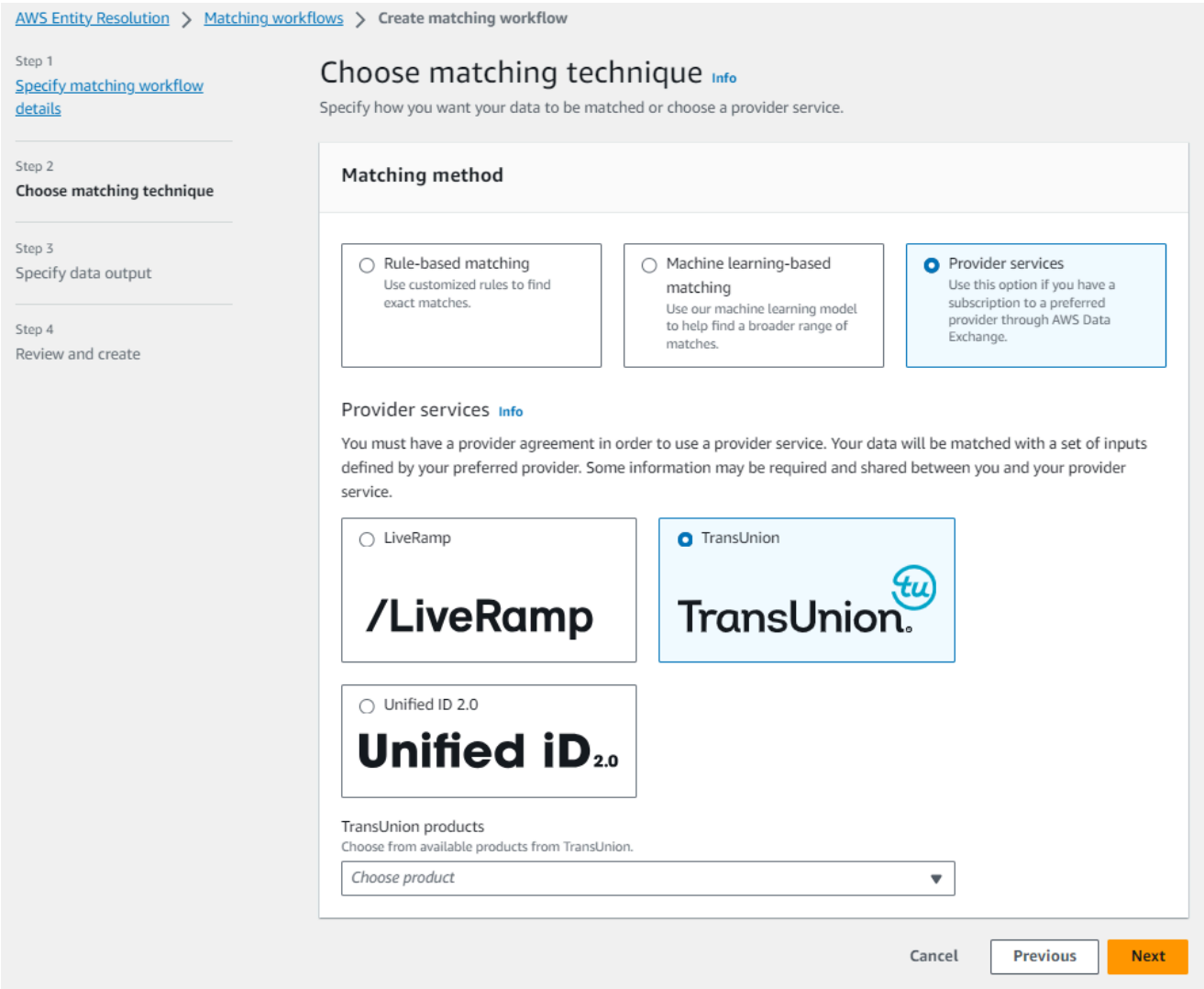
5. Untuk Langkah 2: Pilih teknik pencocokan:

a. Untuk metode Pencocokan, pilih Layanan penyedia.

b. Untuk layanan Penyedia, pilih TransUnion.

> **Note**
>
> Pastikan format file input data dan normalisasi selaras dengan pedoman layanan penyedia.

c. Untuk TransUnion produk, pilih produk dari daftar dropdown.



d. Untuk pementasan Data, pilih lokasi Amazon S3 untuk penyimpanan sementara data Anda saat diproses.

   Anda harus memiliki izin untuk pementasan data lokasi Amazon S3. Untuk informasi selengkapnya, lihat the section called “Membuat peran pekerjaan alur kerja”.

6. Pilih Berikutnya.
7. Untuk Langkah 3: Tentukan output data:

   a. Untuk tujuan dan format keluaran Data, pilih lokasi Amazon S3 untuk output data dan apakah format Data akan menjadi Data yang dinormalisasi atau Data asli.

   b. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, masukkan AWS KMS kuncinyaARN.

c. Lihat output TransUnion yang dihasilkan.

   Ini adalah informasi tambahan yang dihasilkan oleh TransUnion.

d. Untuk keluaran Data, tentukan bidang mana yang ingin Anda sertakan, sembunyikan, atau tutupi, lalu lakukan tindakan yang disarankan berdasarkan sasaran Anda.

Tujuan Anda	Opsi yang disarankan
Sertakan bidang	Pertahankan status output sebagai Termasuk.
Sembunyikan bidang (kecualikan dari output)	Pilih bidang Output, lalu pilih Sembunyikan.
Bidang topeng	Pilih bidang Output, dan kemudian pilih output Hash.
Setel ulang pengaturan sebelumnya	Pilih Reset.

e. Untuk keluaran yang dihasilkan Sistem, lihat semua bidang yang disertakan.

f. Pilih Berikutnya.

8. Untuk Langkah 4: Tinjau dan buat:

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat dan jalankan.

      Sebuah pesan muncul, menunjukkan bahwa alur kerja yang cocok telah dibuat dan bahwa pekerjaan telah dimulai.

9. Pada halaman detail alur kerja yang cocok, pada tab Metrik, lihat yang berikut ini di bawah Metrik pekerjaan terakhir:

   - ID Job.
   - Status pekerjaan alur kerja yang cocok: Antrian, Sedang berlangsung, Selesai, Gagal
   - Waktu selesai untuk pekerjaan alur kerja.
   - Jumlah Rekaman yang diproses.
   - Jumlah Rekaman yang tidak diproses.
   - Pertandingan Unik IDs yang dihasilkan.

- Jumlah catatan Input.

Anda juga dapat melihat metrik pekerjaan untuk mencocokkan pekerjaan alur kerja yang sebelumnya telah dijalankan di bawah riwayat Job.

10. Setelah pekerjaan alur kerja yang cocok selesai (Status Selesai), Anda dapat pergi ke tab Output data dan kemudian pilih lokasi Amazon S3 Anda untuk melihat hasilnya.

Membuat alur kerja yang cocok dengan 2.0 UID

Jika Anda berlangganan layanan Unified ID 2.0, Anda dapat mengaktifkan kampanye iklan dengan identitas deterministik dan bersandar pada interoperabilitas dengan banyak peserta yang UID2 diaktifkan di seluruh ekosistem periklanan. Untuk informasi selengkapnya, lihat Ikhtisar Unified ID 2.0.

Layanan Unified ID 2.0 menyediakan UID 2 mentah, yang digunakan untuk membangun kampanye iklan di platform The Trade Desk. UID2.0 dihasilkan menggunakan kerangka open source.

Dalam satu alur kerja Anda dapat menggunakan salah satu **`Email Address`** atau **`Phone number`** untuk UID2 generasi mentah tetapi tidak keduanya. Jika keduanya hadir dalam pemetaan skema, maka alur kerja akan memilih **`Email Address`** dan **`Phone number`** akan menjadi bidang pass-through. Untuk mendukung keduanya, buat pemetaan skema baru di mana dipetakan tetapi **`Email Address`** tidak **`Phone number`** dipetakan. Kemudian, buat alur kerja kedua menggunakan pemetaan skema baru ini.

> **Note**
>
> Mentah UID2s dibuat dengan menambahkan garam dari ember garam yang diputar kira-kira setahun sekali, UID2 menyebabkan bahan mentah juga diputar dengannya. Oleh karena itu, disarankan agar Anda menyegarkan mentah UID2s setiap hari. Untuk informasi selengkapnya, lihat https://unifiedid.com/docs/getting-started/gs-faqs# 2 -incremental-updates how-often-should-uid. s-be-refreshed-for

Untuk membuat alur kerja yang cocok dengan UID 2.0:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, di bawah Alur Kerja, pilih Pencocokan.

3. Pada halaman Pencocokan alur kerja, di sudut kanan atas, pilih Buat alur kerja yang cocok.
4. Untuk Langkah 1: Tentukan detail alur kerja yang cocok, lakukan hal berikut:

   a. Masukkan nama alur kerja yang cocok dan deskripsi opsional.

   b. Untuk input Data, pilih AWS Glue database dari dropdown, pilih AWS Glue tabel, lalu pilih pemetaan Skema yang sesuai.

      Anda dapat menambahkan hingga 20 input data.

   c. Biarkan opsi Normalisasi data dipilih, sehingga input data (**`Email Address`**atau**`Phone number`**) dinormalisasi sebelum pencocokan.

      Untuk informasi selengkapnya tentang **`Email Address`** normalisasi, lihat Normalisasi Alamat Email dalam dokumentasi UID 2.0.

      Untuk informasi selengkapnya tentang **`Phone number`** normalisasi, lihat Normalisasi Nomor Telepon di dokumentasi UID 2.0.

   d. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.

Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-matching-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun.

Opsi	Tindakan yang disarankan
	Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

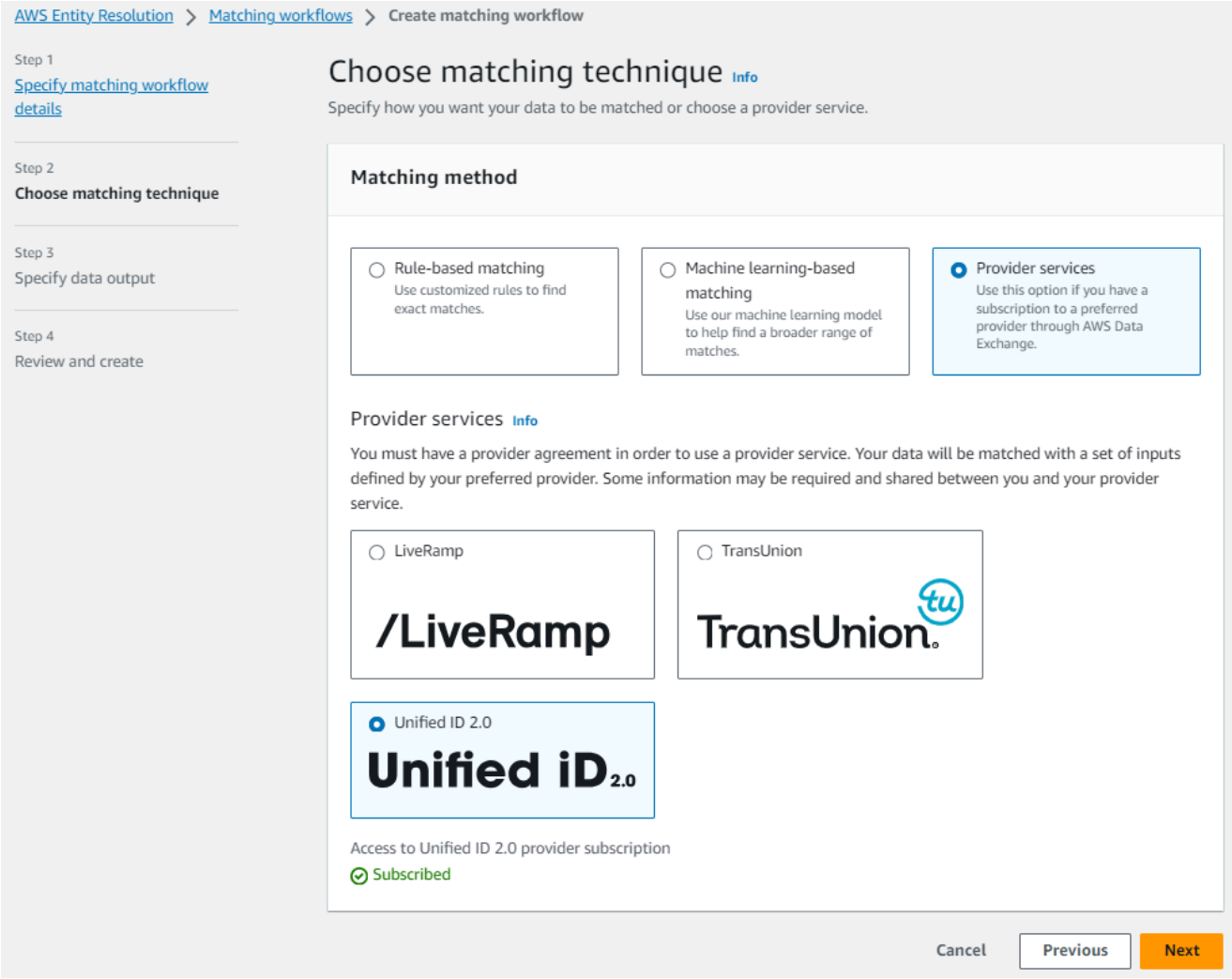
e. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

f. Pilih Berikutnya.

5. Untuk Langkah 2: Pilih teknik pencocokan:

a. Untuk metode Pencocokan, pilih Layanan penyedia.

b. Untuk layanan Penyedia, pilih Unified ID 2.0.



c. Pilih Berikutnya.

6. Untuk Langkah 3: Tentukan output data:

   a. Untuk tujuan dan format keluaran Data, pilih lokasi Amazon S3 untuk output data dan apakah format Data akan menjadi Data yang dinormalisasi atau Data asli.

   b. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, masukkan AWS KMS kuncinyaARN.

   c. Lihat keluaran Unified ID 2.0 yang dihasilkan.

      Ini adalah daftar semua informasi tambahan yang dihasilkan oleh UID 2.0

   d. Untuk keluaran Data, tentukan bidang mana yang ingin Anda sertakan, sembunyikan, atau tutupi, lalu lakukan tindakan yang disarankan berdasarkan sasaran Anda.

Tujuan Anda	Opsi yang disarankan
Sertakan bidang	Pertahankan status output sebagai Termasuk.
Sembunyikan bidang (kecualikan dari output)	Pilih bidang Output, lalu pilih Sembunyikan.
Bidang topeng	Pilih bidang Output, dan kemudian pilih output Hash.
Setel ulang pengaturan sebelumnya	Pilih Reset.

e. Untuk keluaran yang dihasilkan Sistem, lihat semua bidang yang disertakan.

f. Pilih Berikutnya.

7. Untuk Langkah 4: Tinjau dan buat:

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat dan jalankan.

      Sebuah pesan muncul, menunjukkan bahwa alur kerja yang cocok telah dibuat dan bahwa pekerjaan telah dimulai.

8. Pada halaman detail alur kerja yang cocok, pada tab Metrik, lihat yang berikut ini di bawah Metrik pekerjaan terakhir:

   - ID Job.
   - Status pekerjaan alur kerja yang cocok: Antrian, Sedang berlangsung, Selesai, Gagal
   - Waktu selesai untuk pekerjaan alur kerja.
   - Jumlah Rekaman yang diproses.
   - Jumlah Rekaman yang tidak diproses.
   - Pertandingan Unik IDs yang dihasilkan.
   - Jumlah catatan Input.

   Anda juga dapat melihat metrik pekerjaan untuk mencocokkan pekerjaan alur kerja yang sebelumnya telah dijalankan di bawah riwayat Job.

9. Setelah pekerjaan alur kerja yang cocok selesai (Status Selesai), Anda dapat pergi ke tab Output data dan kemudian pilih lokasi Amazon S3 Anda untuk melihat hasilnya.

Mengedit alur kerja yang cocok

Mengedit alur kerja yang cocok memungkinkan Anda untuk menjaga proses resolusi entitas Anda up-to-date dan responsif terhadap perubahan persyaratan organisasi Anda dari waktu ke waktu. Anda mungkin ingin menyesuaikan kriteria, teknik, atau keluaran data yang cocok untuk meningkatkan akurasi dan efisiensi proses resolusi entitas. Jika Anda mengidentifikasi masalah atau kesalahan dalam hasil alur kerja saat ini, mengeditnya dapat membantu Anda mendiagnosis dan menyelesaikan masalah tersebut.

Untuk mengedit alur kerja yang cocok:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur Kerja, pilih Pencocokan.
3. Pilih alur kerja yang cocok.
4. Pada halaman detail alur kerja yang cocok, di sudut kanan atas, pilih Edit.
5. Pada halaman Tentukan detail alur kerja yang cocok, buat perubahan yang diperlukan lalu pilih Berikutnya.
6. Pada halaman Pilih teknik pencocokan, buat perubahan yang diperlukan dan kemudian pilih Berikutnya.
7. Pada halaman Tentukan keluaran data, buat perubahan yang diperlukan lalu pilih Berikutnya.
8. Pada halaman Tinjau dan simpan, buat perubahan yang diperlukan lalu pilih Simpan.

Menghapus alur kerja yang cocok

Jika alur kerja yang cocok tidak lagi digunakan atau sudah usang, menghapusnya dapat membantu menjaga ruang kerja Anda tetap teratur dan rapi. Jika Anda telah mengembangkan alur kerja baru yang ditingkatkan yang menggantikan yang lebih lama, menghapus alur kerja lama dapat membantu memastikan Anda hanya menggunakan sebagian besar proses. up-to-date

Untuk menghapus alur kerja yang cocok:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur Kerja, pilih Pencocokan.
3. Pilih alur kerja yang cocok.
4. Pada halaman detail alur kerja yang cocok, di sudut kanan atas, pilih Hapus.
5. Konfirmasikan penghapusan dan kemudian pilih Hapus.

Menemukan ID Pencocokan untuk alur kerja pencocokan berbasis aturan

Setelah menjalankan alur kerja pencocokan berbasis aturan, Anda dapat menemukan ID Pencocokan yang sesuai dan aturan terkait untuk catatan yang diproses.

Untuk menemukan ID Pencocokan untuk alur kerja pencocokan berbasis aturan:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur Kerja, pilih Pencocokan.
3. Pilih alur kerja pencocokan berbasis aturan yang telah diproses (Status Job Selesai).
4. Pada halaman detail alur kerja yang cocok, pilih tab Temukan ID kecocokan.
5. Lakukan salah satu hal berikut ini:

Jika...	Lalu...
Hanya ada satu pemetaan skema yang terkait dengan alur kerja ini.	Lihat pemetaan Skema yang dipilih secara default.
Ada lebih dari satu pemetaan skema yang terkait dengan alur kerja ini.	Pilih pemetaan Skema dari daftar dropdown.

6. Perluas aturan Pencocokan.
7. Masukkan Nilai untuk setiap tombol Match.

Opsi Normalisasi data dipilih secara default, sehingga input data dinormalisasi sebelum pencocokan. Jika Anda tidak ingin menormalkan data, batalkan pilihan opsi Normalisasi data.

> **Tip**
>
> Masukkan nilai sebanyak yang Anda bisa untuk membantu menemukan ID Pencocokan.

8. Pilih Lihat.
9. Lihat ID Pencocokan yang sesuai dan aturan terkait yang digunakan untuk pencocokan.

Menghapus catatan dari alur kerja pencocokan berbasis aturan atau berbasis ML

Jika Anda perlu mematuhi peraturan manajemen data, Anda dapat menghapus catatan dari alur kerja pencocokan berbasis aturan atau berbasis ML.

Untuk menghapus catatan dari alur kerja pencocokan berbasis aturan atau berbasis ML

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur Kerja, pilih Pencocokan.
3. Pilih alur kerja pencocokan berbasis aturan atau berbasis ML.
4. Pada halaman detail alur kerja yang cocok, pilih Hapus unik IDs dari daftar dropdown Tindakan.
5. Masukkan ID unik yang ingin Anda hapus di IDs bagian Unik.

   Anda dapat memasukkan hingga 10 unikIDs.
6. Tentukan sumber Input dari mana untuk menghapus unikIDs.

   Jika hanya ada satu sumber Input untuk alur kerja, sumber Input dicantumkan secara default.

   Jika Anda hanya menentukan satu sumber Input, keunikan IDs di sumber input lain tidak akan terpengaruh.
7. Pilih Hapus unik IDs.

Memecahkan masalah alur kerja yang cocok

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat menjalankan alur kerja yang cocok.

Saya menerima file kesalahan setelah menjalankan alur kerja yang cocok

Penyebab umum

Alur kerja yang cocok dapat memiliki beberapa proses dan hasilnya (keberhasilan atau kesalahan) ditulis ke folder dengan nama `jobId` sebagai.

Hasil yang berhasil untuk alur kerja yang cocok ditulis ke `success` folder yang berisi banyak file, dan setiap file berisi subset dari catatan yang berhasil.

Kesalahan untuk alur kerja yang cocok ditulis ke `error` folder dengan beberapa bidang, dengan masing-masing berisi subset catatan kesalahan.

File kesalahan dapat dibuat karena alasan berikut:

- ID Unik adalah:
  - null
  - hilang dalam deretan data
  - hilang dalam catatan di tabel data
  - diulang di baris data lain dalam tabel data
  - tidak ditentukan
  - tidak unik dalam sumber yang sama
  - tidak unik di berbagai sumber
  - tumpang tindih antar sumber
  - melebihi 38 karakter (hanya alur kerja pencocokan berbasis aturan)
- Salah satu bidang dalam pemetaan skema menyertakan nama yang dicadangkan:
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - MatchID
  - HashingProtocol

- ConfidenceLevel
- Sumber

> **Note**
>
> Jika catatan dalam file kesalahan dibuat karena alasan yang tercantum sebelumnya, Anda dikenakan biaya, karena menimbulkan biaya pemrosesan untuk layanan. Jika catatan dalam file kesalahan disebabkan oleh kesalahan server internal, Anda tidak dikenakan biaya.

Resolusi

Untuk mengatasi masalah ini

1. Periksa untuk melihat apakah ID Unik valid.

   Jika ID Unik tidak valid, perbarui ID Unik di tabel data Anda, simpan tabel data baru, buat pemetaan skema baru, dan jalankan alur kerja yang cocok lagi.
2. Periksa apakah salah satu bidang dalam pemetaan skema menyertakan nama cadangan.

   Jika salah satu bidang menyertakan nama cadangan, buat pemetaan skema baru dengan nama baru, dan jalankan alur kerja yang cocok lagi.

Memetakan data masukan menggunakan alur kerja pemetaan ID

Alur kerja pemetaan ID adalah pekerjaan pemrosesan data yang memetakan data dari sumber data input ke target data input berdasarkan metode pemetaan ID yang ditentukan. Ini menghasilkan tabel pemetaan ID.

Alur kerja pemetaan ID memerlukan sumber data input dan target data input. Sumber dan target input data Anda bergantung pada jenis pemetaan ID yang ingin Anda lakukan. Ada dua cara untuk melakukan pemetaan ID: layanan berbasis aturan atau penyedia:

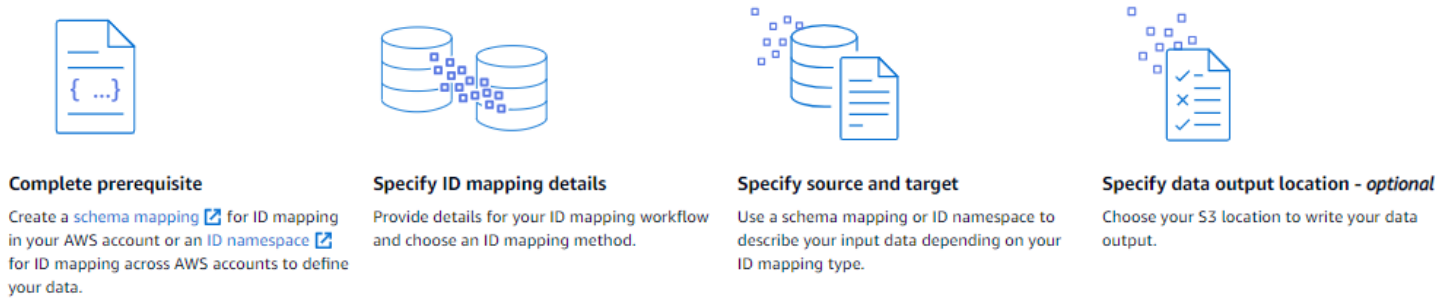
- Pemetaan ID berbasis aturan — Anda menggunakan aturan yang cocok untuk menerjemahkan data pihak pertama dari sumber ke target.
- Pemetaan ID layanan penyedia — Anda menggunakan layanan LiveRamp penyedia untuk menerjemahkan data pihak ketiga dari sumber ke target.

> **Note**
>
> Alur kerja pemetaan ID layanan penyedia di saat Resolusi Entitas AWS ini terintegrasi dengan. LiveRamp Jika Anda memiliki langganan ke LiveRamp layanan, maka Anda dapat membuat alur kerja pemetaan ID dengan LiveRamp untuk melakukan transcoding. Dengan LiveRamp transcoding, Anda dapat menerjemahkan satu set sumber R ampIDs ke rampID tujuan target apa pun. Dengan menggunakan rampID sebagai token untuk mewakili pelanggan Anda, Anda dapat menghindari berbagi data pelanggan secara langsung dengan platform iklan.
> Untuk informasi selengkapnya, lihat Melakukan Terjemahan Melalui ADX di situs web LiveRamp dokumentasi.

Anda dapat melakukan pemetaan ID antara dua kumpulan data dalam salah satu skenario berikut:

- Di dalam diri Anda sendiri Akun AWS
- Di dua yang berbeda Akun AWS

Diagram berikut merangkum cara mengatur alur kerja pemetaan ID.



Topik

- Alur kerja pemetaan ID untuk satu Akun AWS
- Alur kerja pemetaan ID di dua Akun AWS
- Menjalankan alur kerja pemetaan ID
- Menjalankan alur kerja pemetaan ID dengan tujuan keluaran baru
- Mengedit alur kerja pemetaan ID
- Menghapus alur kerja pemetaan ID
- Menambahkan atau memperbarui kebijakan sumber daya untuk alur kerja pemetaan ID

Alur kerja pemetaan ID untuk satu Akun AWS

Alur kerja pemetaan ID untuk satu Akun AWS memungkinkan Anda melakukan pemetaan ID antara dua kumpulan data Anda sendiri. Akun AWS

Sebelum Anda membuat alur kerja pemetaan ID sendiri Akun AWS, Anda harus terlebih dahulu menyelesaikan prasyarat.

Setelah Anda membuat dan menjalankan alur kerja pemetaan ID, Anda dapat melihat output (tabel pemetaan ID) dan menggunakannya untuk analisis.

Topik berikut memandu Anda melalui serangkaian langkah untuk membuat alur kerja pemetaan ID dalam hal yang sama. Akun AWS

Topik

- Prasyarat
- Membuat alur kerja pemetaan ID (berbasis aturan)
- Membuat alur kerja pemetaan ID (layanan penyedia)

Prasyarat

Sebelum membuat alur kerja pemetaan ID untuk salah satu Akun AWS menggunakan metode pemetaan ID berbasis Aturan atau layanan Penyedia, Anda harus terlebih dahulu melakukan hal berikut:

- Selesaikan tugas dalam Menyiapkan Resolusi AWS Entitas.
- Buat pemetaan skema atau Buat alur kerja yang cocok.
- (Hanya pemetaan ID layanan penyedia) Sebelum membuat alur kerja pemetaan ID LiveRamp, Anda harus memilih bucket pementasan data Amazon Simple Storage Service (Amazon S3) untuk sementara waktu untuk menulis output alur kerja pemetaan ID.

  Jika Anda menggunakan layanan LiveRamp penyedia untuk menerjemahkan data pihak ketiga, tambahkan kebijakan izin berikut, yang memungkinkan Anda mengakses bucket pementasan data.

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

Dalam kebijakan izin sebelumnya, ganti masing-masing *<user input placeholder>* dengan informasi Anda sendiri.

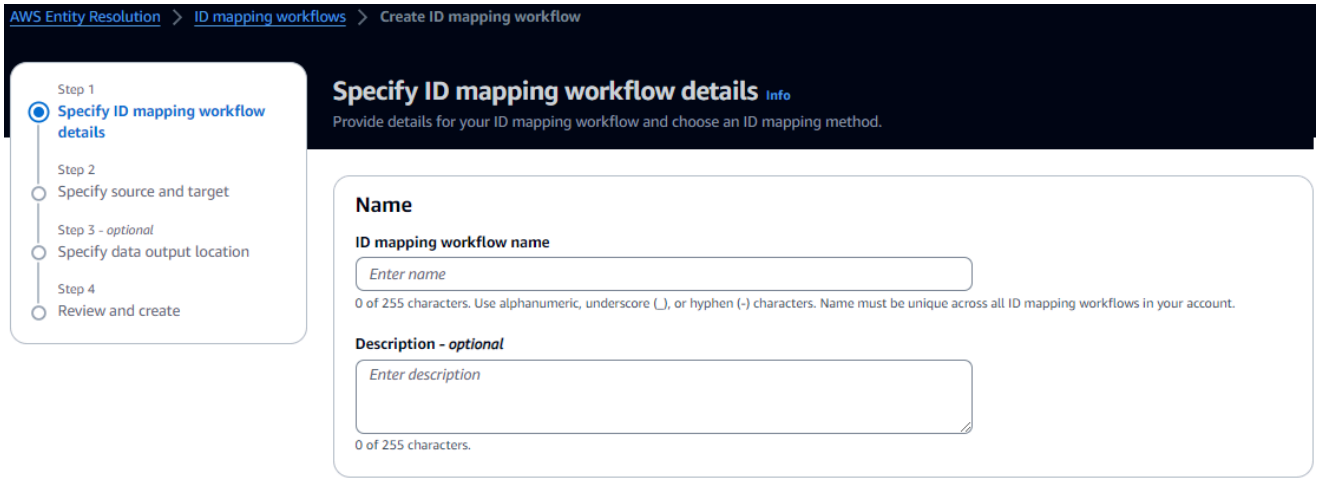
staging-bucket	Bucket Amazon S3 yang menyimpan sementara data Anda saat menjalankan alur kerja berbasis layanan penyedia.

Membuat alur kerja pemetaan ID (berbasis aturan)

Topik ini menjelaskan proses pembuatan alur kerja pemetaan ID untuk Akun AWS yang menggunakan aturan pencocokan untuk menerjemahkan data pihak pertama dari sumber ke target.

Untuk membuat alur kerja pemetaan ID berbasis aturan untuk satu Akun AWS

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih pemetaan ID.
3. Pada halaman alur kerja pemetaan ID, di sudut kanan atas, pilih Buat alur kerja pemetaan ID.
4. Untuk Langkah 1: Tentukan detail alur kerja pemetaan ID, lakukan hal berikut.
    a. Masukkan nama alur kerja pemetaan ID dan Deskripsi opsional.



b. Untuk metode pemetaan ID, pilih Berbasis aturan.

c. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

d. Pilih Berikutnya.

5. Untuk Langkah 2: Tentukan sumber dan target, lakukan hal berikut.

a. Untuk Sumber, pilih skenario yang berlaku untuk Anda dan kemudian ambil tindakan yang disarankan.

Skenario	Tindakan yang disarankan
Gunakan database AWS Glue, tabel AWS Glue, dan pemetaan skema Anda sendiri dalam alur kerja pemetaan ID.	1. Pilih Pemetaan skema. 2. Pilih AWS Gluedatabase dari dropdown, pilih AWS Glue tabel, lalu pilih pemetaan Skema yang sesuai. Anda dapat menambahkan hingga 19 input data.
Gunakan alur kerja pencocokan yang ada yang menunjuk ke data rekaman yang ingin Anda gunakan dalam alur kerja pemetaan ID.	1. Pilih Alur kerja yang cocok. 2. Pilih alur kerja Pencocokan yang ada dari daftar dropdown.

b. Untuk Target, pilih alur kerja Pencocokan yang ada dari daftar tarik-turun.

c. Untuk parameter Aturan, lakukan hal berikut.

   i. Tentukan kontrol Aturan dengan memilih salah satu opsi berikut berdasarkan jenis sumber Anda.

Jenis sumber	Tindakan yang disarankan
Alur kerja yang cocok	Tentukan kontrol Aturan dengan memilih apakah Sumber, Target, atau keduanya dapat memberikan aturan dalam alur kerja pemetaan ID. Kontrol aturan harus kompatibel antara sumber dan target yang akan digunakan dalam alur kerja pemetaan ID. Misalnya, jika namespace ID sumber membatasi aturan ke target tetapi namespace ID target membatasi aturan ke sumber, ini menghasilkan kesalahan.
Pemetaan skema	Lewatkan langkah ini.

   ii. Untuk parameter Perbandingan dan pencocokan, tipe Perbandingan secara otomatis diatur ke Beberapa bidang input.

   Ini karena kedua peserta telah memilih opsi ini sebelumnya.

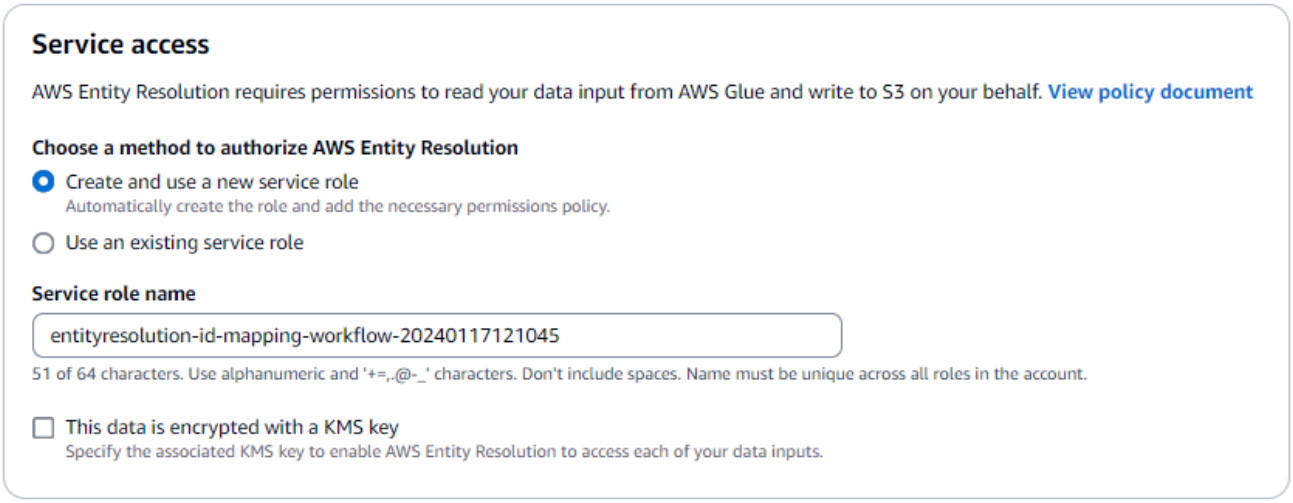
d. Tentukan jenis pencocokan Rekam dengan memilih salah satu opsi berikut berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Batasi jenis pencocokan rekaman untuk menyimpan hanya satu catatan yang cocok di sumber untuk setiap rekaman yang cocok dalam target saat Anda membuat alur kerja pemetaan ID.	Satu sumber untuk satu target

Tujuan Anda	Opsi yang disarankan
Batasi jenis pencocokan rekaman untuk menyimpan semua catatan yang cocok di sumber untuk setiap rekaman yang cocok dalam target saat Anda membuat alur kerja pemetaan ID.	Banyak sumber untuk satu target

> **Note**
>
> Anda harus menentukan batasan yang kompatibel untuk ruang nama ID sumber dan target.

e. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.



Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-id-mapping-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.

Opsi	Tindakan yang disarankan
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

6. Pilih Berikutnya.
7. Untuk Langkah 3: Tentukan lokasi keluaran data - opsional, lakukan hal berikut.
   a. Untuk tujuan keluaran Data, lakukan hal berikut:
      i. Pilih lokasi Amazon S3 untuk output data.
      ii. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, lalu masukkan AWS KMS kunci ARN atau pilih Buat AWS KMS kunci.
   b. Pilih Berikutnya.
8. Untuk Langkah 4: Tinjau dan buat, lakukan hal berikut.
   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.
   b. Pilih Buat.

Sebuah pesan muncul, menunjukkan bahwa alur kerja pemetaan ID telah dibuat.

Setelah membuat alur kerja pemetaan ID, Anda siap menjalankan alur kerja pemetaan ID.

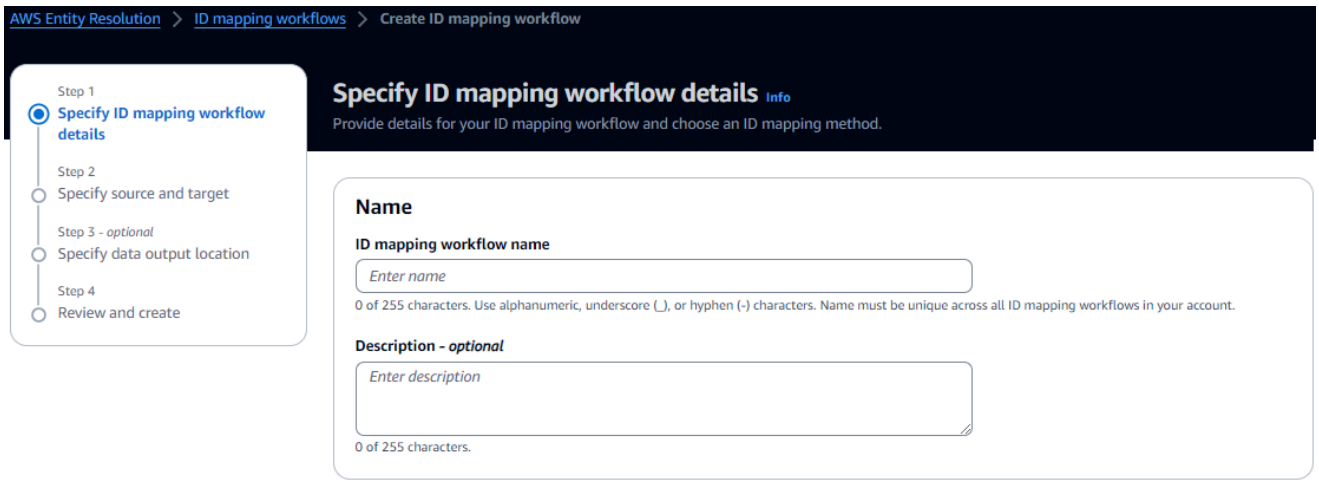
Membuat alur kerja pemetaan ID (layanan penyedia)

Topik ini menjelaskan proses pembuatan alur kerja pemetaan ID untuk yang Akun AWS menggunakan layanan penyedia yang disebut. LiveRamp LiveRamp menerjemahkan satu set sumber R ampIDs ke set lain menggunakan R ampIDs yang dipertahankan atau diturunkan.

Untuk membuat alur kerja pemetaan ID berbasis layanan penyedia untuk satu Akun AWS

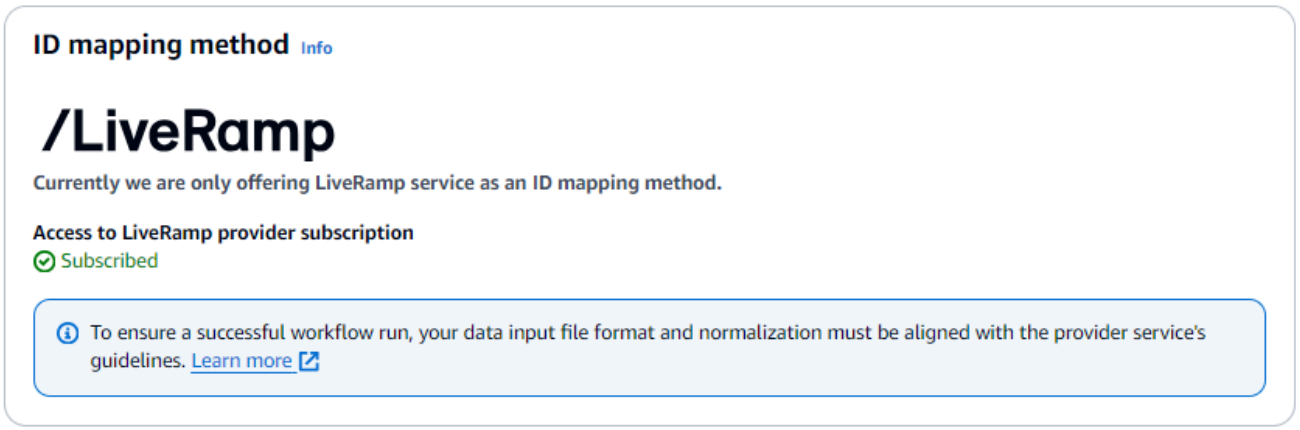
1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih pemetaan ID.
3. Pada halaman alur kerja pemetaan ID, di sudut kanan atas, pilih Buat alur kerja pemetaan ID.
4. Untuk Langkah 1: Tentukan detail alur kerja pemetaan ID, lakukan hal berikut.

   a. Masukkan nama alur kerja pemetaan ID dan Deskripsi opsional.



   b. Untuk metode pemetaan ID, pilih Layanan penyedia.

      Resolusi Entitas AWS saat ini menawarkan layanan LiveRamp penyedia sebagai metode pemetaan ID. Jika Anda memiliki langganan LiveRamp, maka status akan muncul sebagai Berlangganan. Untuk informasi selengkapnya tentang cara berlangganan LiveRamp, lihatLangkah 1: Berlangganan layanan penyedia di AWS Data Exchange.



> **Note**
>
> Pastikan format file input data Anda selaras dengan pedoman layanan penyedia. Untuk informasi selengkapnya tentang LiveRamp pedoman pemformatan file masukan, lihat Melakukan Terjemahan Melalui ADX di situs web LiveRamp dokumentasi.

c. Untuk LiveRamp konfigurasi, masukkan nilai berikut yang LiveRamp menyediakan:

- Manajer ID Klien ARN
- Manajer rahasia klien ARN

d. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

e. Pilih Berikutnya.

5. Untuk Langkah 2: Tentukan sumber dan target, lakukan hal berikut.

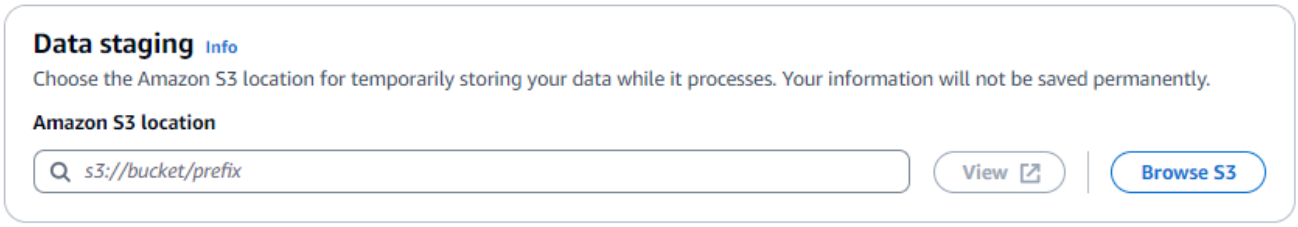
a. Untuk Sumber, pilih skenario yang berlaku untuk Anda dan kemudian ambil tindakan yang disarankan.

Skenario	Tindakan yang disarankan
Gunakan database AWS Glue, tabel AWS Glue, dan pemetaan skema Anda sendiri dalam alur kerja pemetaan ID.	1. Pilih Pemetaan skema. 2. Pilih AWS Gluedatabase dari dropdown, pilih AWS Glue tabel, lalu pilih pemetaan Skema yang sesuai. Anda dapat menambahkan hingga 19 input data.
Gunakan alur kerja pencocokan yang ada yang menunjuk ke data rekaman yang ingin Anda gunakan dalam alur kerja pemetaan ID.	1. Pilih Alur kerja yang cocok. 2. Pilih alur kerja Pencocokan yang ada dari daftar dropdown.

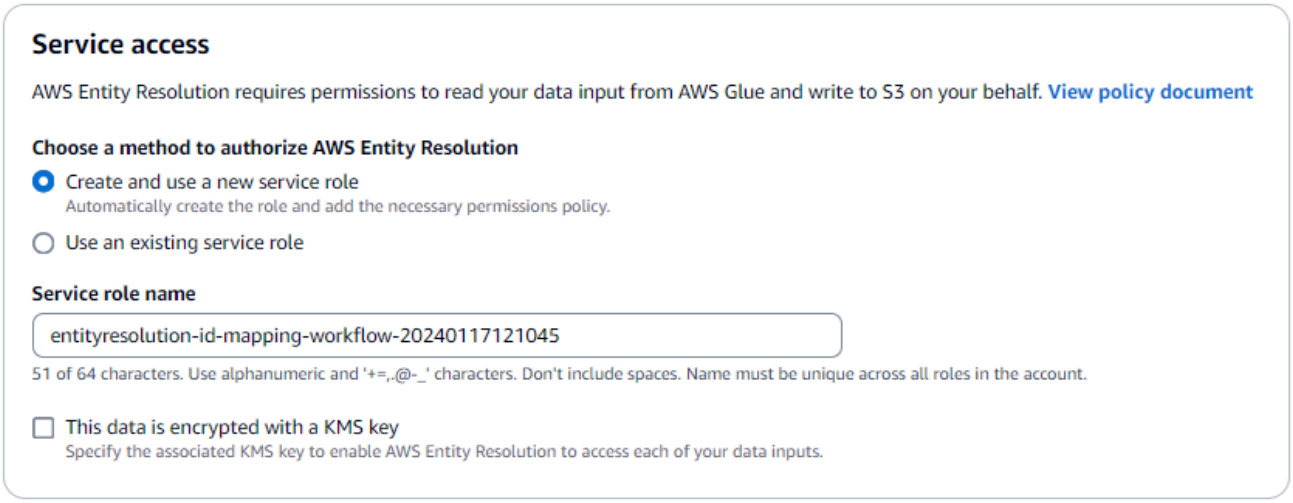
b. Untuk Target, lakukan salah satu tindakan berikut berdasarkan metode pemetaan ID yang Anda pilih.

Metode pemetaan ID	Tindakan yang disarankan
Berbasis aturan	Pilih alur kerja Pencocokan yang ada dari daftar dropdown.
Layanan penyedia	Masukkan pengenal domain LiveRamp klien yang ditargetkan untuk transcodi ng yang LiveRamp disediakan di domain Target. 

c. Untuk pementasan Data, pilih lokasi Amazon S3 tempat Anda ingin menulis sementara output alur kerja pemetaan ID.



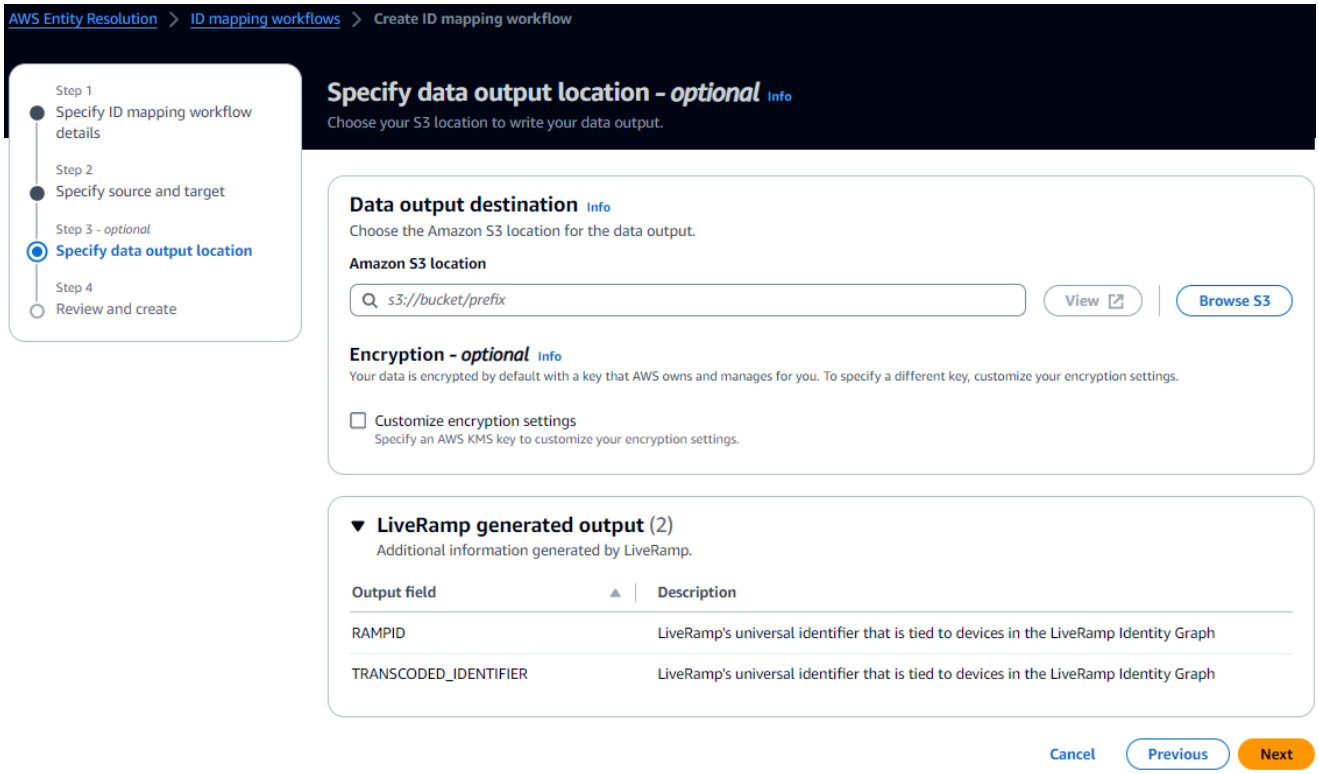
d. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.



Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-id-mapping-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.

Opsi	Tindakan yang disarankan
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

6. Pilih Berikutnya.
7. Untuk Langkah 3: Tentukan lokasi keluaran data - opsional, lakukan hal berikut.
   a. Untuk tujuan keluaran Data, lakukan hal berikut:
      i. Pilih lokasi Amazon S3 untuk output data.
      ii. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, lalu masukkan AWS KMS kunci ARN atau pilih Buat AWS KMS kunci.
   b. Lihat output LiveRamp yang dihasilkan.
   c. Pilih Berikutnya.



8. Untuk Langkah 4: Tinjau dan buat, lakukan hal berikut.

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat.

   Sebuah pesan muncul, menunjukkan bahwa alur kerja pemetaan ID telah dibuat.

9. Setelah membuat alur kerja pemetaan ID, Anda siap menjalankan alur kerja pemetaan ID.

Alur kerja pemetaan ID di dua Akun AWS

Alur kerja pemetaan ID di dua Akun AWS memungkinkan Anda melakukan pemetaan ID antara dua kumpulan data di dua. Akun AWS Ini biasanya dilakukan antara Anda sendiri Akun AWS dan yang lain Akun AWS.

Misalnya, penayang dapat membuat alur kerja pemetaan ID menggunakan namespace ID target mereka sendiri (milik mereka sendiri Akun AWS) dan namespace ID sumber pengiklan (di tempat lain). Akun AWS

Sebelum Anda membuat alur kerja pemetaan ID di dua Akun AWS, Anda harus terlebih dahulu menyelesaikan prasyarat.

Setelah Anda membuat alur kerja pemetaan ID, Anda dapat melihat output (tabel pemetaan ID) dan menggunakannya untuk analisis.

Topik berikut memandu Anda melalui serangkaian langkah untuk membuat alur kerja pemetaan ID di dua: Akun AWS

Topik

Prasyarat

Sebelum Anda membuat alur kerja pemetaan ID di dua Akun AWS, Anda harus terlebih dahulu melakukan hal berikut:

- Selesaikan tugas dalam Mengatur Resolusi Entitas AWS.
- Buat sumber namespace ID.
- Buat target namespace ID.
- Dapatkan namespace ID ARN jika Anda menggunakan sumber namespace ID dari yang lain. Akun AWS
- (Hanya layanan penyedia) Membuat alur kerja pemetaan ID di dua Akun AWS memerlukan izin LiveRamp untuk mengakses bucket S3 dan AWS Key Management Service (AWS KMS) kunci yang dikelola pelanggan.

  Sebelum Anda membuat alur kerja pemetaan ID di dua Akun AWS dengan LiveRamp, tambahkan kebijakan izin berikut, yang memungkinkan LiveRamp untuk mengakses bucket S3 dan kunci yang dikelola pelanggan.

```
{
    "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"
            }
        }
    }]
}
```

Dalam kebijakan izin sebelumnya, ganti masing-masing *<user input placeholder>* dengan informasi Anda sendiri.

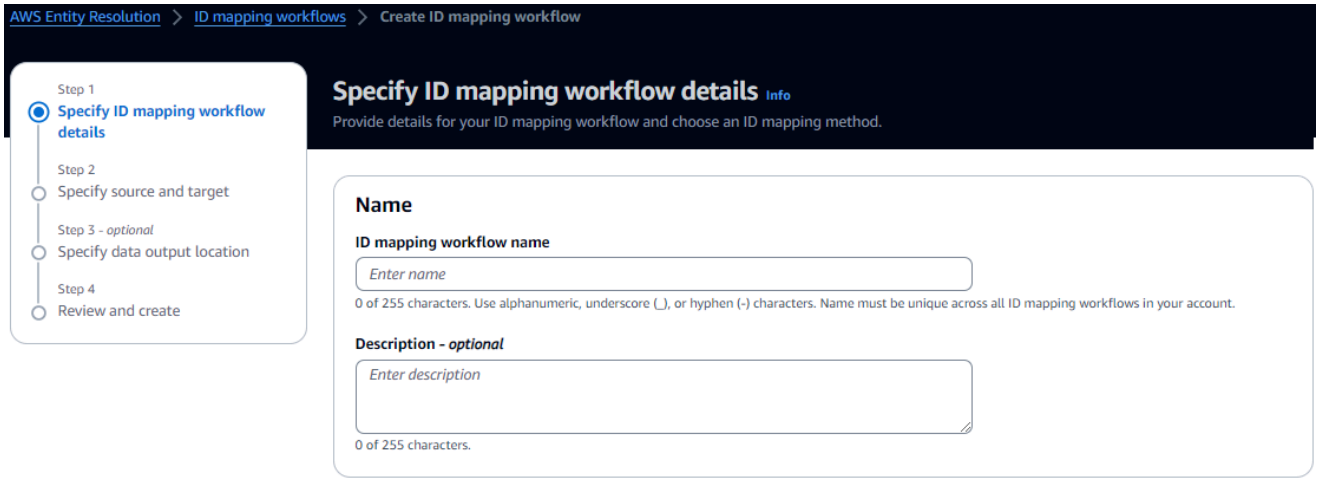
<KMSKeyARN>	Kunci ARN yang dikelola AWS KMS pelanggan.

Membuat alur kerja pemetaan ID (berbasis aturan)

Setelah menyelesaikan prasyarat, Anda dapat membuat satu atau beberapa alur kerja pemetaan ID untuk menggunakan aturan yang cocok untuk menerjemahkan data pihak pertama dari sumber ke target.

Untuk membuat alur kerja pemetaan ID berbasis aturan di dua Akun AWS

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih pemetaan ID.
3. Pada halaman alur kerja pemetaan ID, di sudut kanan atas, pilih Buat alur kerja pemetaan ID.
4. Untuk Langkah 1: Tentukan detail alur kerja pemetaan ID, lakukan hal berikut.
    a. Masukkan nama alur kerja pemetaan ID dan Deskripsi opsional.



b. Untuk metode pemetaan ID, pilih Berbasis aturan.

c. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

d. Pilih Berikutnya.

5. Untuk Langkah 2: Tentukan sumber dan target, lakukan hal berikut.

a. Aktifkan Opsi lanjutan.

b. Untuk Sumber, pilih Pencocokan alur kerja, lalu pilih alur kerja Pencocokan yang ada dari daftar tarik-turun.

c. Untuk Target, pilih Pencocokan alur kerja, lalu pilih alur kerja Pencocokan yang ada dari daftar tarik-turun.

d. Untuk parameter Aturan, tentukan kontrol Aturan dengan memilih apakah Sumber atau Target dapat memberikan aturan dalam alur kerja pemetaan ID.

   Kontrol aturan harus kompatibel antara sumber dan target yang akan digunakan dalam alur kerja pemetaan ID. Misalnya, jika namespace ID sumber membatasi aturan ke target tetapi namespace ID target membatasi aturan ke sumber, ini menghasilkan kesalahan.

e. Untuk parameter Perbandingan dan pencocokan, lakukan hal berikut.

   i. Tentukan tipe Perbandingan dengan memilih opsi berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Temukan kombinasi kecocokan di seluruh data yang disimpan di beberapa	Beberapa bidang masukan

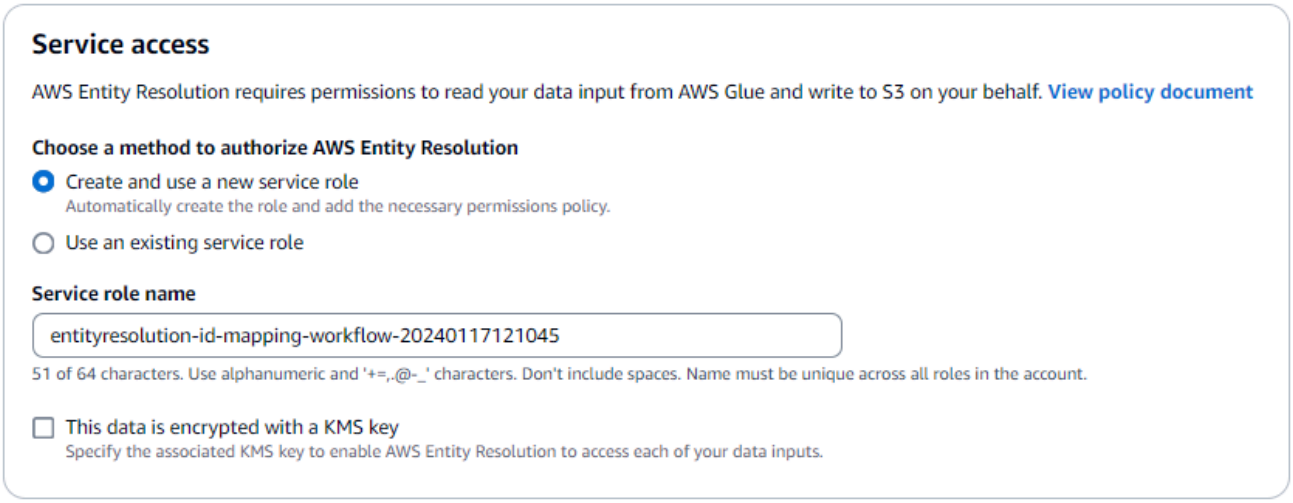
Tujuan Anda	Opsi yang disarankan
bidang input, terlepas dari apakah data berada di bidang input yang sama atau berbeda.	
Batasi perbandingan dalam satu bidang input, ketika data serupa yang disimpan di beberapa bidang input tidak boleh dicocokkan.	Bidang masukan tunggal

ii. Tentukan jenis pencocokan Rekam dengan memilih opsi berdasarkan tujuan Anda.

Tujuan Anda	Opsi yang disarankan
Batasi jenis pencocokan rekaman untuk menyimpan hanya satu catatan yang cocok di sumber untuk setiap rekaman yang cocok dalam target saat Anda membuat alur kerja pemetaan ID.	Satu sumber untuk satu target
Batasi jenis pencocokan rekaman untuk menyimpan semua catatan yang cocok di sumber untuk setiap rekaman yang cocok dalam target saat Anda membuat alur kerja pemetaan ID.	Banyak sumber untuk satu target

> **Note**
>
> Anda harus menentukan batasan yang kompatibel untuk ruang nama ID sumber dan target.

f. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.



Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-id-mapping-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.

Opsi	Tindakan yang disarankan
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

6. Pilih Berikutnya.
7. Untuk Langkah 3: Tentukan lokasi keluaran data - opsional, lakukan hal berikut.
   a. Untuk tujuan keluaran Data, lakukan hal berikut.
      i. Pilih lokasi Amazon S3 untuk output data.
      ii. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, lalu masukkan AWS KMS kunci ARN atau pilih Buat AWS KMS kunci.
   b. Lihat output LiveRamp yang dihasilkan.
   c. Pilih Berikutnya.
8. Untuk Langkah 4: Tinjau dan buat, lakukan hal berikut.
   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

b. Pilih Buat.

Sebuah pesan muncul, menunjukkan bahwa alur kerja pemetaan ID telah dibuat.

Setelah membuat alur kerja pemetaan ID, Anda siap menjalankan alur kerja pemetaan ID.

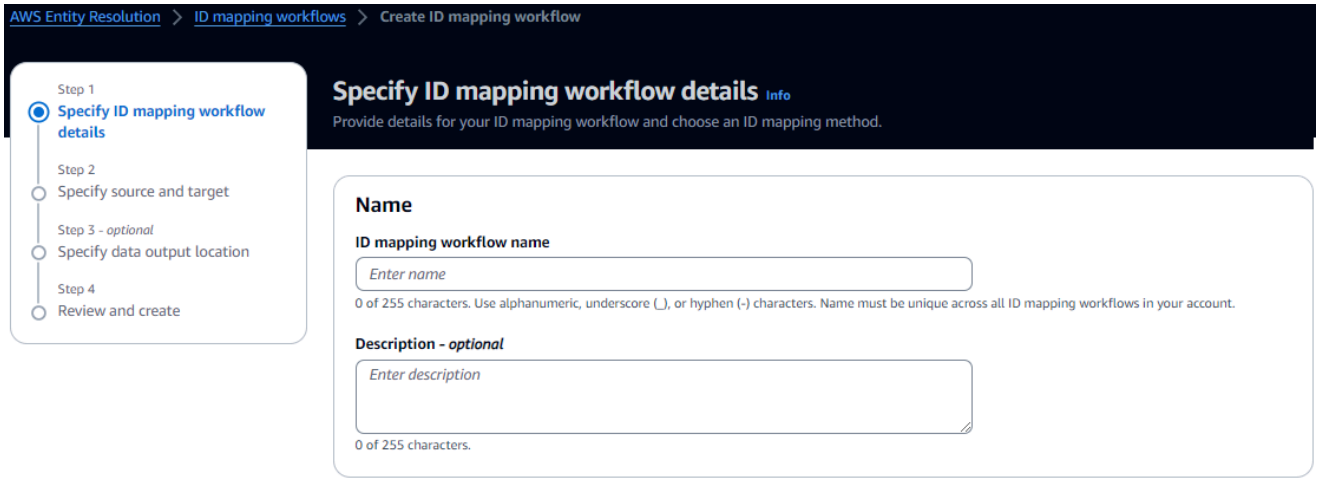
Membuat alur kerja pemetaan ID (layanan penyedia)

Setelah menyelesaikan prasyarat, Anda dapat membuat satu atau beberapa alur kerja pemetaan ID menggunakan layanan penyedia. LiveRamp LiveRamp menerjemahkan satu set sumber R ampIDs ke set lain menggunakan R ampIDs yang dipertahankan atau diturunkan.

Untuk membuat alur kerja pemetaan ID menggunakan layanan penyedia

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih pemetaan ID.
3. Pada halaman alur kerja pemetaan ID, di sudut kanan atas, pilih Buat alur kerja pemetaan ID.
4. Untuk Langkah 1: Tentukan detail alur kerja pemetaan ID, lakukan hal berikut.

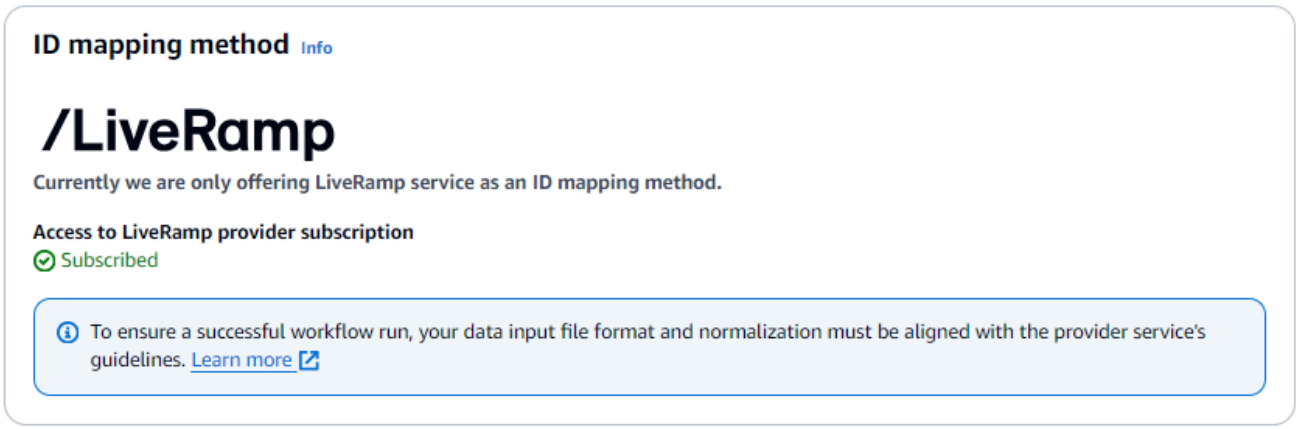
   a. Masukkan nama alur kerja pemetaan ID dan Deskripsi opsional.



   b. Untuk metode pemetaan ID, pilih Layanan penyedia.

   Resolusi Entitas AWS saat ini menawarkan layanan LiveRamp penyedia sebagai metode pemetaan ID. Jika Anda memiliki langganan LiveRamp, maka status akan muncul sebagai

Berlangganan. Untuk informasi selengkapnya tentang cara berlangganan LiveRamp, lihat[Langkah 1: Berlangganan layanan penyedia di AWS Data Exchange](#).



> **Note**
>
> Pastikan format file input data Anda selaras dengan pedoman layanan penyedia. Untuk informasi selengkapnya tentang LiveRamp pedoman pemformatan file masukan, lihat Melakukan Terjemahan Melalui ADX di situs web LiveRamp dokumentasi.

c. Untuk LiveRamp konfigurasi, masukkan nilai berikut yang LiveRamp menyediakan:

- Manajer ID Klien ARN
- Manajer rahasia klien ARN

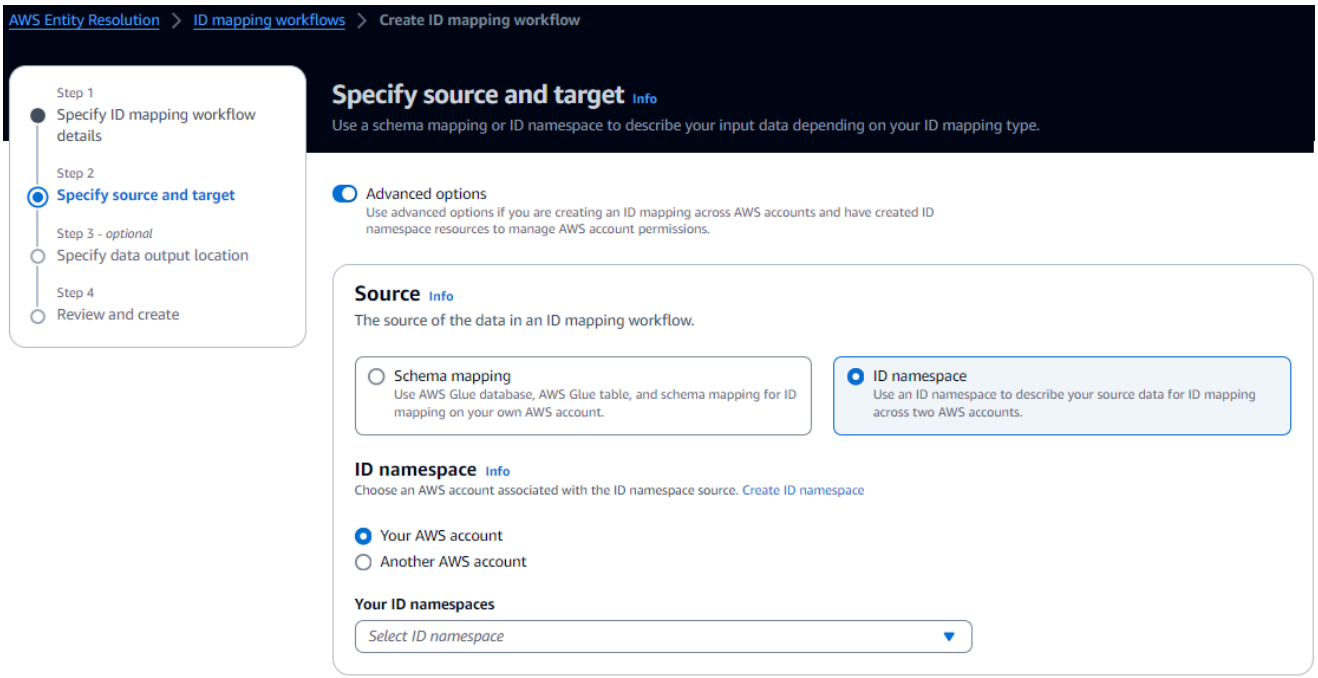
d. (Opsional) Untuk mengaktifkan Tag untuk sumber daya, pilih Tambahkan tag baru, lalu masukkan pasangan Kunci dan Nilai.

e. Pilih Berikutnya.

5. Untuk Langkah 2: Tentukan sumber dan target, lakukan hal berikut.

a. Aktifkan Opsi lanjutan.

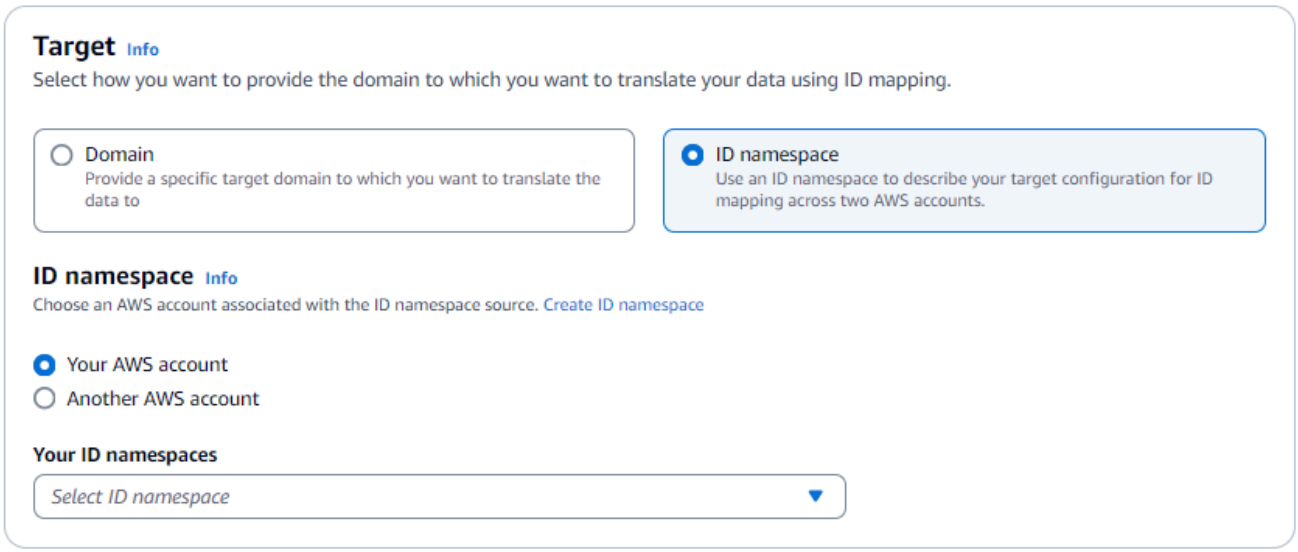
b. Untuk Sumber, pilih ID namespace.



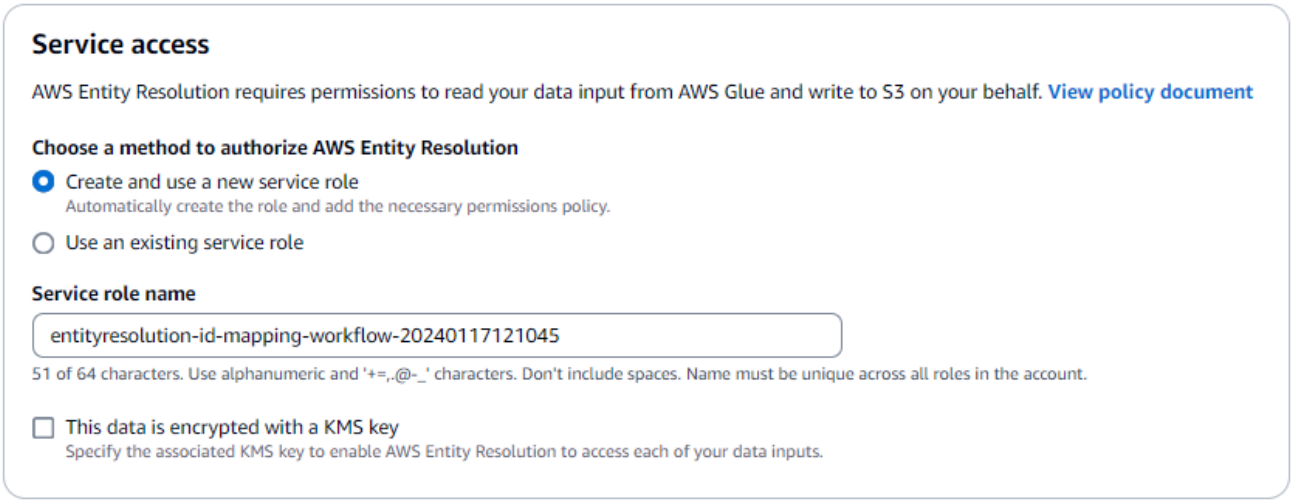
c. Untuk namespace ID, identifikasi lokasi namespace ID, lalu lakukan tindakan yang disarankan.

Lokasi namespace ID	Tindakan yang disarankan
Milik Anda sendiri Akun AWS	1. Pilih Anda Akun AWS. 2. Pilih namespace ID dari daftar tarik-tur un ruang nama ID Anda.
milik orang lain Akun AWS	1. Pilih yang lain Akun AWS. 2. Masukkan namespace ARN ID.

d. Untuk Target, pilih ID namespace.



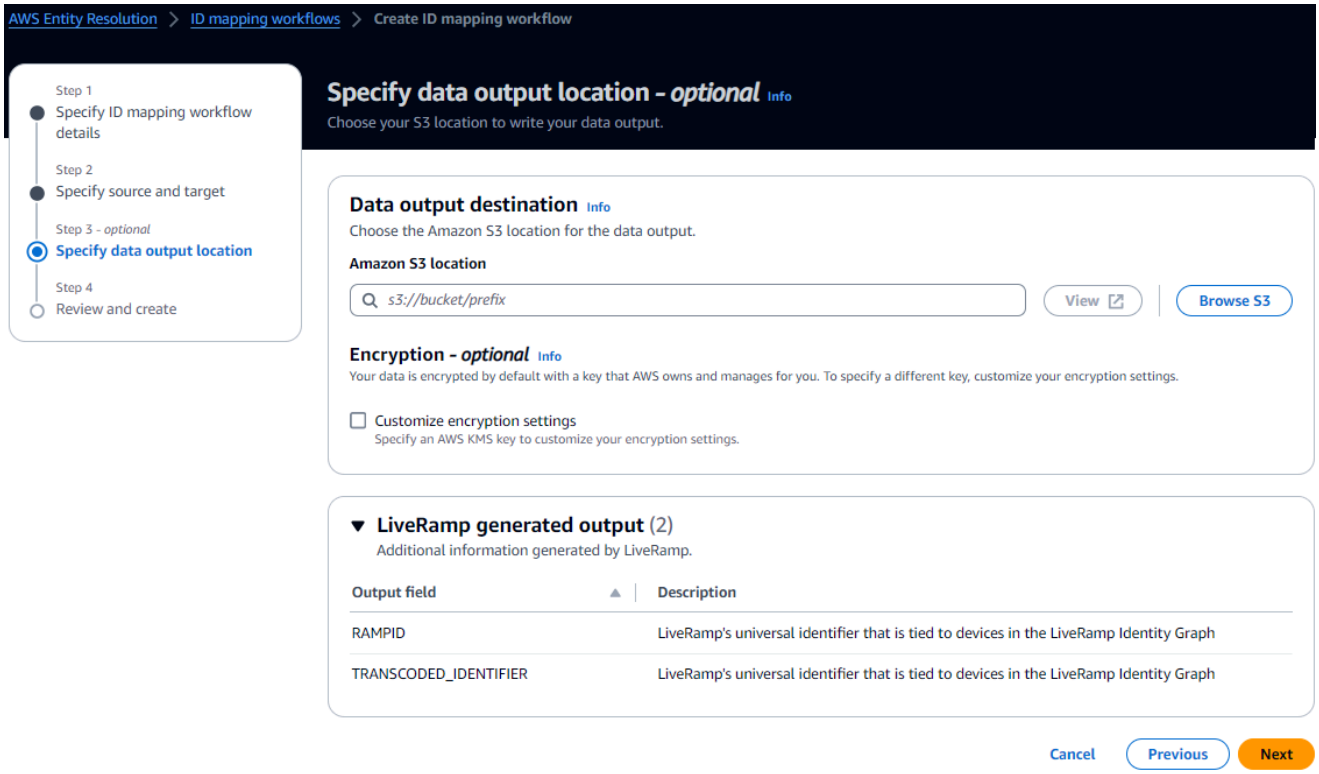
e. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.



Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-id-mapping-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.

Opsi	Tindakan yang disarankan
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. 2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

6. Pilih Berikutnya.
7. Untuk Langkah 3: Tentukan lokasi keluaran data - opsional, lakukan hal berikut.
   a. Untuk tujuan keluaran Data, lakukan hal berikut.
      i. Pilih lokasi Amazon S3 untuk output data.
      ii. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, lalu masukkan AWS KMS kunci ARN atau pilih Buat AWS KMS kunci.
   b. Lihat output LiveRamp yang dihasilkan.
   c. Pilih Berikutnya.



8. Untuk Langkah 4: Tinjau dan buat, lakukan hal berikut.

   a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

   b. Pilih Buat.

      Sebuah pesan muncul, menunjukkan bahwa alur kerja pemetaan ID telah dibuat.

Setelah membuat alur kerja pemetaan ID, Anda siap menjalankan alur kerja pemetaan ID.

Menjalankan alur kerja pemetaan ID

Setelah Anda membuat alur kerja pemetaan ID untuk satu Akun AWS atau membuat alur kerja pemetaan ID di dua Akun AWS, Anda dapat menjalankan alur kerja pemetaan ID. Alur kerja pemetaan ID mengeluarkan file. CSV

Untuk menjalankan alur kerja pemetaan ID

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih pemetaan ID.

3. Pilih alur kerja pemetaan ID.
4. Pada halaman detail alur kerja pemetaan ID, di sudut kanan atas, pilih Jalankan.
5. Pada halaman detail alur kerja yang cocok, pada tab Metrik, lihat yang berikut ini di bawah Metrik pekerjaan terakhir:

   - ID Job
   - Waktu selesai untuk pekerjaan alur kerja
   - Status pekerjaan alur kerja yang cocok: Antrian, Sedang berlangsung, Selesai, Gagal
   - Jumlah Rekaman yang diproses
   - Jumlah Rekaman yang tidak diproses
   - Jumlah catatan Input

   Di bawah Riwayat pekerjaan, Anda juga dapat melihat metrik pekerjaan untuk pekerjaan alur kerja pemetaan ID yang sebelumnya dijalankan.
6. Setelah pekerjaan alur kerja pemetaan ID selesai (status Selesai), pilih Keluaran data, lalu pilih lokasi Amazon S3 Anda untuk melihat hasilnya.

   Setelah Anda mendapatkan CSV file Anda, Anda dapat bergabung `RAMPID` dengan file`TRANSCODED_ID`.

Menjalankan alur kerja pemetaan ID dengan tujuan keluaran baru

Setelah Anda membuat alur kerja pemetaan ID untuk satu Akun AWS atau membuat alur kerja pemetaan ID di dua Akun AWS, Anda dapat memilih lokasi S3 yang berbeda untuk menulis output data Anda.

Untuk menjalankan alur kerja pemetaan ID dengan tujuan keluaran baru

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih pemetaan ID.
3. Pilih alur kerja pemetaan ID.
4. Pada halaman detail alur kerja pemetaan ID, di sudut kanan atas, pilih Jalankan dengan tujuan keluaran baru dari daftar dropdown Jalankan alur kerja.
5. Untuk tujuan keluaran Data, lakukan hal berikut.

a. Pilih lokasi Amazon S3 untuk output data.

b. Untuk Enkripsi, jika Anda memilih untuk Menyesuaikan pengaturan enkripsi, lalu masukkan AWS KMS kunci ARN atau pilih Buat AWS KMS kunci.

6. Untuk menentukan izin akses Layanan, pilih opsi dan lakukan tindakan yang disarankan.

Opsi	Tindakan yang disarankan
Membuat dan menggunakan peran layanan baru	• Resolusi Entitas AWS membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`entityresolution-id-mapping-workflow-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, pilih opsi Data ini dienkripsi oleh kunci. KMS Kemudian, masukkan AWS KMS kunci yang digunakan untuk mendekripsi input data Anda.
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk mencantumkan peran, Anda dapat memasukkan Amazon Resource Name (ARN) peran yang ingin Anda gunakan. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia.

Opsi	Tindakan yang disarankan
	2. Lihat peran layanan dengan memilih tautan Lihat di IAM eksternal. Secara default, Resolusi Entitas AWS tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan.

7. Pilih Jalankan.
8. Pada halaman detail alur kerja yang cocok, pada tab Metrik, lihat yang berikut ini di bawah Metrik pekerjaan terakhir:

   - ID Job
   - Waktu selesai untuk pekerjaan alur kerja
   - Status pekerjaan alur kerja yang cocok: Antrian, Sedang berlangsung, Selesai, Gagal
   - Jumlah Rekaman yang diproses
   - Jumlah Rekaman yang tidak diproses
   - Jumlah catatan Input

   Di bawah Riwayat pekerjaan, Anda juga dapat melihat metrik pekerjaan untuk pekerjaan alur kerja pemetaan ID yang sebelumnya dijalankan.
9. Setelah pekerjaan alur kerja pemetaan ID selesai (status Selesai), pilih Keluaran data, lalu pilih lokasi Amazon S3 Anda untuk melihat hasilnya.

   Setelah Anda mendapatkan CSV file Anda, Anda dapat bergabung `RAMPID` dengan file`TRANSCODED_ID`.

Mengedit alur kerja pemetaan ID

Mengedit alur kerja pemetaan ID memungkinkan Anda untuk menjaga kemampuan resolusi entitas Anda up-to-date dan selaras dengan kebutuhan bisnis Anda yang terus berkembang dari waktu ke waktu. Anda mungkin ingin menyesuaikan aturan pemetaan, teknik, dan parameter, Anda dapat mengoptimalkan alur kerja untuk memberikan hasil pencocokan ID yang lebih akurat dan andal. Anda mungkin juga ingin menambahkan sumber data baru, memperluas jenis yang IDs dipetakan,

atau memasukkan kriteria pencocokan tambahan ke dalam alur kerja. Jika Anda mengidentifikasi masalah atau kesalahan dalam hasil pemetaan ID, pengeditan dengan alur kerja dapat membantu Anda mendiagnosis dan menyelesaikan masalah tersebut.

Untuk mengedit alur kerja pemetaan ID:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih pemetaan ID.
3. Pilih alur kerja pemetaan ID.
4. Pada halaman detail alur kerja pemetaan ID, di sudut kanan atas, pilih Edit.
5. Pada halaman Tentukan detail alur kerja pemetaan ID, buat perubahan yang diperlukan lalu pilih Berikutnya.
6. Pada halaman Tentukan keluaran data, buat perubahan yang diperlukan lalu pilih Berikutnya.
7. Pada halaman Tinjau dan simpan, buat perubahan yang diperlukan lalu pilih Simpan.

Menghapus alur kerja pemetaan ID

Jika Anda tidak lagi menggunakan alur kerja pemetaan ID, menghapusnya dapat membantu merampingkan manajemen alur kerja Anda. Selain itu, menghapus alur kerja pemetaan ID yang berlebihan atau kurang efisien yang melayani tujuan serupa dapat membantu Anda mengkonsolidasikan proses Anda.

Untuk menghapus alur kerja pemetaan ID:

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih pemetaan ID.
3. Pilih alur kerja pemetaan ID.
4. Pada halaman detail alur kerja pemetaan ID, di sudut kanan atas, pilih Hapus.
5. Konfirmasikan penghapusan dan kemudian pilih Hapus.

Menambahkan atau memperbarui kebijakan sumber daya untuk alur kerja pemetaan ID

Kebijakan sumber daya memungkinkan pembuat sumber daya pemetaan ID mengakses sumber daya alur kerja pemetaan ID Anda.

Untuk menambah atau memperbarui kebijakan sumber daya

1. Masuk ke AWS Management Console dan buka Resolusi Entitas AWS konsol dengan Anda Akun AWS, jika Anda belum melakukannya.
2. Di panel navigasi kiri, di bawah Alur kerja, pilih pemetaan ID.
3. Pilih alur kerja pemetaan ID.
4. Pada halaman detail alur kerja pemetaan ID, pilih tab Izin.
5. Di bagian Kebijakan sumber daya, pilih Edit.
6. Tambahkan atau perbarui kebijakan di JSON editor.
7. Pilih Simpan perubahan.

Integrasikan dengan Resolusi Entitas AWS sebagai penyedia

Resolusi Entitas AWS Integrasi penyedia pihak ketiga membantu pelanggan melindungi privasi konsumen dan menjaga kepatuhan terhadap undang-undang kedaulatan data. Penyedia pihak ketiga, seperti LiveRamp dan TransUnion, menerjemahkan pengenal konsumen ke dalam iklanIDs, seperti Ramp IDs dan Fabrick. IDs Pengidentifikasi iklan ini biasanya digunakan dalam alat periklanan dan pemasaran, untuk mencegah data konsumen diekspor ke non-AWS sistem yang dikelola. Bagian ini memberikan panduan bagi penyedia untuk berintegrasi dengan Resolusi Entitas AWS untuk menyandikan atau mentranskode pengenal konsumen ke dalam iklan IDs untuk digunakan dalam alur kerja pencocokan berbasis layanan penyedia.

Untuk informasi lebih lanjut tentang layanan penyedia yang saat ini terintegrasi dengan Resolusi Entitas AWS, lihat Membuat alur kerja pencocokan berbasis layanan penyedia.

Topik

Persyaratan

Sebelum berintegrasi sebagai penyedia layanan dengan Resolusi Entitas AWS, lengkapi persyaratan berikut.

Topik

Daftar layanan penyedia di AWS Data Exchange

Sebagai penyedia pihak ketiga, Anda harus mencantumkan produk Anda di Katalog Produk AWSData Exchange (ADX). Setelah produk Anda terdaftar di AWS Data Exchange Katalog Produk, pelanggan dapat berlangganan produk Anda melalui penawaran publik atau pribadi.

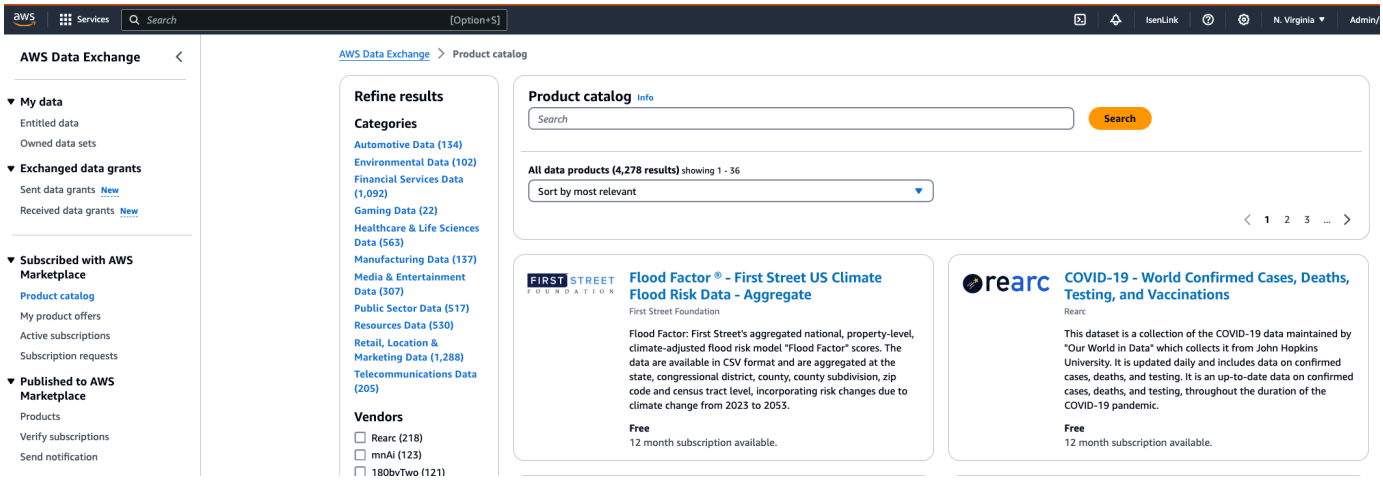
Untuk membuat daftar layanan penyedia di AWS Data Exchange

1. Jika Anda adalah penyedia produk data baru di AWS Data Exchange, selesaikan langkah-langkah di bagian berjudul Memulai sebagai penyedia di AWS Data Exchange Panduan Pengguna.
2. Buat kumpulan REST API data dan publikasikan produk baru yang berisi APIs AWS Data Exchange dengan mengikuti langkah-langkah di bagian berjudul Cara mempublikasikan produk APIs yang mengandung AWS Data Exchange Panduan Pengguna. Anda dapat menyelesaikan proses dengan menggunakan salah satu AWS Data Exchange konsol atau AWS Command Line Interface.

   Jika Anda telah menetapkan visibilitas produk Publik, penawaran publik tersedia untuk semua pelanggan.

   Jika Anda telah mengatur visibilitas produk Pribadi, selesaikan langkah-langkah di bagian berjudul Buat penawaran khusus di AWS Data Exchange Panduan Pengguna, tergantung pada kasus penggunaan Anda.

   Gambar berikut menunjukkan contoh produk yang tersedia di AWS Data Exchange Katalog Produk.



3. Setelah produk tersedia di AWS Data Exchange Katalog Produk, pelanggan dapat berlangganan produk dengan cara berikut.

   - Berlangganan produk publik.
   - Gunakan penawaran pribadi (penawaran khusus) yang telah dikeluarkan oleh layanan penyedia.

- Gunakan penawaran Bawa Langganan Anda Sendiri (BYOS).

Untuk informasi selengkapnya, lihat Berlangganan dan mengakses produk yang APIs terdapat di AWS Data Exchange Panduan Pengguna.

Identifikasi atribut Anda

Atribut data input adalah definisi tipe entitas yang akan diselesaikan dalam alur kerja. Beberapa contoh atribut adalah`FirstName`,`LastName`,`Email`, atau`Custom String`.

Ketika Anda mengidentifikasi atribut Anda, Anda harus mencatat persyaratan atau pedoman apa pun.

Example Contoh

Berikut ini adalah contoh validasi untuk mengidentifikasi atribut penyedia.

- Entah `LastName` atribut `FirstName` atau adalah wajib.
- Jika `Email` atribut ada, itu harus di-hash.

Sebagai penyedia, Anda harus mengidentifikasi atribut dalam produk layanan penyedia Anda dan kemudian mengkomunikasikan atribut ini ke Resolusi Entitas AWS Tim Pengembangan Bisnis di `<aws-entity-resolution-bd@amazon .com>` untuk validasi tambahan sebelum melanjutkan.

Meminta Resolusi Entitas AWS APISpesifikasi terbuka

Resolusi Entitas AWS memiliki API spesifikasi Terbuka yang dapat Anda gunakan sebagai penyedia sebagai jabat tangan yang berisi yang APIs terlibat dalam integrasi. Untuk informasi selengkapnya, lihat Menggunakan Resolusi Entitas AWS APISpesifikasi terbuka.

Untuk meminta API definisi Terbuka, hubungi Resolusi Entitas AWS Tim Pengembangan Bisnis di `<aws-entity-resolution-bd@amazon .com>`.

Menggunakan Resolusi Entitas AWS APISpesifikasi terbuka

APISpesifikasi Terbuka mendefinisikan semua protokol yang terkait dengan Resolusi Entitas AWS. Spesifikasi ini diperlukan untuk mengimplementasikan integrasi.

APIDefinisi Terbuka berisi API operasi berikut:

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

Untuk meminta API spesifikasi Terbuka, hubungi Resolusi Entitas AWS Tim Pengembangan Bisnis di `<aws-entity-resolution-bd@amazon .com>`.

APISpesifikasi Terbuka mendukung dua jenis integrasi untuk pengkodean dan transcoding pengenal konsumen pemrosesan batch dan pemrosesan sinkron. Setelah Anda memperoleh API spesifikasi Terbuka, terapkan jenis integrasi pemrosesan untuk kasus penggunaan Anda.

Topik

- Integrasi pemrosesan batch
- Integrasi pemrosesan sinkron

Integrasi pemrosesan batch

Integrasi pemrosesan batch mengikuti pola desain asinkron. Setelah alur kerja dimulai pada AWS Data Exchange, itu mengirimkan pekerjaan melalui titik akhir integrasi penyedia dan kemudian alur kerja menunggu penyelesaian pekerjaan ini dengan secara berkala melakukan polling untuk status pekerjaan. Solusi ini lebih diinginkan untuk menjalankan pekerjaan yang mungkin memakan waktu lebih lama dan memiliki throughput penyedia yang lebih rendah. Penyedia akan memasukkan lokasi kumpulan data sebagai tautan Amazon S3, yang dapat mereka proses di ujungnya dan menulis hasilnya ke lokasi S3 keluaran yang telah ditentukan.

Integrasi pemrosesan batch diaktifkan menggunakan tiga API definisi. Resolusi Entitas AWS akan memanggil titik akhir penyedia yang tersedia melalui AWS Data Exchange dalam urutan sebagai berikut:

1. `POST CreateJob`: API Operasi ini mengirimkan informasi pekerjaan kepada penyedia untuk diproses. Informasi ini adalah tentang jenis pekerjaan; Encoding atau Transcoding, lokasi S3, Skema yang disediakan oleh pelanggan, dan properti pekerjaan tambahan yang diperlukan.

Ini API mengembalikan a`JobId`, dan Status untuk Job akan menjadi salah satu dari yang berikut:`PENDING`,`READY`,`IN_PROGRESS`,`COMPLETE`, atau`FAILED`.

Permintaan sampel untuk pengkodean

```
POST /jobs
{
  "actionType": "ID_ASSIGNMENT",
  "s3SourceLocation": "string",
  "s3TargetLocation": "string",
  "jobProperties": {
    "assignmentJobProperties": {
      "fieldMappings": [
        {
          "name": "string",
          "type": "NAME"
        }
      ]
    }
  },
  "customerSpecifiedJobProperties": {
    "property1": "string",
    "property2": "string"
  },
  "outputSourceConfiguration": {
    "KMSArn": "string"
  }
}
```

Sampel respon

```
{
  "jobId": "string",
  "status": "PENDING"
}
```

2. `POST StartJob`: Ini API memungkinkan penyedia tahu untuk memulai pekerjaan berdasarkan yang `JobId` disediakan. Ini memungkinkan penyedia untuk melakukan validasi apa pun yang diperlukan dari `CreateJob` sampai. `StartJob`

   Ini API mengembalikan a`JobId`, `Status` untuk Job`statusMessage`, dan`statusCode`.

Permintaan sampel untuk pengkodean

```
POST/jobs/{jobId}
{
  "customerSpecifiedJobProperties": {
    "property1": "string",
    "property2": "string"
  }
}
```

Sampel respon

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

3. `GET GetJob`: Ini API menginformasikan Resolusi Entitas AWS jika pekerjaan telah selesai atau status lainnya.

   Ini API mengembalikan a`JobId`, `Status` untuk Job`statusMessage`, dan`statusCode`.

   Permintaan sampel untuk pengkodean

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

   Sampel respon

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

Definisi lengkap dari ini APIs disediakan dalam Resolusi Entitas AWS APISpesifikasi terbuka.

Integrasi pemrosesan sinkron

Solusi pemrosesan sinkron lebih diinginkan untuk penyedia yang memiliki waktu respons mendekati waktu nyata dengan waktu respons waktu nyata dengan throughput yang lebih tinggi dan lebih tinggi. TPS Ini Resolusi Entitas AWS alur kerja mempartisi dataset dan membuat beberapa permintaan secara API paralel. Bagian Resolusi Entitas AWS alur kerja kemudian menangani penulisan hasil ke lokasi output yang diinginkan.

Proses ini diaktifkan menggunakan salah satu API definisi. Resolusi Entitas AWS memanggil titik akhir penyedia yang tersedia melalui AWS Data Exchange:

`POST AssignIdentities`: Ini API mengirimkan data ke penyedia menggunakan `source_id` pengenal dan `recordFields` terkait dengan catatan itu.

Ini API mengembalikan`assignedRecords`.

Permintaan sampel untuk pengkodean

```
POST /assignment
{
  "sourceRecords": [
    {
      "sourceId": "string",
      "recordFields": [
        {
          "name": "string",
          "type": "NAME",
          "value": "string"
        }
      ]
    }
  ]
}
```

Sampel respon

```
{
  "assignedRecords": [
    {
      "sourceRecord": {
        "sourceId": "string",
```

```
        "recordFields": [
          {
            "name": "string",
            "type": "NAME",
            "value": "string"
          }
        ]
      },
      "identity": any
    }
  ]
}
```

Definisi lengkap dari ini APIs disediakan dalam Resolusi Entitas AWS APISpesifikasi terbuka.

Tergantung pada pendekatan mana yang dipilih penyedia, Resolusi Entitas AWS akan membuat konfigurasi untuk penyedia yang akan digunakan untuk memulai pengkodean atau transcoding. Selain itu, konfigurasi ini tersedia untuk pelanggan menggunakan yang APIs disediakan oleh Resolusi Entitas AWS.

Konfigurasi ini dapat diakses menggunakan Amazon Resource Name (ARN), yang berasal dari tempat layanan penyedia menawarkan AWS Data Exchange di-host, dan jenis layanan penyedia. Resolusi Entitas AWS mengacu pada ini ARN sebagai`providerServiceARN`.

Menguji integrasi penyedia

Sementara Resolusi Entitas AWS menghosting layanan pencocokan data, integrasi penyedia adalah komponen pihak ketiga yang penting untuk alur kerja end-to-end yang cocok. Ada beberapa tes yang Resolusi Entitas AWS telah menetapkan untuk penyedia yang menambahkan perlindungan ketika integrasi ini gagal. Pendekatan ini memberikan kesempatan bagi penyedia untuk memantau kesehatan layanan mereka sesuai dengan kasus end-to-end uji ini.

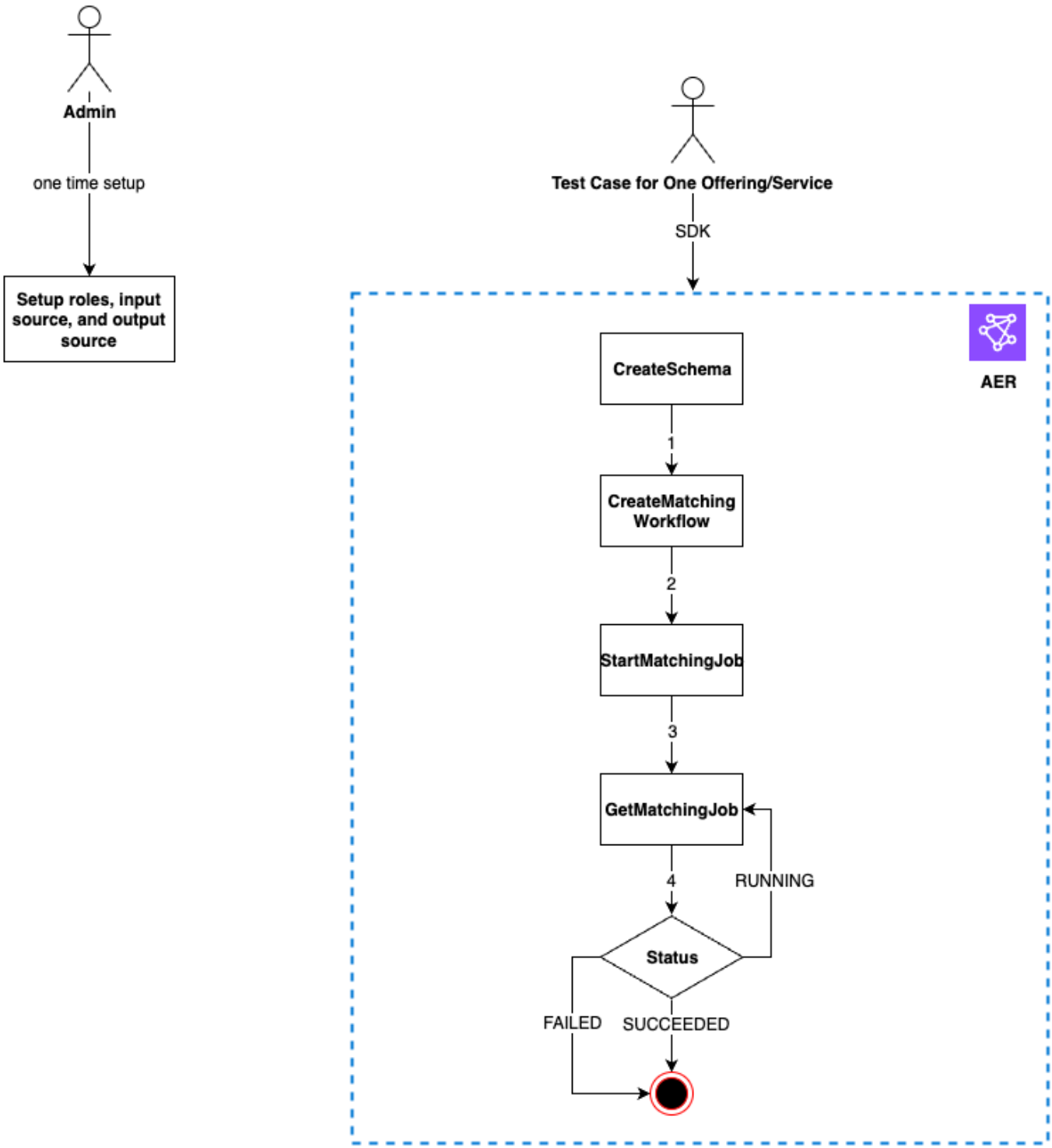
Penyedia dapat menggunakan akun pengujian dan data mereka sendiri untuk menjalankan kasus end-to-end uji ini menggunakan Resolusi Entitas AWS Kit Pengembangan Perangkat Lunak (SDK). Jika ada masalah dari penyedia, Resolusi Entitas AWS menggunakan jalur eskalasi yang disukai untuk meningkatkan masalah. Selain itu, penyedia perlu menerapkan pemantauan mereka sendiri pada hasil tes. Penyedia harus berbagi Akun AWS IDsyang digunakan untuk menjalankan tes ini dengan Resolusi Entitas AWS.

Jalankan yang sukses berarti penyedia dapat mengatur data mereka, menggunakan layanan mereka sendiri melalui Resolusi Entitas AWS, dan status pekerjaan kembali Selesai tanpa kesalahan. Hal ini dapat dilakukan secara terprogram menggunakan yang disediakan oleh APIs Resolusi Entitas AWS.

Misalnya, penyedia dapat mengatur bucket S3, sumber input, peran, skema, dan alur kerja sesuai dengan layanan mereka. Setelah pengaturan ini selesai, penyedia dapat menjalankan alur kerja ini sekali sehari dengan 200 catatan untuk menguji layanan mereka. Dalam pendekatan ini, penyedia menggunakan pilihan mereka SDK dan menjalankan end-to-end tes untuk layanan mereka yang ditawarkan melalui AWS Data Exchange menggunakan akun uji mereka. Penyedia diharapkan untuk menjalankan tes ini untuk setiap penawaran atau layanan mereka.

> **Note**
>
> Penyedia harus menyediakan Resolusi Entitas AWS sang Akun AWS ID (`accountId`)yang mereka gunakan untuk menjalankan alur kerja ini untuk pengujian. Selain itu, penyedia perlu memantau tes ini dan memastikan bahwa mereka lulus, yang berarti bahwa penyedia perlu mengaktifkan pemberitahuan jika terjadi kegagalan untuk mengatasi masalah yang sesuai.

Diagram berikut menunjukkan kasus uji end-to-end alur kerja yang khas.



Untuk menguji integrasi penyedia

1. (Penyiapan satu kali) Siapkan sumber daya untuk Resolusi Entitas AWS dengan mengikuti prosedur diMengatur Resolusi Entitas AWS.

Setelah menyelesaikan prosedur penyiapan satu kali, Anda harus menyiapkan peran, data, dan sumber data Anda. Anda sekarang siap untuk menguji integrasi penyedia menggunakan salah satu Resolusi Entitas AWS konsol atauAPIs.

2. Uji integrasi penyedia menggunakan salah satu Resolusi Entitas AWS APIsatau konsol.

API

Untuk menguji integrasi penyedia menggunakan Resolusi Entitas AWS APIs

1. Buat pemetaan skema menggunakan file. CreateSchemaMapping API Untuk daftar lengkap bahasa pemrograman yang didukung, lihat bagian Lihat Juga pada bagian CreateSchemaMapping API.

   Pemetaan skema adalah proses yang Anda beri tahu Resolusi Entitas AWS bagaimana menafsirkan data Anda untuk pencocokan. Anda menentukan skema tabel data input yang ingin Anda baca Resolusi AWS Entitas ke dalam alur kerja yang cocok.

   Saat membuat pemetaan skema, pengenal unik harus ditunjuk dan ditetapkan ke setiap baris data masukan yang dibaca oleh Resolusi AWS Entitas. Misalnya:`Primary_key`,`Row_ID`,`Record_ID`.

   Example Membuat pemetaan skema untuk sumber data yang berisi dan **`idemail`**

   Berikut ini adalah contoh pemetaan skema untuk sumber data yang berisi `id` dan: `email`

```
[
  {
    "fieldName": "id",
    "type": "UNIQUE_ID"
  },
  {
    "fieldName": "email",
    "type": "EMAIL_ADDRESS"
  }
]
```

Example Membuat pemetaan skema untuk sumber data yang berisi **`id`** dan **`email`** menggunakan Java SDK

Berikut ini adalah contoh pemetaan skema untuk sumber data yang berisi `id` dan `email` menggunakan Java: SDK

```
EntityResolutionClient.createSchemaMapping(
            CreateSchemaMappingRequest.builder()
                                        .schemaName(<schema-name>)
                                        .mappedInputFields([

 SchemaInputAttribute.builder().fieldName("id").type("UNIQUE_ID").build(),

 SchemaInputAttribute.builder().fieldName("email").type("EMAIL_ADDRESS").build()
                                         ])
                                        .build()

)
```

2. Buat alur kerja yang cocok menggunakan file. CreateMatchingWorkflow API Untuk daftar lengkap bahasa pemrograman yang didukung, lihat bagian Lihat Juga pada bagian CreateMatchingWorkflow API.

   Example Membuat alur kerja yang cocok menggunakan Java SDK

   Berikut ini adalah contoh alur kerja yang cocok menggunakan JavaSDK:

```
EntityResolutionClient.createMatchingWorkflow(
            CreateMatchingWorkflowRequest.builder()
                                         .workflowName(<workflow-name>)
                                         .inputSourceConfig(

 InputSource.builder().inputSourceARN(<glue-inputsource-from-
step1>).schemaName(<schema-name-from-step2>).build()
                                         )

 .outputSourceConfig(OutputSource.builder().outputS3Path(<output-s3-
path>).output(<output-1>, <output-2>, <output-3>).build())

 .resolutionTechniques(ResolutionTechniques.builder()

   .resolutionType(PROVIDER)
```

```
   .providerProperties(ProviderProperties.builder()
                                          .providerServiceArn(<provider-arn>)
                                           .providerConfiguration(<configuration-
depending-on-service>)

 .intermediateSourceConfiguration(<intermedaite-s3-path>)
                                          .build())
   .build()
                                          .roleArn(<role-from-step1>)
                                          .build()

)
```

Setelah alur kerja yang cocok disiapkan, Anda dapat menjalankan alur kerja.

3. Jalankan alur kerja yang cocok menggunakan file. StartMatchingJob API Untuk menjalankan alur kerja yang cocok, Anda harus membuat alur kerja yang cocok menggunakan titik akhir. `CreateMatchingWorkflow`

   Untuk daftar lengkap bahasa pemrograman yang didukung, lihat bagian Lihat Juga pada bagian StartMatchingJob API.

   Example Menjalankan alur kerja yang cocok menggunakan Java SDK

   Berikut ini adalah contoh alur kerja pencocokan yang berjalan menggunakan JavaSDK:

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

4. Pantau status alur kerja menggunakan file. GetMatchingJob API

   Ini API mengembalikan status, metrik, dan kesalahan (jika ada) yang terkait dengan pekerjaan.

Example Memantau alur kerja yang cocok menggunakan Java SDK

Berikut ini adalah contoh pemantauan pekerjaan alur kerja yang cocok menggunakan JavaSDK:

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

end-to-end Tes selesai jika alur kerja telah selesai dengan sukses.

Console

Untuk menguji integrasi penyedia menggunakan Resolusi Entitas AWS konsol

1. Buat pemetaan skema dengan mengikuti langkah-langkah di. Membuat pemetaan skema

   Pemetaan skema adalah proses yang Anda beri tahu Resolusi Entitas AWS bagaimana menafsirkan data Anda untuk pencocokan. Anda menentukan skema tabel data input yang Anda inginkan Resolusi Entitas AWS untuk membaca alur kerja yang cocok.

   Saat membuat pemetaan skema, pengidentifikasi unik harus ditunjuk dan ditetapkan ke setiap baris data masukan yang Resolusi Entitas AWS membaca. Misalnya:`Primary_key`,`Row_ID`,`Record_ID`.

   Example Pemetaan skema untuk sumber data yang mengandung dan **`idemail`**

   Berikut ini adalah contoh pemetaan skema untuk sumber data yang berisi `id` dan: `email`

```
[
  {
    "fieldName": "id",
    "type": "UNIQUE_ID"
  },
  {
    "fieldName": "email",
    "type": "EMAIL_ADDRESS"
  }
```

```
]
```

2. Buat dan jalankan alur kerja yang cocok dengan mengikuti langkah-langkah diMembuat alur kerja pencocokan berbasis layanan penyedia.

   Membuat alur kerja yang cocok adalah proses yang Anda atur untuk menentukan data input agar cocok bersama dan bagaimana pencocokan harus dilakukan. Dalam alur kerja berbasis penyedia, jika akun memiliki langganan dengan layanan penyedia melalui AWS Data Exchange, Anda dapat mencocokkan pengenal yang dikenal dengan penyedia pilihan Anda. Bergantung pada penyedia dan layanan mana yang Anda gunakan untuk melakukan pengujian ujung ke ujung, Anda dapat mengonfigurasi alur kerja yang sesuai.

   Bagian Resolusi Entitas AWS konsol menggabungkan tindakan buat dan jalankan dalam satu tombol. Setelah Anda memilih Buat dan jalankan, sebuah pesan muncul, yang menunjukkan bahwa alur kerja yang cocok telah dibuat dan bahwa pekerjaan telah dimulai.
3. Pantau status alur kerja pada halaman Pencocokan alur kerja.

   end-to-end Pengujian selesai jika alur kerja telah selesai dengan sukses (Status Job Selesai).

   Pada tab Metrik pada halaman detail alur kerja yang cocok, Anda dapat melihat yang berikut ini di bawah Metrik pekerjaan terakhir:

   - ID Job.
   - Status pekerjaan alur kerja yang cocok: Antrian, Sedang berlangsung, Selesai, Gagal
   - Waktu selesai untuk pekerjaan alur kerja.
   - Jumlah Rekaman yang diproses.
   - Jumlah Rekaman yang tidak diproses.
   - Pertandingan Unik IDs yang dihasilkan.
   - Jumlah catatan Input.

   Anda juga dapat melihat metrik pekerjaan untuk mencocokkan pekerjaan alur kerja yang sebelumnya telah dijalankan di bawah riwayat Job.

Keamanan di Resolusi Entitas AWS

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud - AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan Layanan AWS diAWS Cloud. AWSjuga menyediakan layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi secara berkala efektivitas keamanan kami sebagai bagian dari Program Kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku diResolusi Entitas AWS, lihat AWSLayanan dalam Cakupan melalui Program Kepatuhan AWS .
- Keamanan dalam cloud — Tanggung jawab Anda ditentukan oleh Layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan regulasi yang berlaku.

Dokumentasi ini akan membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Resolusi Entitas AWS. Topik berikut menunjukkan cara mengonfigurasi Resolusi Entitas AWS untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan Layanan AWS yang lain yang membantu Anda untuk memantau dan mengamankan Resolusi Entitas AWS sumber daya Anda.

Topik

Perlindungan data di Resolusi Entitas AWS

Bagian AWS model tanggung jawab bersama model berlaku untuk perlindungan data di Resolusi Entitas AWS. Seperti yang dijelaskan dalam model ini, AWS bertanggung jawab untuk melindungi

infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk menjaga kontrol atas konten Anda yang di-host di infrastruktur ini. Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat AWS Model Tanggung Jawab Bersama dan posting GDPR blog di AWS Blog Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda untuk melindungi Akun AWS kredensi dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS kegiatan, lihat Bekerja dengan CloudTrail jalan setapak di AWS CloudTrail Panduan Pengguna.
- Gunakan AWS solusi enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atauAPI, gunakan FIPS titik akhir. Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Resolusi Entitas AWS atau lainnya Layanan AWS menggunakan konsol,API, AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensil dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi data saat istirahat untuk Resolusi Entitas AWS

Resolusi Entitas AWS menyediakan enkripsi secara default untuk melindungi data pelanggan sensitif saat istirahat menggunakan AWS kunci enkripsi yang dimiliki.

AWSkunci yang dimiliki — Resolusi Entitas AWS menggunakan kunci ini secara default untuk secara otomatis mengenkripsi data yang dapat diidentifikasi secara pribadi. Anda tidak dapat melihat, mengelola, atau menggunakan AWS memiliki kunci, atau mengaudit penggunaannya. Namun, Anda tidak perlu mengambil tindakan apa pun untuk melindungi kunci yang mengenkripsi data Anda. Untuk informasi selengkapnya, lihat kunci yang AWS dimiliki di AWS Key Management Service Panduan Pengembang.

Enkripsi data saat istirahat secara default membantu mengurangi overhead operasional dan kompleksitas yang terlibat dalam melindungi data sensitif. Pada saat yang sama, Anda dapat menggunakannya untuk membangun aplikasi aman yang memenuhi kepatuhan enkripsi yang ketat dan persyaratan peraturan.

Atau, Anda juga dapat memberikan KMS kunci terkelola pelanggan untuk enkripsi saat membuat sumber daya alur kerja yang cocok.

Kunci terkelola pelanggan - Resolusi Entitas AWS mendukung penggunaan KMS kunci terkelola pelanggan simetris yang Anda buat, miliki, dan kelola untuk memungkinkan enkripsi data sensitif Anda. Karena Anda memiliki kontrol penuh atas lapisan enkripsi ini, Anda dapat melakukan tugas-tugas seperti:

- Menetapkan dan memelihara kebijakan utama
- Menetapkan dan memelihara IAM kebijakan dan hibah
- Mengaktifkan dan menonaktifkan kebijakan utama
- Memutar bahan kriptografi kunci
- Menambahkan tanda
- Membuat alias kunci
- Kunci penjadwalan untuk penghapusan

Untuk informasi selengkapnya, lihat kunci terkelola pelanggan di AWS Key Management Service Panduan Pengembang.

Untuk informasi lebih lanjut tentang AWS KMS, lihat Apa itu Layanan Manajemen AWS Kunci?

Manajemen kunci

Bagaimana Resolusi Entitas AWS menggunakan hibah di AWS KMS

Resolusi Entitas AWS membutuhkan hibah untuk menggunakan kunci yang dikelola pelanggan Anda. Saat Anda membuat alur kerja yang cocok yang dienkripsi dengan kunci yang dikelola pelanggan, Resolusi Entitas AWS membuat hibah atas nama Anda dengan mengirimkan CreateGrantpermintaan ke AWS KMS. Hibah di AWS KMS digunakan untuk memberi Resolusi Entitas AWS akses ke KMS kunci di akun pelanggan. Resolusi Entitas AWS memerlukan hibah untuk menggunakan kunci yang dikelola pelanggan Anda untuk operasi internal berikut:

- Kirim GenerateDataKeypermintaan ke AWS KMS untuk menghasilkan kunci data yang dienkripsi oleh kunci yang dikelola pelanggan Anda.
- Kirim permintaan Dekripsi ke AWS KMS untuk mendekripsi kunci data terenkripsi sehingga mereka dapat digunakan untuk mengenkripsi data Anda.

Anda dapat mencabut akses ke hibah, atau menghapus akses layanan ke kunci yang dikelola pelanggan kapan saja. Jika Anda melakukannya, Resolusi Entitas AWS tidak akan dapat mengakses data apa pun yang dienkripsi oleh kunci yang dikelola pelanggan, yang memengaruhi operasi yang bergantung pada data tersebut. Misalnya, jika Anda menghapus akses layanan ke kunci Anda melalui hibah dan mencoba memulai pekerjaan untuk alur kerja yang cocok yang dienkripsi dengan kunci pelanggan, maka operasi akan mengembalikan kesalahan. `AccessDeniedException`

Membuat kunci yang dikelola pelanggan

Anda dapat membuat kunci terkelola pelanggan simetris dengan menggunakan AWS Management Console, atau AWS KMS APIs.

Untuk membuat kunci terkelola pelanggan simetris

Resolusi Entitas AWS mendukung enkripsi menggunakan KMSkunci enkripsi simetris. Ikuti langkah-langkah untuk Membuat kunci terkelola pelanggan simetris di AWS Key Management Service Panduan Pengembang.

Pernyataan kebijakan utama

Kebijakan utama mengontrol akses ke kunci yang dikelola pelanggan Anda. Setiap kunci yang dikelola pelanggan harus memiliki persis satu kebijakan utama, yang berisi pernyataan yang

menentukan siapa yang dapat menggunakan kunci dan bagaimana mereka dapat menggunakannya. Saat membuat kunci terkelola pelanggan, Anda dapat menentukan kebijakan kunci. Untuk informasi selengkapnya, lihat Mengelola akses ke kunci terkelola pelanggan di AWS Key Management Service Panduan Pengembang.

Untuk menggunakan kunci yang dikelola pelanggan Anda dengan Resolusi Entitas AWS sumber daya, API operasi berikut harus diizinkan dalam kebijakan utama:

- `kms:DescribeKey`— Memberikan informasi seperti kunciARN, tanggal pembuatan (dan tanggal penghapusan, jika berlaku), status kunci, dan tanggal asal dan kedaluwarsa (jika ada) dari materi utama. Ini termasuk bidang, sepertiKeySpec, yang membantu Anda membedakan berbagai jenis KMS kunci. Ini juga menampilkan penggunaan kunci (enkripsi, penandatanganan, atau pembuatan dan verifikasiMACs) dan algoritma yang didukung oleh KMS kunci. Resolusi Entitas AWS memvalidasi bahwa `KeySpec` adalah `SYMMETRIC_DEFAULT` dan `KeyUsage` sedang`ENCRYPT_DECRYPT`.
- `kms:CreateGrant`— Menambahkan hibah ke kunci yang dikelola pelanggan. Memberikan akses kontrol ke KMS kunci tertentu, yang memungkinkan akses ke operasi hibah Resolusi Entitas AWS membutuhkan. Untuk informasi selengkapnya tentang Menggunakan Hibah, lihat AWS Key Management Service Panduan Pengembang.

Hal ini memungkinkan Resolusi Entitas AWS untuk melakukan hal berikut:

- Panggilan `GenerateDataKey` untuk menghasilkan kunci data terenkripsi dan menyimpannya, karena kunci data tidak segera digunakan untuk mengenkripsi.
- Panggilan `Decrypt` untuk menggunakan kunci data terenkripsi yang disimpan untuk mengakses data terenkripsi.
- Siapkan kepala sekolah yang pensiun untuk memungkinkan layanan. `RetireGrant`

Berikut ini adalah contoh pernyataan kebijakan yang dapat Anda tambahkan Resolusi Entitas AWS:

```
{
      "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"
        }
      }
}
```

Izin untuk pengguna

Ketika Anda mengonfigurasi KMS kunci sebagai kunci default untuk enkripsi, kebijakan KMS kunci default memungkinkan setiap pengguna dengan akses ke KMS tindakan yang diperlukan untuk menggunakan KMS kunci ini untuk mengenkripsi atau mendekripsi sumber daya. Anda harus memberikan izin kepada pengguna untuk memanggil tindakan berikut agar dapat menggunakan enkripsi KMS kunci yang dikelola pelanggan:

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

Selama `CreateMatchingWorkflow`permintaan, Resolusi Entitas AWS akan mengirim DescribeKeydan CreateGrantpermintaan ke AWS KMS atas nama Anda. Ini akan mengharuskan IAM entitas yang membuat `CreateMatchingWorkflow` permintaan dengan KMS kunci yang dikelola pelanggan untuk memiliki `kms:DescribeKey` izin pada kebijakan KMS utama.

Selama permintaan `CreateIdMappingWorkflow`dan `StartIdMappingJob`permintaan, Resolusi Entitas AWS akan mengirim DescribeKeydan CreateGrantpermintaan ke AWS KMS atas nama Anda. Ini akan mengharuskan IAM entitas membuat `CreateIdMappingWorkflow` dan `StartIdMappingJob` meminta dengan KMS kunci yang dikelola pelanggan untuk memiliki `kms:DescribeKey` izin pada kebijakan KMS utama. Penyedia akan dapat mengakses kunci yang dikelola pelanggan untuk mendekripsi data di Resolusi Entitas AWS Bucket Amazon S3.

Berikut ini adalah contoh pernyataan kebijakan yang dapat Anda tambahkan untuk penyedia untuk mendekripsi data di Resolusi Entitas AWS Ember Amazon S3:

```
{
    "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"
            }
        }
    }]
}
```

Ganti masing-masing *<user input placeholder>* dengan informasi Anda sendiri.

<KMSKeyARN>	AWS KMS Nama Sumber Daya Amazon.

Demikian pula, IAM entitas yang memanggil `StartMatchingJob`API harus memiliki `kms:Decrypt` dan `kms:GenerateDataKey` izin pada KMS kunci terkelola pelanggan yang disediakan dalam alur kerja yang cocok.

Untuk informasi selengkapnya tentang menentukan izin dalam kebijakan, lihat AWS Key Management Service Panduan Pengembang.

Untuk informasi selengkapnya tentang pemecahan masalah akses kunci, lihat AWS Key Management Service Panduan Pengembang.

Menentukan kunci yang dikelola pelanggan untuk Resolusi Entitas AWS

Anda dapat menentukan kunci yang dikelola pelanggan sebagai enkripsi lapisan kedua untuk sumber daya berikut:

Alur kerja yang cocok - Saat Anda membuat sumber daya alur kerja yang cocok, Anda dapat menentukan kunci data dengan memasukkan, yang KMSArn Resolusi Entitas AWS digunakan untuk mengenkripsi data pribadi yang dapat diidentifikasi yang disimpan oleh sumber daya.

KMSArn— Masukkan kunciARN, yang merupakan pengidentifikasi kunci untuk AWS KMS kunci yang dikelola pelanggan.

Anda dapat menentukan kunci terkelola pelanggan sebagai enkripsi lapisan kedua untuk sumber daya berikut jika Anda membuat atau menjalankan alur kerja pemetaan ID di dua Akun AWS:

Alur kerja pemetaan ID atau Alur kerja pemetaan ID Mulai - Saat Anda membuat sumber daya alur kerja pemetaan ID atau memulai pekerjaan alur kerja pemetaan ID, Anda dapat menentukan kunci data dengan memasukkan, yang KMSArn Resolusi Entitas AWS digunakan untuk mengenkripsi data pribadi yang dapat diidentifikasi yang disimpan oleh sumber daya.

KMSArn— Masukkan kunciARN, yang merupakan pengidentifikasi kunci untuk AWS KMS kunci yang dikelola pelanggan.

Memantau kunci enkripsi Anda untuk Resolusi Entitas AWS Layanan

Saat Anda menggunakan AWS KMS kunci yang dikelola pelanggan dengan Anda Resolusi Entitas AWS Sumber daya layanan, Anda dapat menggunakan AWS CloudTrailatau Amazon CloudWatch Log untuk melacak permintaan itu Resolusi Entitas AWS mengirim ke AWS KMS.

Contoh berikut adalah AWS CloudTrail acara untuk`CreateGrant`,`GenerateDataKey`,`Decrypt`, dan `DescribeKey` untuk memantau AWS KMS Operasi yang disebut oleh Resolusi Entitas AWS untuk mengakses data yang dienkripsi oleh kunci yang dikelola pelanggan Anda:

Topik

- CreateGrant
- DescribeKey
- GenerateDataKey
- Dekripsi

CreateGrant

Saat Anda menggunakan AWS KMS kunci terkelola pelanggan untuk mengenkripsi sumber daya alur kerja yang cocok, Resolusi Entitas AWS mengirimkan `CreateGrant` permintaan atas nama Anda untuk mengakses KMS kunci di Akun AWS. Hibah yang Resolusi Entitas AWS create khusus untuk sumber daya yang terkait dengan AWS KMS kunci yang dikelola pelanggan. Selain itu, Resolusi Entitas AWS menggunakan `RetireGrant` operasi untuk menghapus hibah saat Anda menghapus sumber daya.

Contoh peristiwa berikut mencatat `CreateGrant` operasi:


```
{
    "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

Resolusi Entitas AWS menggunakan `DescribeKey` operasi untuk memverifikasi apakah AWS KMS kunci terkelola pelanggan yang terkait dengan sumber daya yang cocok ada di akun dan Wilayah.

Contoh peristiwa berikut mencatat `DescribeKey` operasi.

```
{
    "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

Saat Anda mengaktifkan AWS KMS kunci terkelola pelanggan untuk sumber daya alur kerja yang cocok, Resolusi Entitas AWS mengirimkan `GenerateDataKey` permintaan melalui Amazon Simple Storage Service (Amazon S3) ke AWS KMS yang menentukan AWS KMS kunci yang dikelola pelanggan untuk sumber daya.

Contoh peristiwa berikut mencatat `GenerateDataKey` operasi.


```
{
    "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"
}
```


Dekripsi

Saat Anda mengaktifkan AWS KMS kunci terkelola pelanggan untuk sumber daya alur kerja yang cocok, Resolusi Entitas AWS mengirimkan `Decrypt` permintaan melalui Amazon Simple Storage

Service (Amazon S3) ke AWS KMS yang menentukan AWS KMS kunci yang dikelola pelanggan untuk sumber daya.

Contoh peristiwa berikut mencatat `Decrypt` operasi.


```
{
    "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"
}
```

Pertimbangan

Resolusi Entitas AWS tidak mendukung pembaruan alur kerja yang cocok dengan KMS kunci terkelola pelanggan baru. Dalam kasus seperti itu, Anda dapat membuat alur kerja baru dengan KMS kunci yang dikelola pelanggan.

Pelajari selengkapnya

Sumber daya berikut memberikan informasi lebih lanjut tentang enkripsi data saat istirahat.

Untuk informasi selengkapnya tentang konsep dasar Layanan Manajemen AWS Kunci, lihat AWS Key Management Service Panduan Pengembang.

Untuk informasi selengkapnya tentang praktik terbaik Keamanan untuk Layanan Manajemen AWS Utama, lihat AWS Key Management Service Panduan Pengembang.

Akses Resolusi Entitas AWS menggunakan titik akhir antarmuka (AWS PrivateLink)

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara Anda VPC dan Resolusi Entitas AWS. Anda dapat mengakses Resolusi Entitas AWS seolah-olah itu ada di AndaVPC, tanpa menggunakan gateway internet, NAT perangkat, VPN koneksi, atau AWS Direct Connect koneksi. Instans di Anda VPC tidak memerlukan alamat IP publik untuk mengakses Resolusi Entitas AWS.

Anda membuat koneksi pribadi ini dengan membuat titik akhir antarmuka, didukung oleh AWS PrivateLink. Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola pemohon yang berfungsi sebagai titik masuk untuk lalu lintas yang ditakdirkan Resolusi Entitas AWS.

Untuk informasi selengkapnya, lihat Akses Layanan AWS lewat AWS PrivateLinkdi AWS PrivateLink Panduan.

Pertimbangan untuk Resolusi Entitas AWS

Sebelum Anda menyiapkan titik akhir antarmuka untuk Resolusi Entitas AWS, tinjau Pertimbangan di AWS PrivateLink Panduan.

Resolusi Entitas AWS mendukung membuat panggilan ke semua API tindakannya melalui titik akhir antarmuka.

VPCkebijakan endpoint didukung untuk Resolusi Entitas AWS. Secara default, akses penuh ke Resolusi Entitas AWS diizinkan melalui titik akhir antarmuka. Atau, Anda dapat mengaitkan grup keamanan dengan antarmuka jaringan titik akhir untuk mengontrol lalu lintas Resolusi Entitas AWS melalui titik akhir antarmuka.

Buat titik akhir antarmuka untuk Resolusi Entitas AWS

Anda dapat membuat titik akhir antarmuka untuk Resolusi Entitas AWS menggunakan VPC konsol Amazon atau AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLink Panduan.

Buat titik akhir antarmuka untuk Resolusi Entitas AWS menggunakan nama layanan berikut:

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

Jika Anda mengaktifkan privat DNS untuk titik akhir antarmuka, Anda dapat membuat API permintaan Resolusi Entitas AWS menggunakan DNS nama Regional defaultnya. Misalnya, `entityresolution.us-east-1.amazonaws.com`.

Buat kebijakan titik akhir untuk titik akhir antarmuka Anda

Kebijakan endpoint adalah IAM sumber daya yang dapat Anda lampirkan ke titik akhir antarmuka. Kebijakan endpoint default memungkinkan akses penuh ke Resolusi Entitas AWS melalui titik akhir antarmuka. Untuk mengontrol akses yang diizinkan Resolusi Entitas AWS dari AndaVPC, lampirkan kebijakan titik akhir kustom ke titik akhir antarmuka.

kebijakan titik akhir mencantumkan informasi berikut:

- Prinsipal yang dapat melakukan tindakan (Akun AWS, IAM pengguna, dan IAM peran).
- Tindakan yang dapat dilakukan.
- Sumber daya untuk melakukan tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan menggunakan kebijakan titik akhir di AWS PrivateLink Panduan.

Contoh: kebijakan VPC endpoint untuk Resolusi Entitas AWS tindakan

Berikut ini adalah contoh kebijakan endpoint kustom. Saat Anda melampirkan kebijakan ini ke titik akhir antarmuka Anda, kebijakan ini akan memberikan akses ke yang tercantum Resolusi Entitas AWS tindakan untuk semua kepala sekolah pada semua sumber daya.

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

Manajemen identitas dan akses untuk Resolusi Entitas AWS

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAMadministrator mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. Resolusi Entitas AWS IAMadalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

> **Note**
>
> Resolusi Entitas AWS mendukung kebijakan lintas akun. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun IAM di Panduan IAM Pengguna.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Resolusi Entitas AWS bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk Resolusi Entitas AWS
- AWS kebijakan terkelola untuk Resolusi Entitas AWS
- Memecahkan masalah Resolusi Entitas AWS identitas dan akses

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan Resolusi Entitas AWS.

Pengguna layanan — Jika Anda menggunakan Resolusi Entitas AWS layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak Resolusi Entitas AWS fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Resolusi Entitas AWS, lihat Memecahkan masalah Resolusi Entitas AWS identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas Resolusi Entitas AWS sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke Resolusi Entitas AWS. Tugas Anda adalah menentukan Resolusi Entitas AWS fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasarIAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakannya IAM Resolusi Entitas AWS, lihatBagaimana Resolusi Entitas AWS bekerja dengan IAM.

IAMadministrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses Resolusi Entitas AWS. Untuk melihat contoh kebijakan Resolusi Entitas AWS berbasis identitas yang dapat Anda gunakan, lihat. IAM Contoh kebijakan berbasis identitas untuk Resolusi Entitas AWS

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peranIAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Versi AWS Tanda Tangan 4 untuk API permintaan di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor di Panduan AWS IAM Identity Center Pengguna dan Autentikasi AWS multi-faktor IAM di Panduan Pengguna. IAM

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di IAMPanduan Pengguna.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensi yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat IAM Identitas, lihat Apa itu Pusat IAM Identitas? dalam AWS IAM Identity Center User Guide.

Pengguna dan grup IAM

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensi jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk IAM pengguna di Panduan IAM Pengguna.

IAMperan

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Untuk mengambil IAM peran sementara di dalam AWS Management Console, Anda dapat beralih dari pengguna ke IAM peran (konsol). Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Metode untuk mengambil peran dalam Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas mengkorelasikan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.
  - Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.

  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredensil sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat Ringkasan JSON kebijakan di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Menentukan IAM izin khusus dengan kebijakan yang dikelola pelanggan di Panduan Pengguna. IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat Memilih antara kebijakan terkelola dan kebijakan sebaris di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan IAM Pengguna.

Bagaimana Resolusi Entitas AWS bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses Resolusi Entitas AWS, pelajari IAM fitur apa yang tersedia untuk digunakan Resolusi Entitas AWS.

IAMfitur yang dapat Anda gunakan dengan Resolusi Entitas AWS

IAMfitur	Resolusi Entitas AWS dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Ya
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC(tag dalam kebijakan)	Parsial
Kredensial sementara	Ya
Teruskan sesi akses (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara Resolusi Entitas AWS dan AWS layanan lain bekerja dengan sebagian besar IAM fitur, lihat AWS layanan yang berfungsi IAM di Panduan IAM Pengguna.

Kebijakan berbasis identitas untuk Resolusi Entitas AWS

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Menentukan IAM izin khusus dengan kebijakan yang dikelola pelanggan di Panduan Pengguna. IAM

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk Resolusi Entitas AWS

Untuk melihat contoh kebijakan Resolusi Entitas AWS berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk Resolusi Entitas AWS

Kebijakan berbasis sumber daya dalam Resolusi Entitas AWS

Mendukung kebijakan berbasis sumber daya: Ya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau IAM entitas di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak

diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun IAM di Panduan IAM Pengguna.

Tindakan kebijakan untuk Resolusi Entitas AWS

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

`Action`Elemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar Resolusi Entitas AWS tindakan, lihat Tindakan yang Ditentukan oleh Resolusi Entitas AWS dalam Referensi Otorisasi Layanan.

Tindakan kebijakan Resolusi Entitas AWS menggunakan awalan berikut sebelum tindakan:

```
entityresolution
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

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

Untuk melihat contoh kebijakan Resolusi Entitas AWS berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk Resolusi Entitas AWS

Sumber daya kebijakan untuk Resolusi Entitas AWS

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya dan jenis Resolusi Entitas AWS sumber dayaARNs, lihat Sumber Daya yang Ditentukan oleh Resolusi Entitas AWS dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh Resolusi Entitas AWS.

Untuk melihat contoh kebijakan Resolusi Entitas AWS berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk Resolusi Entitas AWS

Kunci kondisi kebijakan untuk Resolusi Entitas AWS

Mendukung kunci kondisi kebijakan khusus layanan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan IAM Pengguna.

Untuk melihat daftar kunci Resolusi Entitas AWS kondisi, lihat Kunci Kondisi untuk Resolusi Entitas AWS Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang Ditentukan oleh Resolusi Entitas AWS.

Untuk melihat contoh kebijakan Resolusi Entitas AWS berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk Resolusi Entitas AWS

ACLsdi Resolusi Entitas AWS

MendukungACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

ABACdengan Resolusi Entitas AWS

Mendukung ABAC (tag dalam kebijakan): Sebagian

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari. ABAC Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABACmembantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnyaABAC, lihat Menentukan izin dengan ABAC otorisasi di IAMPanduan Pengguna. Untuk melihat tutorial dengan langkah-langkah penyiapanABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di IAMPanduan Pengguna.

Menggunakan kredensi sementara dengan Resolusi Entitas AWS

Mendukung kredensi sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensil sementara, lihat Layanan AWS yang berfungsi IAM di IAMPanduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat Beralih dari pengguna ke IAM peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensi sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensi sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensi keamanan sementara di. IAM

Teruskan sesi akses untuk Resolusi Entitas AWS

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah

tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.

Peran layanan untuk Resolusi Entitas AWS

Mendukung peran layanan: Ya

Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak Resolusi Entitas AWS fungsionalitas. Edit peran layanan hanya jika Resolusi Entitas AWS memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Resolusi Entitas AWS

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan, lihat AWS layanan yang berfungsi dengannya. IAM Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Resolusi Entitas AWS

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi Resolusi Entitas AWS sumber daya. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS

Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat Membuat JSON IAM kebijakan (konsol) di Panduan Pengguna. IAM

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Resolusi Entitas AWS, termasuk format ARNs untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Resolusi Entitas AWS dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Resolusi Entitas AWS
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus Resolusi Entitas AWS sumber daya di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan AWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di IAM Panduan Pengguna.

- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakanSSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat elemen IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM IAMAccess Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Memvalidasi kebijakan dengan IAM Access Analyzer di IAMPanduan Pengguna.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di dalam Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat APIAkses aman dengan MFA di Panduan IAM Pengguna.

Untuk informasi selengkapnya tentang praktik terbaik diIAM, lihat Praktik terbaik keamanan IAM di Panduan IAM Pengguna.

Menggunakan konsol Resolusi Entitas AWS

Untuk mengakses Resolusi Entitas AWS konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang Resolusi Entitas AWS sumber daya di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau. AWS API Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan API operasi yang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan Resolusi Entitas AWS konsol, lampirkan juga kebijakan Resolusi Entitas AWS `ConsoleAccess` atau `ReadOnly` AWS

terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna di Panduan IAM Pengguna.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan IAM pengguna melihat kebijakan sebaris dan terkelola yang dilampirkan pada identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan atau. AWS CLI AWS API

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

AWS kebijakan terkelola untuk Resolusi Entitas AWS

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSEntityResolutionConsoleFullAccess

Anda dapat melampirkan kebijakan `AWSEntityResolutionConsoleFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan akses penuh ke Resolusi Entitas AWS titik akhir dan sumber daya.

Kebijakan ini juga memungkinkan akses baca tertentu ke terkait Layanan AWS seperti S3, AWS Glue, Tagging, dan AWS KMS konsol dapat menampilkan pilihan dan menggunakan pilihan yang dipilih untuk melakukan tindakan resolusi entitas. Beberapa sumber daya dipersempit untuk memuat nama `entityresolution` layanan.

Karena Resolusi Entitas AWS bergantung pada peran yang diteruskan untuk melakukan tindakan pada AWS sumber daya terkait, kebijakan ini juga memberikan izin untuk memilih dan meneruskan peran yang diinginkan.

Detail izin

Kebijakan ini mencakup izin berikut.

- `EntityResolutionAccess`— Memungkinkan kepala sekolah akses penuh ke titik Resolusi Entitas AWS akhir dan sumber daya.
- `GlueSourcesConsoleDisplay`— Memberikan akses ke daftar AWS Glue tabel sebagai opsi sumber data dan skema tabel impor sumber data untuk pengalaman pengguna.
- `S3BucketsConsoleDisplay`— Memberikan akses untuk mencantumkan semua bucket S3 sebagai opsi sumber data.
- `S3SourcesConsoleDisplay`— Memberikan akses untuk menampilkan bucket S3 sebagai opsi sumber data.
- `TaggingConsoleDisplay`— Memberikan akses untuk membaca kunci dan nilai penandaan.
- `KMSConsoleDisplay`Memberikan akses untuk mendeskripsikan kunci dan daftar alias AWS Key Management Service untuk mendekripsi dan mengenkripsi sumber data.
- `ListRolesToPickForPassing`— Memberikan akses untuk membuat daftar semua peran sehingga pengguna dapat memilih peran yang akan diteruskan.
- `PassRoleToEntityResolutionService`— Memberikan akses untuk meneruskan peran yang dipersempit ke layanan. Resolusi Entitas AWS
- `ManageEventBridgeRules`— Memberikan akses untuk membuat, memperbarui, dan menghapus EventBridge aturan Amazon untuk mendapatkan pemberitahuan S3.
- `ADXReadAccess`— Memberikan akses AWS Data Exchange untuk memverifikasi apakah pelanggan memiliki hak atau berlangganan.

```
{
    "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 kebijakan terkelola: AWSEntityResolutionConsoleReadOnlyAccess

Anda dapat melampirkan `AWSEntityResolutionConsoleReadOnlyAccess` ke entitas IAM Anda.

Kebijakan ini memberikan akses hanya-baca ke titik Resolusi Entitas AWS akhir dan sumber daya.

Detail izin

Kebijakan ini mencakup izin berikut.

- `EntityResolutionRead`— Memungkinkan akses hanya-baca kepala sekolah ke titik akhir dan sumber daya. Resolusi Entitas AWS

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

Resolusi Entitas AWS pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola Resolusi Entitas AWS sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat Resolusi Entitas AWS dokumen.

Perubahan	Deskripsi	Tanggal
`AWSEntityResolutionConsoleFullAccess` – Pembaruan ke kebijakan yang sudah ada	Ditambahkan `ADXReadAccess` dan `ManageEventBridgeRules` untuk mengaktifkan opsi layanan penyedia dalam alur kerja yang cocok.	16 Oktober 2023
Resolusi Entitas AWS mulai melacak perubahan	Resolusi Entitas AWS mulai melacak perubahan untuk kebijakan yang AWS dikelola.	18 Agustus 2023

Memecahkan masalah Resolusi Entitas AWS identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Resolusi Entitas AWS danIAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Resolusi Entitas AWS
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses Resolusi Entitas AWS sumber daya saya

Saya tidak berwenang untuk melakukan tindakan di Resolusi Entitas AWS

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberikan nama pengguna dan kata sandi Anda.

Contoh kesalahan berikut terjadi ketika `mateojackson` IAM pengguna mencoba menggunakan konsol untuk melihat detail tentang *`my-example-widget`* sumber daya fiksi tetapi tidak memiliki izin `entityresolution:`*`GetWidget`* fiksi.

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

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *my-example-widget* menggunakan tindakan `entityresolution:`*GetWidget*.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran Resolusi Entitas AWS.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Resolusi Entitas AWS. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses Resolusi Entitas AWS sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Resolusi Entitas AWS mendukung fitur ini, lihatBagaimana Resolusi Entitas AWS bekerja dengan IAM.

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki di Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna yang diautentikasi secara eksternal (federasi identitas) di Panduan Pengguna. IAM
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

Validasi kepatuhan untuk Resolusi Entitas AWS

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk HIPAA Keamanan dan Kepatuhan di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat HIPAA aplikasi yang memenuhi syarat.

> **Note**
>
> Tidak semua Layanan AWS HIPAA memenuhi syarat. Untuk informasi selengkapnya, lihat Referensi Layanan yang HIPAA Memenuhi Syarat.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi ()). ISO
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCIDSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Resolusi Entitas AWS praktik terbaik kepatuhan

Bagian ini memberikan praktik dan rekomendasi terbaik untuk kepatuhan saat Anda menggunakannya Resolusi Entitas AWS.

Standar Keamanan Data Industri Kartu Pembayaran (PCIDSS)

Resolusi Entitas AWS mendukung pemrosesan, penyimpanan, dan transmisi data kartu kredit oleh pedagang atau penyedia layanan, dan telah divalidasi sebagai sesuai dengan Industri Kartu Pembayaran (PCI) Standar Keamanan Data (DSS). Untuk informasi selengkapnya PCIDSS, termasuk cara meminta salinan Paket AWS PCI Kepatuhan, lihat PCIDSSLevel 1.

Sistem dan Kontrol Organisasi (SOC)

Resolusi Entitas AWS sesuai dengan langkah-langkah Kontrol Sistem dan Organisasi (SOC), termasuk SOC 1, SOC 2, dan SOC 3. SOClaporan independen, laporan pemeriksaan pihak ketiga yang menunjukkan bagaimana AWS mencapai kontrol dan tujuan kepatuhan utama. Audit ini memastikan adanya perlindungan dan prosedur yang sesuai untuk melindungi dari risiko yang dapat memengaruhi keamanan, kerahasiaan, dan ketersediaan data pelanggan dan perusahaan. Hasil audit pihak ketiga ini tersedia di situs web AWS SOC Kepatuhan, di mana Anda dapat melihat laporan yang dipublikasikan untuk mendapatkan informasi lebih lanjut tentang kontrol yang mendukung AWS operasi dan kepatuhan.

Ketahanan di Resolusi Entitas AWS

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Resolusi Entitas AWS menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Pemantauan Resolusi Entitas AWS

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja Resolusi Entitas AWS dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton Resolusi Entitas AWS, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama Anda Akun AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Topik

Logging panggilan Resolusi Entitas AWS API menggunakan AWS CloudTrail

Resolusi Entitas AWS terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Resolusi Entitas AWS. CloudTrail menangkap semua panggilan API untuk Resolusi Entitas AWS sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari Resolusi Entitas AWS konsol dan panggilan kode ke operasi Resolusi Entitas AWS API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. Resolusi Entitas AWS Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat Resolusi Entitas AWS, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Resolusi Entitas AWS informasi di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Resolusi Entitas AWS, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa

AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk Resolusi Entitas AWS, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua Resolusi Entitas AWS tindakan dicatat oleh CloudTrail dan didokumentasikan dalam Referensi Resolusi Entitas AWS API.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.

Memahami entri file Resolusi Entitas AWS log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta,

tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Buat sumber daya Resolusi AWS Entitas dengan AWS CloudFormation

AWSResolusi Entitas terintegrasi dengan AWS CloudFormation, layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya Anda sehingga Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat template yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace dan AWS::EntityResolution::PolicyStatement), dan AWS CloudFormation ketentuan serta mengonfigurasi sumber daya tersebut untuk Anda.

Bila Anda menggunakan AWS CloudFormation, Anda dapat menggunakan kembali template Anda untuk mengatur sumber daya Resolusi AWS Entitas Anda secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

AWSResolusi Entitas dan AWS CloudFormation template

Untuk menyediakan dan mengonfigurasi sumber daya untuk Resolusi AWS Entitas dan layanan terkait, Anda harus memahami AWS CloudFormation templat. Template adalah file teks yang diformat dalam JSON atauYAML. Template ini menjelaskan sumber daya yang ingin Anda sediakan di AWS CloudFormation tumpukan Anda. Jika Anda tidak terbiasa dengan JSON atauYAML, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan AWS CloudFormation template. Untuk informasi selengkapnya, lihat Apa itu AWS CloudFormation Designer? di Panduan Pengguna AWS CloudFormation .

AWSResolusi Entitas mendukung pembuatan AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace dan AWS::EntityResolution::PolicyStatement masuk AWS CloudFormation. Untuk informasi selengkapnya, termasuk contoh JSON dan YAML templat untuk AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace dan AWS::EntityResolution::PolicyStatement, lihat referensi jenis sumber daya Resolusi AWS Entitas di Panduan AWS CloudFormation Pengguna.

Templat berikut ini tersedia:

- Alur kerja yang cocok

  Buat `MatchingWorkflow` objek, yang menyimpan konfigurasi pekerjaan pemrosesan data yang akan dijalankan.

  Untuk informasi selengkapnya, lihat topik berikut.

  AWS::EntityResolution::MatchingWorkflow di Panduan Pengguna AWS CloudFormation

  CreateMatchingWorkflowdalam Resolusi Entitas AWS APIReferensi
- Pemetaan skema

  Buat pemetaan skema, yang mendefinisikan skema tabel catatan pelanggan masukan.

  Untuk informasi selengkapnya, lihat topik berikut.

  AWS::EntityResolution::SchemaMapping di Panduan Pengguna AWS CloudFormation

  CreateSchemaMappingdalam Resolusi Entitas AWS APIReferensi
- Alur kerja pemetaan ID

  Buat `IdMappingWorkflow` objek, yang menyimpan konfigurasi pekerjaan pemrosesan data untuk dijalankan.

  Untuk informasi selengkapnya, lihat topik berikut.

  AWS::EntityResolution::IdMappingWorkflow di Panduan Pengguna AWS CloudFormation

  CreateIdMappingWorkflowdalam Resolusi Entitas AWS APIReferensi
- Ruang nama ID

  Buat `IdNamespace` objek, yang menyimpan metadata yang menjelaskan kumpulan data dan cara menggunakannya.

  Untuk informasi selengkapnya, lihat topik berikut.

  AWS::EntityResolution::IdNamespace di Panduan Pengguna AWS CloudFormation

  CreateIdNamespacedalam Resolusi Entitas AWS APIReferensi
- PolicyStatement

Buat `PolicyStatement` objek.

Untuk informasi selengkapnya, lihat topik berikut.

AWS::EntityResolution::PolicyStatement di Panduan Pengguna AWS CloudFormation

AddPolicyStatementdalam Resolusi Entitas AWS APIReferensi

Pelajari lebih lanjut tentang AWS CloudFormation

Untuk mempelajari selengkapnya AWS CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormation Panduan Pengguna
- AWS CloudFormation APIReferensi
- AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah

Kuota untuk Resolusi Entitas AWS

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing. Layanan AWS Kecuali dinyatakan lain, setiap kuota bersifat khusus per Wilayah. Anda dapat meminta kenaikan untuk beberapa kuota, tetapi kuota lain tidak dapat ditingkatkan.

Untuk melihat kuota Resolusi Entitas AWS, buka konsol Service Quotas. Di panel navigasi, pilih AWSlayanan dan pilih Resolusi Entitas AWS.

Untuk meminta peningkatan kuota, lihat Meminta Peningkatan Kuota dalam Panduan Pengguna Service Quotas. Jika kuota belum tersedia di Service Quotas, gunakan formulir kenaikan batas.

Anda Akun AWS memiliki kuota berikut yang terkait Resolusi Entitas AWS dengan.

Nama	Default	Dapat disesuaikan	Deskripsi
Lowongan kerja pemetaan ID bersamaan	1	Tidak	Jumlah maksimum pekerjaan pemetaan ID yang dapat diproses secara bersamaan di saat ini. Wilayah AWS
Lowongan kerja concurrent matching	1	Tidak	Jumlah maksimum pekerjaan yang cocok yang dapat diproses secara bersamaan di saat ini Wilayah AWS.
Pekerjaan pencocokan layanan penyedia bersamaan	1	Tidak	Jumlah maksimum pekerjaan pencocokan layanan penyedia yang dapat diproses secara bersamaan di saat ini Wilayah AWS.
Masukan data	20	Tidak	Ini adalah daftar tabel masukan yang ingin Anda gunakan dalam alur kerja yang cocok. Setiap input sesuai dengan kolom dalam tabel data AWS Glue input Anda, yang berisi nama kolom dan informasi tambahan yang Resolusi Entitas AWS digunakan untuk

Nama	Default	Dapat disesuaikan	Deskripsi
			tujuan pencocokan. Input harus berisi ID Unik ditambah setidaknya satu kolom input tambahan.
Keluaran data	750	Tidak	Ini adalah daftar `OutputAttribute` objek, yang masing-masing memiliki bidang Nama dan Hashed. Masing-masing objek ini mewakili kolom yang akan disertakan dalam tabel AWS Glue output dan apakah Anda ingin nilai dalam kolom yang akan di-hash.
Skema data	25	Tidak	Jumlah maksimum kolom masukan skema data.
Alur kerja pemetaan ID	10	Ya	Jumlah maksimum alur kerja pemetaan ID yang dapat Anda buat saat ini Akun AWS . Wilayah AWS
Ruang nama ID	10	Ya	Jumlah maksimum ruang nama ID yang dapat Anda buat Akun AWS dalam hal ini saat ini. Wilayah AWS
Pertandingan IDs	500	Tidak	Jumlah maksimum catatan yang dapat dikonsolidasikan di bawah satu matchID per beban kerja.
Aturan pertandingan	15	Tidak	Untuk pencocokan berbasis aturan, ini adalah nomor aturan yang diterapkan yang menghasilkan kumpulan rekaman yang cocok. Ini adalah bagian dari metadata alur kerja yang cocok yang akan disertakan dalam output.
Alur kerja yang cocok	10	Ya	Jumlah maksimum alur kerja yang cocok.

Nama	Default	Dapat disesuaikan	Deskripsi
Jumlah aturan per alur kerja	15	Tidak	Jumlah maksimum aturan per alur kerja yang cocok.
Tingkat `GetMatchId` API permintaan	50	Ya	Jumlah maksimum `GetCustomerID` API permintaan per detik.
Pemetaan skema	50	Ya	Jumlah maksimum pemetaan skema yang dapat Anda buat di akun ini di Wilayah saat ini. AWS
Kunci pencocokan unik per seluruh kumpulan aturan	15	Tidak	Jumlah maksimum kunci pencocokan unik per set aturan. Kunci pencocokan menginstruksikan bidang input Resolusi Entitas AWS mana yang harus dianggap sebagai data serupa dan mana yang harus dianggap sebagai data yang berbeda. Ini membantu Resolusi Entitas AWS secara otomatis mengonfigurasi aturan pencocokan berbasis aturan dan membandingkan data serupa yang disimpan di bidang input yang berbeda.

APIkuota pelambatan

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `CreateMatchingWorkflow`	5 TPS	Jumlah maksimum `CreateMatchingWorkflow` API panggilan per detik.
Permintaan tarif `DeleteMatchingWorkflow`	5 TPS	Jumlah maksimum `DeleteMatchingWork`

Sumber Daya	Batas tarif	Deskripsi
		`flow` API panggilan per detik.
Permintaan tarif `GetMatchingWorkflow`	5 TPS	Jumlah maksimum `GetMatchingWorkflow` API panggilan per detik.
Permintaan tarif `ListMatchingWorkflows`	5 TPS	Jumlah maksimum `ListMatchingWorkflows` API panggilan per detik.
Permintaan tarif `UpdateMatchingWorkflow`	5 TPS	Jumlah maksimum `UpdateMatchingWorkflow` API panggilan per detik.
Permintaan tarif `CreateSchemaMapping`	5 TPS	Jumlah maksimum `CreateSchemaMapping` API panggilan per detik.
Permintaan tarif `DeleteSchemaMapping`	5 TPS	Jumlah maksimum `DeleteSchemaMapping` API panggilan per detik.
Permintaan tarif `GetSchemaMapping`	5 TPS	Jumlah maksimum `GetSchemaMapping` API panggilan per detik.
Permintaan tarif `ListSchemaMappings`	5 TPS	Jumlah maksimum `ListSchemaMappings` API panggilan per detik.
Permintaan tarif `UpdateSchemaMapping`	5 TPS	Jumlah maksimum `UpdateSchemaMapping` API panggilan per detik.

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `GetPartnerComponent`	5 TPS	Jumlah maksimum `GetPartnerComponent` API panggilan per detik.
Permintaan tarif `ListPartnerComponents`	5 TPS	Jumlah maksimum `ListPartnerComponents` API panggilan per detik.
Permintaan tarif `TagResource`	5 TPS	Jumlah maksimum `TagResource` API panggilan per detik.
Permintaan tarif `UntagResource`	5 TPS	Jumlah maksimum `UntagResource` API panggilan per detik.
Permintaan tarif `ListTagsForResource`	5 TPS	Jumlah maksimum `ListTagsForResource` API panggilan per detik.
Permintaan tarif `CreateIdMappingWorkflow`	5 TPS	Jumlah maksimum `CreateIdMappingWorkflow` API panggilan per detik.
Permintaan tarif `DeleteIdMappingWorkflow`	5 TPS	Jumlah maksimum `DeleteIdMappingWorkflow` API panggilan per detik.
Permintaan tarif `GetIdMappingWorkflow`	5 TPS	Jumlah maksimum `GetIdMappingWorkflow` API panggilan per detik.

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `ListIdMappingWorkflow`	5 TPS	Jumlah maksimum `ListIdMappingWorkflow` API panggilan per detik.
Permintaan tarif `UpdateIdMappingWorkflow`	5 TPS	Jumlah maksimum `UpdateIdMappingWorkflow` API panggilan per detik.
Permintaan tarif `ListProviderServices`	5 TPS	Jumlah maksimum `ListProviderServices` API panggilan per detik.
Permintaan tarif `GetProviderService`	5 TPS	Jumlah maksimum `GetProviderService` API panggilan per detik.
Permintaan tarif `CreateIdNamespace`	5 TPS	Jumlah maksimum `CreateIdNamespace` API panggilan per detik.
Permintaan tarif `DeleteIdNamespace`	5 TPS	Jumlah maksimum `DeleteIdNamespace` API panggilan per detik.
Permintaan tarif `GetIdNamespace`	5 TPS	Jumlah maksimum `GetIdNamespace` API panggilan per detik.
Permintaan tarif `ListIdNamespaces`	5 TPS	Jumlah maksimum `ListIdNamespaces` API panggilan per detik.
Permintaan tarif `UpdateIdNamespace`	5 TPS	Jumlah maksimum `UpdateIdNamespace` API panggilan per detik.

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `AddPolicyStatement`	5 TPS	Jumlah maksimum `AddPolicyStatement` API panggilan per detik.
Permintaan tarif `DeletePolicyStatement`	5 TPS	Jumlah maksimum `DeletePolicyStatement` API panggilan per detik.
Permintaan tarif `GetPolicy`	5 TPS	Jumlah maksimum `GetPolicy` API panggilan per detik.
Permintaan tarif `PutPolicy`	5 TPS	Jumlah maksimum `PutPolicy` API panggilan per detik.
Permintaan tarif `GetMatchingJob`	10 TPS	Jumlah maksimum `GetMatchingJob` API panggilan per detik.
Permintaan tarif `ListMatchingJobs`	5 TPS	Jumlah maksimum `ListMatchingJobs` API panggilan per detik.
Permintaan tarif `StartMatchingJob`	5 TPS	Jumlah maksimum `StartMatchingJob` API panggilan per detik.
Permintaan tarif `GetMatchId`	50 TPS	Jumlah maksimum `GetMatchId` API panggilan per detik.
Permintaan tarif `GetIdMappingJob`	10 TPS	Jumlah maksimum `GetIdMappingJob` API panggilan per detik.

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `ListIdMappingJobs`	5 TPS	Jumlah maksimum `ListIdMappingJobs` API panggilan per detik.
Permintaan tarif `StartIdMappingJob`	5 TPS	Jumlah maksimum `StartIdMappingJob` API panggilan per detik.
Permintaan tarif `BatchDeleteUniqueId`	5 TPS	Jumlah maksimum `BatchDeleteUniqueId` API panggilan per detik.

Riwayat dokumen untuk Panduan Resolusi Entitas AWS Pengguna

Tabel berikut menjelaskan rilis dokumentasi untuk Resolusi Entitas AWS.

Untuk pemberitahuan tentang pembaruan dokumentasi ini, Anda dapat berlangganan RSS umpan. Untuk berlangganan RSS pembaruan, Anda harus mengaktifkan RSS plug-in untuk browser yang Anda gunakan.

Perubahan	Deskripsi	Tanggal
Integrasi penyedia	Pembaruan khusus dokumentasi. Pelanggan dapat belajar bagaimana mengintegrasikan sebagai layanan penyedia dengan Resolusi Entitas AWS.	Agustus 8, 2024
Alur kerja pemetaan ID - pembaruan	Pelanggan sekarang dapat menggunakan aturan pencocokan untuk menerjemahkan data pihak pertama dalam alur kerja pemetaan ID.	Juli 23, 2024
Alur kerja yang cocok - perbarui	Pelanggan sekarang dapat menghapus catatan dari alur kerja pencocokan berbasis aturan atau berbasis ML untuk membantu mematuhi peraturan manajemen data.	April 8, 2024
Alur kerja pemetaan ID - pembaruan	Pelanggan sekarang dapat menggunakan alur kerja pemetaan ID di beberapa. Akun AWS	April 2, 2024

AWS CloudFormation Sumber Daya - Sumber daya baru dan diperbarui	AWSResolusi Entitas telah menambahkan sumber daya berikut: `AWS::EntityResolution::IdNamespace` `AWS::EntityResolution::PolicyStatement` dan memperbarui sumber daya berikut:`AWS::EntityResolution::IdMappingWorkflow` .	April 2, 2024
Temukan ID Pertandingan	Pelanggan sekarang dapat menemukan ID Pencocokan yang sesuai dan aturan terkait untuk alur kerja berbasis aturan yang diproses.	Maret 25, 2024
Alur kerja yang cocok - perbarui	Resolusi Entitas AWS sekarang mendukung RAMPID penugasan PII berbasis dalam alur kerja LiveRamp pencocokan berbasis layanan penyedia.	Februari 12, 2024
AWS PrivateLink	Resolusi Entitas AWS sekarang mendukung keamanan data tambahan dengan AWS PrivateLink yang membantu pelanggan mengakses layanan yang dihosting secara AWS pribadi.	20 Oktober 2023

AWS CloudFormation Sumber Daya - Sumber daya baru dan diperbarui	Resolusi Entitas AWS telah menambahkan sumber daya berikut: `AWS::EntityResolution:IdMappingWorkflow` dan memperbarui sumber daya berikut: `AWS::EntityResolution::MatchingWorkflow` dan`AWS::EntityResolution::Schemamapping` .	19 Oktober 2023
Perbarui ke kebijakan yang ada	Izin baru berikut telah ditambahkan ke kebijakan `AWSEntityResolutionConsoleFullAccess` terkelola: `ADXReadAccess` dan`ManageEventBridgeRules` .	16 Oktober 2023
Pemetaan skema - pembaruan	Pelanggan sekarang memiliki kemampuan untuk mengedit dan memperbarui skema data yang ada.	16 Oktober 2023
Alur kerja yang cocok - perbarui	Pelanggan sekarang dapat memilih layanan penyedia data pilihan untuk membantu mencocokkan dan menautkan data mereka.	16 Oktober 2023

Alur kerja pemetaan ID	Pelanggan dapat menggunakan alur kerja baru ini untuk menentukan detail pemetaan ID, memilih metode pemetaan ID yang Anda inginkan, dan menentukan bidang input dan output data.	16 Oktober 2023
AWS CloudFormation integrasi	Resolusi Entitas AWS sekarang terintegrasi dengan AWS CloudFormation.	24 Agustus 2023
AWS pembaruan kebijakan terkelola - Kebijakan baru	Resolusi Entitas AWS menambahkan dua kebijakan terkelola baru.	18 Agustus 2023
Rilis awal	Rilis awal Panduan Resolusi Entitas AWS Pengguna	26 Juli 2023

Resolusi Entitas AWS Glosarium

Nama Sumber Daya Amazon (ARN)

Pengidentifikasi unik untuk AWS sumber daya. ARNsdiperlukan saat Anda perlu menentukan sumber daya secara jelas di semua Resolusi Entitas AWS, seperti dalam Resolusi Entitas AWS kebijakan, tag Amazon Relational Database Service (AmazonRDS), dan panggilan. API

Pemrosesan otomatis

Opsi irama pemrosesan untuk pekerjaan alur kerja yang cocok yang memungkinkannya dijalankan secara otomatis saat input data Anda berubah.

Opsi ini hanya tersedia untuk pencocokan berbasis aturan.

Secara default, irama pemrosesan untuk pekerjaan alur kerja yang cocok diatur ke Manual, yang memungkinkannya dijalankan sesuai permintaan. Anda dapat mengatur Pemrosesan otomatis untuk menjalankan pekerjaan alur kerja yang cocok secara otomatis saat input data Anda berubah. Ini membuat output up-to-date alur kerja Anda yang cocok.

AWS KMS key ARN

Ini adalah Nama Sumber Daya AWS KMS Amazon Anda (ARN) untuk enkripsi saat istirahat. Jika tidak disediakan, sistem akan menggunakan KMS kunci Resolusi Entitas AWS terkelola.

Cleartext

Data yang tidak dilindungi secara kriptografi.

Tingkat kepercayaan diri (ConfidenceLevel)

Untuk pencocokan ML, ini adalah tingkat kepercayaan yang diterapkan Resolusi Entitas AWS ketika ML mengidentifikasi kumpulan rekaman yang cocok. Ini adalah bagian dari metadata alur kerja yang cocok yang akan disertakan dalam output.

Dekripsi

Proses mengubah data terenkripsi kembali ke bentuk aslinya. Dekripsi hanya dapat dilakukan jika Anda memiliki akses ke kunci rahasia.

Enkripsi

Proses pengkodean data ke dalam bentuk yang muncul acak menggunakan nilai rahasia yang disebut kunci. Tidak mungkin untuk menentukan plaintext asli tanpa akses ke kunci.

Nama grup

Nama Grup mereferensikan seluruh grup kolom input dan dapat membantu Anda mengelompokkan data yang diuraikan bersama untuk tujuan pencocokan.

Misalnya, jika ada tiga bidang input:**`first_name`**,, dan **`middle_namelast_name`**, Anda dapat mengelompokkannya bersama-sama dengan memasukkan nama Grup **`full_name`** untuk pencocokan dan output.

Hash

Hashing berarti menerapkan algoritma kriptografi yang menghasilkan string karakter yang tidak dapat diubah dan unik dengan ukuran tetap — disebut hash. Resolusi Entitas AWS menggunakan protokol hash Secure Hash Algorithm 256-bit (SHA256) dan akan menampilkan string karakter 32-byte. Di Resolusi Entitas AWS, Anda dapat memilih apakah akan hash nilai data dalam output Anda.

Protokol hash () HashingProtocol

Resolusi Entitas AWS menggunakan protokol hash Secure Hash Algorithm 256-bit (SHA256) dan akan menampilkan string karakter 32-byte. Ini adalah bagian dari metadata alur kerja yang cocok yang akan disertakan dalam output.

Metode pemetaan ID

Bagaimana Anda ingin pemetaan ID dilakukan.

Ada dua metode pemetaan ID:

- Berbasis aturan — Metode yang digunakan untuk menggunakan aturan pencocokan untuk menerjemahkan data pihak pertama dari sumber ke target dalam alur kerja pemetaan ID.
- Layanan penyedia — Metode yang digunakan untuk menggunakan layanan penyedia untuk menerjemahkan data yang disandikan pihak ketiga dari sumber ke target dalam alur kerja pemetaan ID.

  Resolusi Entitas AWS saat ini mendukung LiveRamp sebagai metode pemetaan ID berbasis layanan penyedia. Anda harus berlangganan AWS Data Exchange untuk LiveRamp menggunakan metode ini. Untuk informasi selengkapnya, lihat Langkah 1: Berlangganan layanan penyedia di AWS Data Exchange.

Alur kerja pemetaan ID

Pekerjaan pemrosesan data yang memetakan data dari sumber data input ke target data input berdasarkan metode pemetaan ID yang ditentukan. Ini menghasilkan tabel pemetaan ID. Alur kerja ini mengharuskan Anda untuk menentukan metode pemetaan ID dan data input yang ingin Anda terjemahkan dari sumber ke target.

Anda dapat mengatur alur kerja pemetaan ID untuk dijalankan sendiri Akun AWS atau di dua. Akun AWS

Ruang nama ID

Sumber daya Resolusi Entitas AWS yang berisi metadata yang menjelaskan kumpulan data di beberapa Akun AWS dan cara menggunakan kumpulan data ini dalam alur kerja pemetaan ID.

Ada dua jenis ruang nama ID: `SOURCE` dan. `TARGET` `SOURCE`Berisi konfigurasi untuk data sumber yang akan diproses dalam alur kerja pemetaan ID. `TARGET`Berisi konfigurasi data target yang akan diselesaikan oleh semua sumber. Untuk menentukan data masukan yang ingin Anda selesaikan di dua Akun AWS, buat sumber namespace ID dan target namespace ID untuk menerjemahkan data Anda dari satu set () ke set lain ()`SOURCE`. `TARGET`

Setelah Anda dan anggota lain membuat ruang nama ID dan menjalankan alur kerja pemetaan ID, Anda dapat bergabung dengan kolaborasi AWS Clean Rooms untuk menjalankan gabungan multi tabel pada tabel pemetaan ID, dan menganalisis data.

Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Clean Rooms.

Bidang masukan

Bidang input sesuai dengan nama kolom dari tabel data AWS Glue input Anda.

Sumber Masukan ARN (InputSourceARN)

Amazon Resource Name (ARN) yang dihasilkan untuk input AWS Glue tabel. Ini adalah bagian dari metadata alur kerja yang cocok yang akan disertakan dalam output.

Jenis masukan

Jenis data input. Anda memilihnya dari daftar nilai yang telah dikonfigurasi sebelumnya seperti nama, alamat, nomor telepon, atau alamat email. Jenis input memberi tahu jenis data Resolusi Entitas AWS apa yang Anda sajikan, memungkinkannya diklasifikasikan dan dinormalisasi dengan benar.

Pencocokan berbasis pembelajaran mesin

Pencocokan berbasis pembelajaran mesin (pencocokan ML) menemukan kecocokan di seluruh data Anda yang mungkin tidak lengkap atau mungkin tidak terlihat persis sama. Pencocokan ML adalah proses preset yang akan mencoba mencocokkan catatan di semua data yang Anda masukkan. Pencocokan ML mengembalikan ID kecocokan dan tingkat kepercayaan untuk setiap kumpulan data yang cocok.

Pemrosesan manual

Opsi irama pemrosesan untuk pekerjaan alur kerja yang cocok yang memungkinkannya dijalankan sesuai permintaan.

Opsi ini diatur secara default dan tersedia untuk pencocokan berbasis aturan dan pencocokan berbasis pembelajaran mesin.

Many-to-Many pencocokan

Many-to-many pencocokan membandingkan beberapa contoh data serupa. Nilai di bidang input yang telah ditetapkan kunci kecocokan yang sama akan dicocokkan satu sama lain, terlepas dari apakah mereka berada di bidang input yang sama atau bidang input yang berbeda.

Misalnya, Anda mungkin memiliki beberapa kolom input nomor telepon seperti `mobile_phone` dan `home_phone` yang memiliki tombol kecocokan yang sama “Telepon”. Gunakan many-to-many pencocokan untuk membandingkan data di bidang `mobile_phone` input dengan data di bidang `mobile_phone` input dan data di bidang `home_phone` input.

Aturan pencocokan mengevaluasi data di beberapa bidang input dengan kunci pencocokan yang sama dengan operasi (atau), dan one-to-many pencocokan membandingkan nilai di beberapa bidang input. Ini berarti bahwa jika ada kombinasi `mobile_phone` atau `home_phone` kecocokan antara dua catatan, tombol pencocokan “Telepon” akan mengembalikan kecocokan. Untuk tombol kecocokan “Telepon” untuk menemukan kecocokan, `Record One mobile_phone = Record Two mobile_phone` `Record One mobile_phone = Record Two home_phone` ATAU ATAU `Record One home_phone = Record Two home_phone` ATAU`Record One home_phone = Record Two mobile_phone`.

ID Pertandingan (MatchID)

Untuk pencocokan berbasis aturan dan pencocokan ML, ini adalah ID yang dihasilkan oleh Resolusi Entitas AWS dan diterapkan ke setiap kumpulan rekaman yang cocok. Ini adalah bagian dari metadata alur kerja yang cocok yang akan disertakan dalam output.

Kunci kecocokan (MatchKey)

Kunci pencocokan menginstruksikan bidang input Resolusi Entitas AWS mana yang harus dipertimbangkan sebagai data serupa dan mana yang harus dipertimbangkan sebagai data yang berbeda. Ini membantu Resolusi Entitas AWS secara otomatis mengonfigurasi aturan pencocokan berbasis aturan dan membandingkan data serupa yang disimpan di bidang input yang berbeda.

Jika ada beberapa jenis informasi nomor telepon seperti bidang `mobile_phone` input dan bidang `home_phone` input dalam data Anda yang ingin Anda bandingkan bersama-sama, Anda bisa memberi keduanya tombol kecocokan “Telepon”. Kemudian pencocokan berbasis aturan dapat dikonfigurasi untuk membandingkan data menggunakan pernyataan “atau” di semua bidang input dengan kunci kecocokan “Telepon” (lihat One-to-One Pencocokan dan Many-to-Many Pencocokan definisi di bagian Alur Kerja Pencocokan).

Jika Anda ingin pencocokan berbasis aturan untuk mempertimbangkan berbagai jenis informasi nomor telepon sepenuhnya secara terpisah, Anda dapat membuat kunci pencocokan yang lebih spesifik seperti “Mobile_Phone” dan “Home_Phone”. Kemudian, saat menyiapkan alur kerja yang

cocok, Anda dapat menentukan bagaimana setiap tombol pencocokan telepon akan digunakan dalam pencocokan berbasis aturan.

Jika no MatchKey ditentukan untuk bidang input tertentu, itu tidak dapat digunakan dalam pencocokan tetapi dapat dilakukan melalui proses alur kerja yang cocok dan dapat menjadi output jika diinginkan.

Cocokkan nama kunci

Nama yang ditetapkan ke Kunci Pencocokan.

Aturan pertandingan (MatchRule)

Untuk pencocokan berbasis aturan, ini adalah nomor aturan yang diterapkan yang menghasilkan kumpulan rekaman yang cocok. Ini adalah bagian dari metadata alur kerja yang cocok yang akan disertakan dalam output.

Pencocokan

Proses menggabungkan dan membandingkan data dari berbagai bidang input, tabel, atau database dan menentukan mana yang sama — atau “cocok” — berdasarkan memenuhi kriteria pencocokan tertentu (misalnya, baik melalui aturan atau model yang cocok).

Alur kerja yang cocok

Proses yang Anda atur untuk menentukan data input untuk dicocokkan bersama dan bagaimana pencocokan harus dilakukan.

Deskripsi alur kerja yang cocok

Deskripsi opsional dari alur kerja yang cocok yang mungkin Anda pilih untuk dimasukkan. Deskripsi membantu Anda membedakan antara alur kerja yang cocok jika Anda membuat lebih dari satu.

Nama alur kerja yang cocok

Nama untuk alur kerja yang cocok yang Anda tentukan.

> **Note**
>
> Nama alur kerja yang cocok harus unik. Mereka tidak dapat memiliki nama yang sama atau kesalahan akan dikembalikan.

Metadata alur kerja yang cocok

Informasi yang dihasilkan dan dihasilkan oleh Resolusi Entitas AWS selama pekerjaan alur kerja yang cocok. Informasi ini diperlukan pada output.

Normalisasi () ApplyNormalization

Pilih apakah akan menormalkan data input seperti yang didefinisikan dalam skema. Normalisasi menstandarisasi data dengan menghapus spasi ekstra dan karakter khusus dan menstandarisasi ke format huruf kecil.

Misalnya, jika bidang input memiliki tipe input`PHONE_NUMBER`, dan nilai-nilai dalam tabel input diformat sebagai`(123) 456-7890`, Resolusi Entitas AWS akan menormalkan nilai ke`1234567890`.

Bagian berikut menjelaskan aturan normalisasi standar kami. Untuk pencocokan berbasis ML secara khusus, lihat. Normalisasi (ApplyNormalization) — hanya berbasis ML

Topik

- Nama
- Email
- Telepon
- Alamat
- Hashed
- Source_ID

Nama

- TRIM= Memangkas spasi putih di depan dan di belakang
- LOWERCASE= Huruf kecil semua karakter alfa

- CONVERT_ ACCENT = Surat beraksen terselubung ke surat biasa
- REMOVE_ _ ALL NON _ ALPHA = Menghapus semua karakter non-alfa [A-za-z]

Email

- TRIM= Memangkas spasi putih di depan dan di belakang
- LOWERCASE= Huruf kecil semua karakter alfa
- CONVERT_ ACCENT = Surat beraksen terselubung ke surat biasa
- EMAIL_ ADDRESS _ UTIL _ NORM = Menghapus setiap titik (.) dari nama pengguna, menghapus apa pun setelah tanda plus (+) di nama pengguna, dan menstandarisasi variasi domain umum
- REMOVE_ _ ALL _ NON EMAIL _ CHARS = Menghapus semua non-alpha-numeric karakter [A-za-z0-9] dan [.@-]

Telepon

- TRIM= Memangkas spasi putih di depan dan di belakang
- REMOVE_ _ ALL NON _ NUMERIC = Menghapus semua karakter non-numerik [0-9]
- REMOVE_ _ ALL LEADING _ ZEROES = Menghapus semua angka nol di depan
- ENSURE_ PREFIX _ WITH _MAP, "phonePrefixMap" = Memeriksa setiap nomor telepon dan mencoba mencocokkannya dengan pola di phonePrefixMap. Jika kecocokan ditemukan, aturan akan menambah atau mengubah awalan nomor telepon untuk memastikannya sesuai dengan format standar yang ditentukan dalam peta.

Alamat

- TRIM= Memangkas spasi putih di depan dan di belakang
- LOWERCASE= Huruf kecil semua karakter alfa
- CONVERT_ ACCENT = Surat beraksen terselubung ke surat biasa
- REMOVE_ _ ALL NON _ ALPHA = Menghapus semua karakter non-alfa [A-za-z]
- RENAME_ WORDS menggunakan ADDRESS _ RENAME _ WORD _ MAP = ganti kata-kata dalam string Alamat dengan kata-kata dari ADDRESS_ RENAME _ WORD _ MAP
- RENAME_ DELIMITERS menggunakan ADDRESS _ RENAME _ DELIMITER _ MAP = ganti pembatas di string Alamat dengan string dari ADDRESS_ _ _ RENAME DELIMITER MAP

- RENAME_ DIRECTIONS menggunakan ADDRESS _ RENAME _ DIRECTION _ MAP = ganti pembatas di string Alamat dengan string dari ADDRESS_ _ _ RENAME DIRECTION MAP
- RENAME_ NUMBERS menggunakan ADDRESS _ RENAME _ NUMBER _ MAP = ganti angka dalam string Alamat dengan string dari ADDRESS_ RENAME _ NUMBER _ MAP
- RENAME_ SPECIAL _ CHARS menggunakan ADDRESS _ RENAME _ SPECIAL _ CHAR _ MAP = ganti karakter khusus di String alamat dengan string dari ADDRESS_ RENAME _ SPECIAL _ CHAR _ MAP

ADDRESS_RENAME_WORD_MAP

Ini adalah kata-kata yang akan diganti namanya saat menormalkan string alamat.

```
"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

Ini adalah pembatas yang akan diganti namanya saat menormalkan string alamat.

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

ADDRESS_RENAME_DIRECTION_MAP

Ini adalah pengidentifikasi arah yang akan diganti namanya saat menormalkan string alamat.

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

ADDRESS_RENAME_NUMBER_MAP

Ini adalah string angka yang akan diganti namanya saat menormalkan string alamat.

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

ADDRESS_RENAME_SPECIAL_CHAR_MAP

Ini adalah string karakter khusus yang akan diganti namanya saat menormalkan string alamat.

```
"ß": "ss",
```

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

Hashed

- TRIM= Memangkas spasi putih di depan dan di belakang

Source_ID

- TRIM= Memangkas spasi putih di depan dan di belakang

Normalisasi (ApplyNormalization) — hanya berbasis ML

Pilih apakah akan menormalkan data input seperti yang didefinisikan dalam skema. Normalisasi menstandarisasi data dengan menghapus spasi ekstra dan karakter khusus dan menstandarisasi ke format huruf kecil.

Misalnya, jika bidang input memiliki tipe input`NAME`, dan nilai-nilai dalam tabel input diformat sebagai`Johns Smith`, Resolusi Entitas AWS akan menormalkan nilai ke`john smith`.

Bagian berikut menjelaskan aturan normalisasi untuk alur kerja pencocokan berbasis pembelajaran mesin.

Topik

- Nama
- Email
- Telepon

Nama

- TRIM= Memangkas spasi putih di depan dan di belakang
- LOWERCASE= Huruf kecil semua karakter alfa

Email

- LOWERCASE= Huruf kecil semua karakter alfa
- Mengganti hanya (at) (peka huruf besar/kecil) dengan simbol @
- Menghapus semua spasi putih, di mana saja dalam nilai
- Menghapus semua yang ada di luar yang pertama "< >" jika ada

Telepon

- TRIM= Memangkas spasi putih di depan dan di belakang
- REMOVE_ _ ALL NON _ NUMERIC = Menghapus semua karakter non-numerik [0-9]
- REMOVE_ _ ALL LEADING _ ZEROES = Menghapus semua angka nol di depan
- ENSURE_ PREFIX _ WITH _MAP, "phonePrefixMap" = Memeriksa setiap nomor telepon dan mencoba mencocokkannya dengan pola di phonePrefixMap. Jika kecocokan ditemukan, aturan akan menambah atau mengubah awalan nomor telepon untuk memastikannya sesuai dengan format standar yang ditentukan dalam peta.

One-to-One pencocokan

One-to-one pencocokan membandingkan contoh tunggal dari data serupa. Bidang masukan dengan kunci kecocokan dan nilai yang sama di bidang input yang sama akan dicocokkan satu sama lain.

Misalnya, Anda mungkin memiliki beberapa kolom input nomor telepon seperti `mobile_phone` dan `home_phone` yang memiliki tombol kecocokan yang sama “Telepon”. Gunakan one-to-one pencocokan untuk membandingkan data di bidang `mobile_phone` input dengan data di bidang `mobile_phone` input dan untuk membandingkan data di bidang `home_phone` input dengan data di bidang `home_phone` input. Data di bidang `mobile_phone` input tidak akan dibandingkan dengan data di bidang `home_phone` input.

Aturan pencocokan mengevaluasi data dalam beberapa bidang input dengan kunci pencocokan yang sama dengan operasi (atau), dan one-to-many pencocokan membandingkan nilai dalam satu bidang input. Ini berarti bahwa jika `mobile_phone` atau `home_phone` cocok antara dua catatan, tombol kecocokan “Telepon” akan mengembalikan kecocokan. Untuk tombol kecocokan “Telepon” untuk menemukan kecocokan, `Record One mobile_phone = Record Two mobile_phone ORRecord One home_phone = Record Two home_phone`.

Aturan pencocokan mengevaluasi data di bidang input dengan kunci pencocokan yang berbeda dengan operasi (dan). Jika Anda ingin pencocokan berbasis aturan mempertimbangkan berbagai jenis informasi nomor telepon secara terpisah, Anda dapat membuat kunci pencocokan yang lebih spesifik seperti “mobile_phone” dan “home_phone”. Jika Anda ingin menggunakan kedua tombol pencocokan dalam aturan untuk menemukan kecocokan, `Record One mobile_phone = Record Two mobile_phone` AND`Record One home_phone = Record Two home_phone`.

Output

Daftar OutputAttributeobjek, yang masing-masing memiliki bidang Nama dan Hashed. Masing-masing objek ini mewakili kolom yang akan disertakan dalam tabel AWS Glue output dan apakah Anda ingin nilai dalam kolom yang akan di-hash.

Keluaran3Path

Tujuan S3 yang Resolusi Entitas AWS akan menulis tabel output.

OutputSourceConfig

Daftar OutputSource objek, yang masing-masing memiliki bidang outputs3Path,, ApplyNormalizationdan Output.

Pencocokan berbasis layanan penyedia

Pencocokan berbasis layanan penyedia adalah proses yang dirancang untuk mencocokkan, menautkan, dan menyempurnakan catatan Anda dengan penyedia layanan data pilihan dan kumpulan data berlisensi. Anda harus berlangganan melalui AWS Data Exchange layanan penyedia untuk menggunakan teknik pencocokan ini.

Resolusi Entitas AWS saat ini terintegrasi dengan penyedia layanan data berikut:

- LiveRamp
- TransUnion
- UID 2.0

Pencocokan berbasis aturan

Pencocokan berbasis aturan adalah proses yang dirancang untuk menemukan kecocokan yang tepat. Pencocokan berbasis aturan adalah seperangkat hierarkis aturan pencocokan air terjun, disarankan oleh Resolusi Entitas AWS, berdasarkan data yang Anda masukkan dan dapat dikonfigurasi sepenuhnya oleh Anda. Semua kunci pencocokan yang disediakan dalam kriteria aturan harus sama persis agar data yang dibandingkan dinyatakan cocok dan metadata terkait menjadi keluaran. Pencocokan berbasis aturan mengembalikan ID Pencocokan dan nomor aturan untuk setiap kumpulan data yang cocok.

Kami merekomendasikan mendefinisikan aturan yang dapat mengidentifikasi entitas secara unik. Pesan aturan Anda untuk menemukan kecocokan yang lebih tepat terlebih dahulu.

Misalnya, katakanlah Anda memiliki dua aturan, Aturan 1 dan Aturan 2.

Aturan-aturan ini memiliki kunci kecocokan berikut:

- Aturan 1 termasuk Nama Lengkap dan Alamat
- Aturan 2 mencakup Nama Lengkap, Alamat, dan Telepon

Karena Aturan 1 berjalan lebih dulu, tidak ada kecocokan yang akan ditemukan oleh Aturan 2 karena semuanya akan ditemukan oleh Aturan 1.

Untuk menemukan kecocokan yang dibedakan berdasarkan Telepon, atur ulang aturannya, seperti ini:

- Aturan 2 mencakup Nama Lengkap, Alamat, dan Telepon
- Aturan 1 termasuk Nama Lengkap dan Alamat

Skema

Istilah yang digunakan untuk struktur atau tata letak yang mendefinisikan bagaimana satu set data diatur dan terhubung.

Deskripsi skema

Deskripsi opsional skema yang dapat Anda pilih untuk dimasukkan. Deskripsi membantu Anda membedakan antara pemetaan skema jika Anda membuat lebih dari satu.

Nama skema

Nama skema.

> **Note**
>
> Nama skema harus unik. Mereka tidak dapat memiliki nama yang sama atau kesalahan akan dikembalikan.

Pemetaan skema

Pemetaan skema Resolusi Entitas AWS adalah proses di mana Anda memberi tahu Resolusi Entitas AWS cara menafsirkan data Anda untuk pencocokan. Anda menentukan skema tabel data input yang ingin Anda baca Resolusi Entitas AWS ke dalam alur kerja yang cocok.

Pemetaan skema ARN

Amazon Resource Name (ARN) yang dihasilkan untuk pemetaan skema.

ID Unik

Pengidentifikasi unik yang Anda tentukan dan yang harus ditetapkan untuk setiap baris data masukan yang Resolusi Entitas AWS dibaca.

Example

Misalnya: **`Primary_key`**, **`Row_ID`**, atau **`Record_ID`**.

Kolom ID Unik diperlukan.

ID Unik harus berupa pengenal unik dalam satu tabel.

Di tabel yang berbeda, ID Unik dapat memiliki nilai duplikat.

Saat alur kerja yang cocok dijalankan, catatan akan ditolak jika ID Unik:

- tidak ditentukan
- tidak unik dalam tabel yang sama

- tumpang tindih dalam hal nama atribut di seluruh sumber.
- melebihi 38 karakter (hanya alur kerja pencocokan berbasis aturan)

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.