Guía del usuario

AWS Entity Resolution

AWS Entity Resolution: Guía del usuario

Table of Contents

¿Qué es AWS Entity Resolution?

AWS Entity Resolution es un servicio que le ayuda a comparar, vincular y mejorar los registros relacionados almacenados en múltiples aplicaciones, canales y almacenes de datos. Puede empezar a utilizar flujos de trabajo de resolución de entidades que sean flexibles, escalables y que puedan conectarse a sus aplicaciones y proveedores de servicios de datos existentes.

AWS Entity Resolution ofrece técnicas de comparación avanzadas, como la coincidencia basada en reglas, la coincidencia basada en el aprendizaje automático (coincidencia ML) y la coincidencia dirigida por el proveedor de servicios de datos. Estas técnicas pueden ayudarle a vincular y mejorar con mayor precisión los registros relacionados de información de clientes, códigos de productos o códigos de datos empresariales.

Puede utilizarlas AWS Entity Resolution para crear una vista unificada de las interacciones con los clientes, vinculando los eventos recientes (como los clics en anuncios, el abandono del carrito y las compras) con las señales seudonimizadas de sus proveedores de servicios de datos en un identificador de entidad único. También puedes realizar un mejor seguimiento de los productos que utilizan códigos diferentes (por ejemplo, SKU o UPC) en todas tus tiendas. Puedes usarlo AWS Entity Resolution para controlar la precisión de las coincidencias y proteger mejor la seguridad de los datos y, al mismo tiempo, minimizar el movimiento de datos.

Temas

¿Es la primera vez que lo utiliza AWS Entity Resolution ?

Si es la primera vez que lo utiliza AWS Entity Resolution, le recomendamos que comience leyendo las siguientes secciones:

- Configurar AWS Entity Resolution

Características de AWS Entity Resolution

AWS Entity Resolution incluye las siguientes funciones:

- Preparación de datos flexible y personalizable

  AWS Entity Resolution lee sus datos AWS Glue para usarlos como entradas para el procesamiento de coincidencias. Puedes especificar un máximo de 20 entradas de datos. AWS Entity Resolution procesa cada fila de la tabla de entrada de datos como un registro, con una entidad única que actúa como clave principal. AWS Entity Resolution puede funcionar en conjuntos de datos cifrados. En primer lugar, defina el esquema de mapeo AWS Entity Resolution para comprender qué campos de entrada quiere usar en su flujo de trabajo coincidente. Puede crear su propio esquema de datos, o plano, a partir de una entrada de AWS Glue datos existente. O bien, puede crear su esquema personalizado mediante una interfaz de usuario interactiva o un editor JSON. De forma predeterminada, AWS Entity Resolution también normaliza las entradas de datos antes de la coincidencia para mejorar el procesamiento de las coincidencias, por ejemplo, eliminando los caracteres especiales y los espacios adicionales y formateando el texto en minúsculas. Si la entrada de datos ya está normalizada, puede desactivar la normalización. También ofrecemos una GitHub biblioteca que puede utilizar para personalizar aún más el proceso de normalización de datos para adaptarlo a sus necesidades.
- Flujos de trabajo configurables que coinciden con

  Un flujo de trabajo de coincidencia de entidades es una secuencia de pasos que se configura para indicar AWS Entity Resolution cómo hacer coincidir la entrada de datos y dónde escribir la salida de datos consolidada. Puede configurar uno o más flujos de trabajo coincidentes para comparar diferentes entradas de datos y utilizar diferentes técnicas de coincidencia, como la coincidencia basada en reglas, la coincidencia mediante aprendizaje automático o la comparación dirigida por un proveedor de servicios de datos sin experiencia en resolución de entidades o aprendizaje automático. También puede ver el estado de las tareas de los flujos de trabajo y las métricas coincidentes existentes, como el número de recursos, el número de registros procesados y el número de coincidencias encontradas.

  - Ready-to-use coincidencia basada en reglas

    Esta técnica de emparejamiento incluye un conjunto de ready-to-use reglas en AWS Management Console o AWS Command Line Interface ()AWS CLI. Puede usar estas reglas

para buscar registros relacionados en función de sus campos de entrada. También puede personalizar las reglas agregando o quitando campos de entrada para cada regla, eliminando reglas, reorganizando la prioridad de las reglas y creando reglas nuevas. También puede restablecer las reglas para devolverlas a sus configuraciones originales. La salida de datos del bucket de Amazon Simple Storage Service (Amazon S3) contiene grupos de coincidencias AWS Entity Resolution que se generan mediante la técnica de coincidencia basada en reglas. Cada grupo de coincidencias tiene asociado el número de regla utilizado para generar esa coincidencia, lo que le ayudará a entenderla. Por ejemplo, el número de la regla puede demostrar la precisión de cada grupo de coincidencias, de modo que la primera regla sea más precisa que la segunda.

- Emparejamiento preconfigurado basado en el aprendizaje automático (coincidencia de aprendizaje automático)

  Esta técnica de comparación incluye un modelo de aprendizaje automático preconfigurado para buscar coincidencias en todas las entradas de datos, especialmente en los registros basados en los consumidores. El modelo utiliza todos los campos de entrada asociados con el nombre, la dirección de correo electrónico, el número de teléfono, la dirección y los tipos de datos de fecha de nacimiento. El modelo genera grupos de coincidencias de registros relacionados con una puntuación de confianza en cada grupo que explica la calidad de la coincidencia en relación con otros grupos de coincidencias. El modelo considera los campos de entrada que faltan y analiza todo el registro en conjunto para representar una entidad. La salida de datos de su bucket de Amazon S3 tiene grupos de coincidencias que se AWS Entity Resolution generan mediante la coincidencia de aprendizaje automático. Aquí es donde cada grupo de coincidencias tiene una puntuación de confianza asociada de 0,0—1,0, que indica la precisión de la coincidencia.

- Hacer coincidir los registros con los proveedores de servicios de datos

  Con AWS Entity Resolution él, puede comparar, vincular y mejorar sus registros con los principales proveedores de servicios de datos y conjuntos de datos con licencia para ampliar su capacidad de comprender, llegar y atender a sus clientes. Por ejemplo, puede añadir atributos a sus datos para mejorar sus registros, o puede mejorar la interoperabilidad de los sistemas y plataformas con los que trabaja para cumplir sus objetivos empresariales. Puede utilizar este flujo de trabajo coincidente con unos pocos clics, lo que elimina la necesidad de crear y mantener integraciones patentadas complejas. Debe tener un acuerdo de licencia con estos proveedores de servicios de datos para aprovechar esta técnica de combinación.

- Procesamiento manual masivo y procesamiento incremental automático

Puede utilizar el procesamiento de datos para convertir las entradas de datos en una tabla de salida de datos consolidada con registros similares que tengan un identificador de coincidencia común generado mediante configuraciones de flujo de trabajo coincidentes entre entidades. Con la API AWS Management Console y/o la AWS CLI, puede ejecutar el procesamiento masivo manual a pedido, en función de su canalización de datos de extracción, transformación y carga (ETL) existente, que vuelve a procesar todos los datos para detectar nuevas coincidencias y actualizar las coincidencias existentes. Además, para los escenarios de coincidencia basados en reglas, puede iniciar el procesamiento incremental automático para que, tan pronto como haya nuevos datos disponibles en su bucket de Amazon S3, el servicio lea esos nuevos registros y los compare con los registros existentes. Esto mantiene sus coincidencias actualizadas con cualquier cambio en los datos de Amazon S3.

- Búsqueda casi en tiempo real

  La búsqueda de cualquier campo de entidad a través de la operación de la AWS Entity Resolution GetMatchId API te ayuda a recuperar de forma sincrónica un identificador de coincidencia existente. Puedes llamar AWS Entity Resolution con los atributos de información de identificación personal (PII) adquiridos a través de diferentes fuentes y canales. AWS Entity Resolution codifica esos atributos para proteger los datos y recupera el identificador de coincidencia correspondiente para vincular y relacionar al cliente. Por ejemplo, puedes registrarte en la web con un nombre, un correo electrónico y una dirección postal asociados. Utilice la operación de AWS Entity Resolution GetMatchId API para averiguar si este cliente o entidad ya existe en los resultados coincidentes almacenados en su bucket de S3, junto con el ID de coincidencia de la entidad correspondiente asociado a él. Tras obtener el identificador de coincidencia de la entidad, podrá encontrar la información transaccional asociada a él en las aplicaciones de origen, como los sistemas de gestión de relaciones con los clientes (CRM) o de plataforma de datos de clientes (CDP).

- Protección de datos y regionalización desde el diseño

  AWS Entity Resolution ofrece una capacidad de cifrado predeterminada que puede ayudarlo a proteger sus datos y le proporciona una clave de cifrado para cada entrada de datos en el servicio. Por ejemplo, AWS Entity Resolution le ofrece la flexibilidad de utilizar datos cifrados y cifrados del servidor para ejecutar flujos de trabajo coincidentes basados en reglas. AWS Entity Resolution admite la regionalización, lo que significa que los flujos de trabajo coincidentes se ejecutan para procesar los datos en el mismo lugar Región de AWS desde el que se utiliza el servicio. También puede cifrar y aplicar un hash a los datos de salida en Amazon S3 antes de utilizar los datos resueltos en otras aplicaciones.

- Transcodificación multipartita

AWS Entity Resolution le ayuda a definir las fuentes de datos y a hacer coincidir las configuraciones entre varias partes que desean utilizar una colaboración de datos, como en. AWS Clean Rooms

Servicios relacionados

Los siguientes Servicios de AWS aspectos están relacionados con AWS Entity Resolution:

- Amazon S3

  Almacene los datos que introduzca AWS Entity Resolution en Amazon S3.

  Para obtener más información, consulte ¿Qué es Amazon S3? en la Guía del usuario de Amazon Simple Storage Service.

- AWS Glue

  Cree AWS Glue tablas a partir de sus datos en Amazon S3 para utilizarlas en AWS Entity Resolution.

  Para obtener más información, consulte ¿Qué es AWS Glue? en la Guía para AWS Glue desarrolladores.

- AWS CloudTrail

  Úselo AWS Entity Resolution con CloudTrail los registros para mejorar el análisis de la Servicio de AWS actividad.

  Para obtener más información, consulte Registrar llamadas a la AWS Entity Resolution API mediante AWS CloudTrail.

- AWS CloudFormation

  Cree los siguientes recursos en AWS CloudFormation: AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace y AWS::EntityResolution::PolicyStatement

  Para obtener más información, consulte Cree recursos de resolución de entidades de AWS con AWS CloudFormation.

Accediendo AWS Entity Resolution

Puede acceder a AWS Entity Resolution través de las siguientes opciones:

- Directamente a través de la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
- Programáticamente a través de la AWS Entity Resolution API. Para obtener más información, consulte la Referencia de la API de AWS Entity Resolution .
  - Si planea llamar a la AWS Entity Resolution API en AWS Lambda tiempo de ejecución, cree su propio paquete de implementación e incluya la versión deseada de la biblioteca del AWS SDK. Para obtener más información, consulta los siguientes ejemplos en la Guía para AWS Lambda desarrolladores:
    - Implemente funciones de Java Lambda con archivos.zip o JAR
    - Trabajar con archivos de archivos.zip para funciones Lambda de Python

Precios para AWS Entity Resolution

Para obtener información acerca de los precios, consulte AWS Entity Resolution Pricing (Precios de Glue).

Configurar AWS Entity Resolution

Antes de usarlo AWS Entity Resolution por primera vez, regístrese AWS y cree un usuario administrador para crear roles.

Registrarse en AWS

Si ya tienes una Cuenta de AWS, omite este paso.

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Crear un usuario administrador

Para crear un usuario administrador, elija una de las siguientes opciones.

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
En IAM Identity Center (recomendado)	Usar credenciales a corto plazo para acceder a AWS. Esto se ajusta a las prácticas recomendadas de seguridad. Para obtener información sobre las prácticas recomendadas, consulta Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.	Siga las instrucciones en Introducción en la Guía del usuario de AWS IAM Identity Center .	Configure el acceso programático configurando el AWS CLI que se utilizará AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario.
En IAM (no recomendado)	Usar credenciales a largo plazo para acceder a AWS.	Siguiendo las instrucciones de Crear un usuario de IAM para acceso de emergencia de la Guía del usuario de IAM.	Configure el acceso programático mediante Administrar las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM.

Crear un rol de IAM para un usuario de consola

Complete el siguiente procedimiento si utiliza la AWS Entity Resolution consola.

Cómo crear un rol de IAM

1. Inicie sesión en la consola de IAM (https://console.aws.amazon.com/iam/) con su cuenta de administrador.
2. En Administración de accesos, elija Roles.

   Puede usar Roles para crear credenciales a corto plazo, lo que se recomienda para aumentar la seguridad. También puede elegir Usuarios para crear credenciales a largo plazo.
3. Elija Crear rol.
4. En el asistente de creación de roles, en Tipo de entidad de confianza, elija Cuenta de AWS.
5. Mantenga seleccionada la opción Esta cuenta y, a continuación, elija Siguiente.
6. En Añadir permisos, selecciona Crear política.

   Se abrirá una nueva pestaña.

   a. Seleccione la pestaña JSON y, a continuación, añada políticas en función de las capacidades otorgadas al usuario de la consola. AWS Entity Resolution ofrece las siguientes políticas administradas basadas en casos de uso comunes:

      - AWS política gestionada: AWSEntity ResolutionConsoleFullAccess
      - AWS política gestionada: AWSEntity ResolutionConsoleReadOnlyAccess

   b. Elija Siguiente: Etiquetas, añada etiquetas (opcional) y, a continuación, elija Siguiente: Revisar.

   c. En Revisar política, introduzca un Nombre y una Descripción y revise el Resumen.

   d. Elija Crear política.

      Ha creado una política para un miembro de la colaboración.

   e. Regrese a la pestaña original y, en Agregar permisos, escriba el nombre de la política que acaba de crear. (es posible que tenga que volver a cargar la página).

   f. Seleccione la casilla de verificación situada junto al nombre de la política que creó y, a continuación, seleccione Siguiente.
7. En Nombre, revisar y crear, introduzca el Nombre del rol y la Descripción.

   a. Revise Seleccionar entidades de confianza e introduzca la Cuenta de AWS correspondiente a la persona o personas que asumirán el rol (si es necesario).

   b. Revise los permisos en Agregar permisos y edítelos si es necesario.

c. Revise las Etiquetas y añada etiquetas si es necesario.

d. Seleccione Crear rol.

Crear un rol de trabajo de flujo de trabajo para AWS Entity Resolution

AWS Entity Resolution usa un rol de trabajo de flujo de trabajo para ejecutar un flujo de trabajo. Puede crear este rol mediante la consola si dispone de los permisos de IAM necesarios. Si no tiene `CreateRole` permisos, pida al administrador que cree el rol.

Para crear un rol de trabajo de flujo de trabajo para AWS Entity Resolution

1. Inicie sesión en la consola de IAM https://console.aws.amazon.com/iam/con su cuenta de administrador.
2. En Administración de accesos, elija Roles.

   Puede usar Roles para crear credenciales a corto plazo, lo que se recomienda para aumentar la seguridad. También puede elegir Usuarios para crear credenciales a largo plazo.
3. Elija Crear rol.
4. En el asistente Crear rol, en Tipo de entidad de confianza, elija Política de confianza personalizada.
5. Copie y pegue la siguiente política de confianza personalizada en el editor JSON.

   JSON

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

```
    ]
}
```

6. Elija Siguiente.
7. En Añadir permisos, selecciona Crear política.

   Se abre una nueva pestaña.

   a. Copia y pega la siguiente política en el editor JSON.

> **Note**
>
> El siguiente ejemplo de política admite los permisos necesarios para leer los recursos de datos correspondientes, como Amazon S3 y AWS Glue. Sin embargo, es posible que tengas que modificar esta política en función de cómo hayas configurado las fuentes de datos.
> Sus AWS Glue recursos y los recursos subyacentes de Amazon S3 deben estar en el mismo lugar Región de AWS que AWS Entity Resolution.
> No necesita conceder AWS KMS permisos si sus fuentes de datos no están cifradas o descifradas.

JSON

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

```
                    "s3:ResourceAccount":[
                        "{{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"
            ]
        }
```

```
    ]
}
```

Reemplace cada *{{user input placeholder}}* por su propia información.

aws-region	Región de AWS de sus recursos. Sus AWS Glue recursos, los recursos subyacentes de Amazon S3 y AWS KMS los recursos deben estar en el Región de AWS mismo lugar queAWS Entity Resolution .
accountId	Su Cuenta de AWS ID.
input-buckets	Buckets de Amazon S3 que contienen los objetos de datos subyacentes desde los AWS Glue que AWS Entity Resolution se leerá.
output-buckets	Los buckets de Amazon S3 son los AWS Entity Resolution que generarán los datos de salida.
input-databases	AWS Glue bases de datos desde las AWS Entity Resolution que leeré.

b. (Opcional) Si el bucket de Amazon S3 de entrada está cifrado con la clave KMS del cliente, añada lo siguiente:

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

Reemplace cada *{{user input placeholder}}* por su propia información.

aws-region	Región de AWS de sus recursos. Sus AWS Glue recursos, los recursos subyacentes de Amazon S3 y AWS KMS los recursos deben estar en el Región de AWS mismo lugar que`AWS Entity Resolution` .
accountId	Su Cuenta de AWS ID.
inputKeys	Ingresa las claves administradas AWS Key Management Service. Si sus fuentes de entrada están cifradas, `AWS Entity Resolution` debe descifrar los datos con su clave.

c. (Opcional) Si es necesario cifrar los datos que se van a escribir en el bucket de Amazon S3 de salida, añada lo siguiente:

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

Reemplace cada *{{user input placeholder}}* por su propia información.

aws-region	Región de AWS de sus recursos. Sus AWS Glue recursos, los recursos subyacentes de Amazon S3 y AWS KMS los recursos deben estar en el Región de AWS mismo lugar que`AWS Entity Resolution` .
accountId	Su Cuenta de AWS ID.
outputKeys	Ingresa las claves administradas AWS Key Management Service. Si necesita cifrar las fuentes de salida, `AWS Entity Resolution` debe cifrar los datos de salida con su clave.

d. (Opcional) Si tiene una suscripción a través AWS Data Exchange de un servicio de proveedor y desea utilizar un rol existente para un flujo de trabajo basado en el servicio de un proveedor, añada lo siguiente:

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

Reemplace cada *{{user input placeholder}}* por su propia información.

aws-region	El Región de AWS lugar donde se otorga el recurso del proveedor. Puede encontrar este valor en el ARN del activo de la AWS Data Exchange consola. Por ejemplo: `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
datasetId	El ID del conjunto de datos, que se encuentra en la AWS Data Exchange consola.
revisionId	La revisión del conjunto de datos, que se encuentra en la AWS Data Exchange consola.
assetId	El ID del activo, que se encuentra en la AWS Data Exchange consola.

8. Vuelva a la pestaña original y, en Añadir permisos, introduzca el nombre de la política que acaba de crear. (es posible que tenga que volver a cargar la página).
9. Seleccione la casilla de verificación situada junto al nombre de la política que creó y, a continuación, seleccione Siguiente.
10. En Nombre, revisar y crear, introduzca el Nombre del rol y la Descripción.

> **Note**
>
> El nombre de la función debe coincidir con el patrón de los `passRole` permisos concedidos al miembro que puede transferirla `workflow job role` para crear un flujo de trabajo coincidente.
> Por ejemplo, si utilizas la política `AWSEntityResolutionConsoleFullAccess` gestionada, recuerda incluirla `entityresolution` en el nombre de tu rol.

a. Revise la sección Seleccionar entidades de confianza y edítela si es necesario.
b. Revise los permisos en Agregar permisos y edítelos si es necesario.
c. Revise las Etiquetas y añada etiquetas si es necesario.
d. Seleccione Crear rol.

Se AWS Entity Resolution ha creado el rol de trabajo del flujo de trabajo para.

Preparar tablas de datos de entrada

En AWS Entity Resolution, cada una de las tablas de datos de entrada contiene registros de origen. Estos registros contienen identificadores del consumidor, como nombre, apellidos, dirección de correo electrónico o número de teléfono. Estos registros de origen se pueden comparar con otros registros de origen que usted proporcione en la misma tabla de datos de entrada o en otras tablas. Cada registro debe tener un identificador de registro único (ID único) y debe definirlo como clave principal al crear un esquema de mapeo interno AWS Entity Resolution.

Todas las tablas de datos de entrada están disponibles como AWS Glue tablas respaldadas por Amazon S3. Puede utilizar sus datos de origen que ya están en Amazon S3 o importar tablas de datos de otros proveedores de SaaS de terceros a Amazon S3. Tras cargar los datos en Amazon S3, puede utilizar un AWS Glue rastreador para crear una tabla de datos en el AWS Glue Data Catalog. A continuación, puede utilizar la tabla de datos como entrada para AWS Entity Resolution.

En las siguientes secciones se describe cómo preparar datos propios y datos de terceros.

Temas

Preparación de los datos de entrada de origen

Los siguientes pasos describen cómo preparar los datos de origen para usarlos en un flujo de trabajo de emparejamiento basado en reglas, un flujo de trabajo de emparejamiento basado en el aprendizaje automático o un flujode trabajo de mapeo de ID.

Paso 1: Prepare tablas de datos propias

Cada tipo de flujo de trabajo coincidente tiene un conjunto diferente de recomendaciones y pautas para garantizar el éxito.

Para preparar tablas de datos propias, consulte la siguiente tabla:

Directrices sobre tablas de datos propias

Tipo de flujo de trabajo	¿Se necesita un identificador único?	Acciones
Flujo de trabajo de coincidencia basado en reglas	Sí	Asegúrese de lo siguiente: • El identificador único existe y no supera los 38 caracteres.

flujo de trabajo de emparejamiento basado en el aprendizaje automático	Sí	Asegúrese de lo siguiente:
		• Existe un identificador único.
		• El conjunto de datos contiene uno de los siguientes tipos:
		  • **`Full Name`**
		  • **`Full Address`**
		  • **`Full phone`**
		  • **`Email address`**
		  • **`Date`**— con una clave de coincidencia (el nombre de la fecha de nacimiento)

Flujo de trabajo de asignación de ID	Sí	Asegúrese de lo siguiente: • Existe un identificador único.

Paso 2: Guarde la tabla de datos de entrada en un formato de datos compatible

Si ya has guardado los datos de entrada de origen en un formato de datos compatible, puedes saltarte este paso.

Para poder AWS Entity Resolution utilizarlos, los datos de entrada deben estar en un formato AWS Entity Resolution compatible.

AWS Entity Resolution admite los siguientes formatos de datos:

- valor separado por comas (CSV)

- Parquet

Paso 3: Cargue la tabla de datos de entrada a Amazon S3

Si ya tiene su tabla de datos de origen en Amazon S3, puede omitir este paso.

> **Note**
>
> Los datos de entrada deben almacenarse en Amazon Simple Storage Service (Amazon S3) en el Cuenta de AWS mismo lugar Región de AWS y en el que desee ejecutar el flujo de trabajo correspondiente.

Para cargar la tabla de datos de entrada a Amazon S3

1. Inicie sesión en la consola de Amazon S3 AWS Management Console y ábrala en https://console.aws.amazon.com/s3/.
2. Elija Buckets y, a continuación, elija un bucket para almacenar su tabla de datos.
3. Elija Cargar y siga las indicaciones de la pantalla.
4. Seleccione la pestaña Objetos para ver el prefijo donde se almacenan sus datos. Anote el nombre de la carpeta.

   Puede seleccionar la carpeta para ver la tabla de datos.

Paso 4: Crear una AWS Glue tabla

> **Note**
>
> Si necesitas AWS Glue tablas particionadas, salta aPaso 4: Crea una tabla particionada AWS Glue.

Los datos de entrada en Amazon S3 deben catalogarse AWS Glue y representarse como una AWS Glue tabla. Para obtener más información sobre cómo crear una AWS Glue tabla con Amazon S3 como entrada, consulte Trabajar con rastreadores en la AWS Glue consola en la Guía para AWS Glue desarrolladores.

En este paso, debe configurar un rastreador AWS Glue que rastree todos los archivos del bucket de S3 y crear una tabla. AWS Glue

> **Note**
>
> AWS Entity Resolution actualmente no es compatible con las ubicaciones de Amazon S3 registradas en AWS Lake Formation.

Para crear una AWS Glue tabla

1. Inicie sesión en AWS Management Console y abra la AWS Glue consola en https://console.aws.amazon.com/glue/.
2. En la barra de navegación, seleccione Rastreadores.
3. Seleccione su bucket de S3 de la lista y, a continuación, elija Crear rastreador.
4. En la página Definir las propiedades del rastreador, introduzca un nombre del rastreador (opcional, una descripción) y, a continuación, seleccione Siguiente.
5. Continúe por la página Añadir rastreador y especifique los detalles.
6. En la página Elegir un rol de IAM, seleccione Elegir un rol de IAM existente y luego seleccione Siguiente.

   También puede seleccionar Crear un rol de IAM o pedir a su administrador cree el rol de IAM si es necesario.
7. En Crear una programación para este rastreador, mantenga el valor predeterminado para la Frecuencia (Ejecutar bajo demanda) y, a continuación, seleccione Siguiente.
8. En Configurar la salida del rastreador, introduzca la AWS Glue base de datos y, a continuación, seleccione Siguiente.
9. Revise todos los detalles y, a continuación, seleccione Finalizar.
10. En la página Rastreadores, active la casilla de verificación situada junto a su bucket de S3 y, a continuación, elija Ejecutar rastreador.
11. Cuando el rastreador termine de ejecutarse, en la barra de AWS Glue navegación, elija Bases de datos y, a continuación, elija el nombre de la base de datos.
12. En la página Base de datos, elija Tablas de {nombre de su base de datos}.

    a. Vea las tablas de la AWS Glue base de datos.

b. Para ver el esquema de una tabla, seleccione una tabla.

c. Anote el nombre de la AWS Glue base de datos y el nombre de AWS Glue la tabla.

Ahora está listo para crear un mapeo de esquemas. Para obtener más información, consulte Crear un esquema de mapeo.

Paso 4: Crea una tabla particionada AWS Glue

> **Note**
>
> La función de AWS Glue partición solo AWS Entity Resolution se admite en los flujos de trabajo de mapeo de ID. Esta función de AWS Glue particionamiento le permite elegir particiones específicas para procesarlas. AWS Entity Resolution
> Si no necesitas AWS Glue tablas particionadas, puedes saltarte este paso.

Una AWS Glue tabla particionada refleja automáticamente las nuevas particiones de la AWS Glue tabla cuando agregas nuevas carpetas a la estructura de datos (por ejemplo, una nueva carpeta de un día en un mes).

Al crear una AWS Glue tabla particionada AWS Entity Resolution, puedes especificar qué particiones quieres procesar en un flujo de trabajo de mapeo de ID. Luego, cada vez que ejecutas el flujo de trabajo de mapeo de ID, solo se procesan los datos de esas particiones, en lugar de procesar todos los datos de toda la AWS Glue tabla. Esta función permite un procesamiento de datos más preciso, eficiente y rentable AWS Entity Resolution, lo que le proporciona un mayor control y flexibilidad a la hora de gestionar las tareas de resolución de entidades.

Puede crear una AWS Glue tabla particionada para la cuenta de origen en un flujo de trabajo de mapeo de ID.

Primero debe catalogar los datos de entrada en Amazon S3 AWS Glue y representarlos como una AWS Glue tabla. Para obtener más información sobre cómo crear una AWS Glue tabla con Amazon S3 como entrada, consulte Trabajar con rastreadores en la AWS Glue consola en la Guía para AWS Glue desarrolladores.

En este paso, configuras un rastreador AWS Glue que rastrea todos los archivos de tu bucket de S3 y, a continuación, creas una tabla particionada. AWS Glue

> **Note**
>
> AWS Entity Resolution actualmente no es compatible con las ubicaciones de Amazon S3 registradas en AWS Lake Formation.

Para crear una tabla particionada AWS Glue

1. Inicie sesión en AWS Management Console y abra la AWS Glue consola en https://console.aws.amazon.com/glue/.
2. En la barra de navegación, seleccione Rastreadores.
3. Seleccione su bucket de S3 de la lista y, a continuación, elija Crear rastreador.
4. En la página Definir las propiedades del rastreador, introduzca el nombre del rastreador, una descripción opcional y, a continuación, seleccione Siguiente.
5. Continúe por la página Añadir rastreador y especifique los detalles.
6. En la página Elegir un rol de IAM, seleccione Elegir un rol de IAM existente y luego seleccione Siguiente.

   También puede seleccionar Crear un rol de IAM o pedir a su administrador cree el rol de IAM si es necesario.
7. En Crear una programación para este rastreador, mantenga el valor predeterminado para la Frecuencia (Ejecutar bajo demanda) y, a continuación, seleccione Siguiente.
8. En Configurar la salida del rastreador, introduzca la AWS Glue base de datos y, a continuación, seleccione Siguiente.
9. Revise todos los detalles y, a continuación, seleccione Finalizar.
10. En la página Rastreadores, active la casilla de verificación situada junto a su bucket de S3 y, a continuación, elija Ejecutar rastreador.
11. Cuando el rastreador termine de ejecutarse, en la barra de AWS Glue navegación, elija Bases de datos y, a continuación, elija el nombre de la base de datos.
12. En la página Base de datos, en Tablas, elija la tabla que desee particionar.
13. En la descripción general de la tabla, selecciona el menú desplegable Acciones y, a continuación, selecciona Editar tabla.

    a. En Propiedades de la tabla, selecciona Añadir.

b. Para la nueva clave, introduzca**`aerPushDownPredicateString`**.

c. Para el nuevo valor, introduzca**`'<PartitionKey>=<PartitionValue'`**.

d. Anote el nombre de la AWS Glue base de datos y el nombre de AWS Glue la tabla.

Ya puede hacer lo siguiente:

- Cree un esquema de mapeo y, a continuación, cree un flujo de trabajo de mapeo de ID para uno Cuenta de AWS.
- Cree una fuente de espacio de nombres de ID, cree un destino de espacio de nombres de ID y, a continuación, cree un flujo de trabajo de mapeo de ID en dos. Cuentas de AWS

Preparar los datos de entrada de terceros

Los servicios de datos de terceros proporcionan identificadores que pueden coincidir con sus identificadores conocidos.

AWS Entity Resolution actualmente es compatible con los siguientes servicios de proveedores de datos de terceros:

Servicios de proveedores de datos

Nombre de la empresa	Disponible Regiones de AWS	Identificador
LiveRamp	EE.UU. Este (Norte de Virginia) (us-east-1), EE.UU. Este (Ohio) (us-East-2) y EE.UU. Oeste (Oregon) (us-west-2)	ID de rampa
TransUnion	EE.UU. Este (Norte de Virginia) (us-east-1), EE.UU. Este (Ohio) (us-East-2) y EE.UU. Oeste (Oregon) (us-west-2)	TransUnion Individuo y hogar IDs
ID unificada 2.0	EE.UU. Este (Norte de Virginia) (us-east-1), EE.UU. Este (Ohio) (us-East-2) y	Dibuja un UID 2

Nombre de la empresa	Disponible Regiones de AWS	Identificador
	EE.UU. Oeste (Oregon) (us-west-2)	

Los siguientes pasos describen cómo preparar los datos de terceros para utilizar un flujo de trabajo de correspondencia basado en el servicio del proveedor o un flujo de trabajo de mapeo de ID basado en el servicio del proveedor.

Temas

- Paso 1: Suscríbase a un servicio de proveedor en AWS Data Exchange
- Paso 2: Prepare tablas de datos de terceros
- Paso 3: Guarde la tabla de datos de entrada en un formato de datos compatible
- Paso 4: Cargue la tabla de datos de entrada a Amazon S3
- Paso 5: Crear una AWS Glue tabla

Paso 1: Suscríbase a un servicio de proveedor en AWS Data Exchange

Si tienes una suscripción a través de un proveedor de servicios AWS Data Exchange, puedes ejecutar un flujo de trabajo coincidente con uno de los siguientes servicios de proveedor para hacer coincidir tus identificadores conocidos con los de tu proveedor preferido. Sus datos se compararán con un conjunto de entradas definido por su proveedor preferido.

Para suscribirse a un servicio de proveedor en AWS Data Exchange

1. Vea la lista de proveedores en AWS Data Exchange. Están disponibles las siguientes listas de proveedores:

   - LiveRamp
     - LiveRampResolución de identidad
     - LiveRampTranscodificación
   - TransUnion
     - TruAudience Resolución y enriquecimiento de la identidad
   - ID unificada 2.0
     - Resolución de identidad de Unified ID 2.0

2. Complete uno de los siguientes pasos, según el tipo de oferta.

   - Oferta privada: si ya tienes una relación con un proveedor, sigue el procedimiento de ofertas y productos privados de la Guía del AWS Data Exchange usuario para aceptar una oferta privada AWS Data Exchange.
   - Traiga su propia suscripción: si ya tiene una suscripción de datos existente con un proveedor, siga el procedimiento de ofertas de Bring Your Own Subscription (BYOS) de la Guía del AWS Data Exchange usuario para aceptar una oferta de BYOS. AWS Data Exchange
3. Una vez que te hayas suscrito a un servicio de proveedor AWS Data Exchange, podrás crear un flujo de trabajo coincidente o un flujo de trabajo de mapeo de identidades con ese servicio de proveedor.

Para obtener más información sobre cómo acceder a un producto de un proveedor que lo contenga APIs, consulte Acceder a un producto de API en la Guía del AWS Data Exchange usuario.

Paso 2: Prepare tablas de datos de terceros

Cada servicio de terceros tiene un conjunto diferente de recomendaciones y directrices para garantizar un flujo de trabajo adecuado.

Para preparar tablas de datos de terceros, consulta la siguiente tabla:

Pautas de servicios para proveedores de datos

Servicio para proveedores	¿Se necesita una identific ación única?	Acciones
LiveRamp	Sí	Asegúrese de lo siguiente: • El identificador único puede ser su propio identificador seudónimo o un identificador de fila. • El formato y la normalización del archivo de entrada de datos se ajustan a las LiveRamp directrices. Para obtener más información sobre las pautas de formato de los archivos de entrada para el flujo de trabajo correspon

Servicio para proveedores	¿Se necesita una identificación única?	Acciones
		diente, consulte Realizar la resolución de identidad mediante ADX en la LiveRamp documentación. Para obtener más información sobre las pautas de formato de los archivos de entrada para el flujo de trabajo de mapeo de ID, consulte Realizar la transcodificación mediante ADX en la documentación. LiveRamp

Servicio para proveedores	¿Se necesita una identific ación única?	Acciones

TransUnion	Sí	Asegúrese de que las siguientes columnas estén `string` escritas en la vista de entrada:
		• Se requiere un ID único y puede ser un ID de CRM, un ID de contacto, un ID de usuario o cualquier ID exclusivo.
		• **`Name`**
		  • **`First Name`**puede estar en minúsculas o mayúsculas, se admiten apodos, pero deben excluirse los títulos y sufijos.
		  • **`Last Name`**puede estar en mayúscula o minúscula, sin incluir las iniciales del medio.
		• **`Address`**
		  • **`Street address1`**y **`Street address1`** se combina en una sola **`Full address`** línea, si está presente.
		  • **`City`**está separado de**`Full address`**.
		  • **`Zip`**(o**`zip plus4`**), sin caracteres especiales como espacios, guiones o espacios en blanco. Utilice valores nulos si no hay datos.
		  • **`State`**se especifica como un código de 2 letras en mayúsculas.
		• • **`Phone`**
		  • **`Phone number`**debe tener 10 dígitos, sin caracteres especiales como espacios o guiones.
		• **`Email addresses`** es texto sin formato o cadenas en minúsculas SHA256 con hash.

Servicio para proveedores	¿Se necesita una identific ación única?	Acciones

		• **`Date of Birth`**está en formato y. `yyy-mm-dd`
		• **`Digital identifiers`** (Dispositivo IDs) se puede incluir IDs con guiones (dispositivo sin procesar de 36 caracteres IDs//IFAs) y sin guiones (dispositivoMAIDs/ /con código hash de 32 y 40 caracteres). IDs MAIDs IFAs
		  • **`IPV4`**es una dirección IP de 32 bits expresada en notación decimal punteada. Por ejemplo: `192.0.2.1`
		  • **`IPV6`**es una dirección IP de 128 bits expresada en notación hexadecimal, separada por dos puntos. Por ejemplo: `2001:db8:0000:0000:0000:0000:0000:0001`
		  • **`MAID`**(ID de publicidad móvil) es una cadena alfanumérica única que se asigna a un dispositivo móvil con fines publicitarios. Una SIRVIENTA suele tener 36 caracteres. Por ejemplo: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

Servicio para proveedores	¿Se necesita una identificación única?	Acciones
ID unificada 2.0	Sí	Asegúrese de lo siguiente: • El identificador único no puede ser un hash. • **`Email addresses`** Se usa uno **`Phone number`** o ambos en el esquema, no en ambos. • UID2 admite tanto el correo electrónico como el número de teléfono para UID2 la generación. Sin embargo, si ambos valores están presentes en la asignación del esquema, el flujo de trabajo duplica cada registro de la salida. Un registro usa el correo electrónico para la UID2 generación y el segundo registro usa el número de teléfono. Si sus datos incluyen una combinación de correos electrónicos y números de teléfono y no desea que se duplique esta duplicación de registros en la salida, lo mejor es crear un flujo de trabajo independiente para cada uno, con asignaciones de esquema independientes. En este escenario, realice los pasos dos veces: cree un flujo de trabajo para los correos electrónicos y otro independiente para los números de teléfono. **Note** Un correo electrónico o un número de teléfono específicos, en cualquier momento específico, dan como resultado el mismo UID2 valor bruto,

Servicio para proveedores	¿Se necesita una identific ación única?	Acciones
		independientemente de quién haya realizado la solicitud. UID2s Las sales crudas se obtienen añadiendo sales de cubos de sal que se giran aproximadamente una vez al año, lo que hace que la materia prima UID2 también se rote con ella. Los diferentes cubos de sal rotan en diferentes momentos del año. AWS Entity Resolution En la actualidad no lleva un registro de los cubos de sal giratorios ni en crudo UID2s, por lo que se recomienda regenerar el crudo a diario. UID2s Para obtener más información, consulta ¿Con qué frecuencia UID2s se deben actualizar las actualizaciones incrementales? en la documentación del UID 2.0.

Paso 3: Guarde la tabla de datos de entrada en un formato de datos compatible

Si ya has guardado los datos de entrada de terceros en un formato de datos compatible, puedes saltarte este paso.

Para poder utilizarlos AWS Entity Resolution, los datos de entrada deben estar en un formato AWS Entity Resolution compatible.

AWS Entity Resolution admite los siguientes formatos de datos:

- valor separado por comas (CSV)

> **Note**
>
> LiveRamp solo admite archivos CSV.

- Parquet

Paso 4: Cargue la tabla de datos de entrada a Amazon S3

Si ya tiene su tabla de datos de terceros en Amazon S3, puede omitir este paso.

> **Note**
>
> Los datos de entrada deben almacenarse en Amazon Simple Storage Service (Amazon S3) en el Cuenta de AWS mismo lugar Región de AWS y en el que desee ejecutar el flujo de trabajo correspondiente.

Para cargar la tabla de datos de entrada a Amazon S3

1. Inicie sesión en la consola de Amazon S3 AWS Management Console y ábrala en https://console.aws.amazon.com/s3/.
2. Elija Buckets y, a continuación, elija un bucket para almacenar su tabla de datos.
3. Elija Cargar y siga las indicaciones de la pantalla.
4. Seleccione la pestaña Objetos para ver el prefijo donde se almacenan sus datos. Anote el nombre de la carpeta.

   Puede seleccionar la carpeta para ver la tabla de datos.

Paso 5: Crear una AWS Glue tabla

Los datos de entrada en Amazon S3 deben catalogarse AWS Glue y representarse como una AWS Glue tabla. Para obtener más información sobre cómo crear una AWS Glue tabla con Amazon S3 como entrada, consulte Trabajar con rastreadores en la AWS Glue consola en la Guía para AWS Glue desarrolladores.

> **Note**
>
> AWS Entity Resolution no admite tablas particionadas.

En este paso, configuras un rastreador AWS Glue que rastrea todos los archivos de tu bucket de S3 y creas una tabla. AWS Glue

> **Note**
>
> AWS Entity Resolution actualmente no es compatible con las ubicaciones de Amazon S3 registradas en AWS Lake Formation.

Para crear una AWS Glue tabla

1. Inicie sesión en AWS Management Console y abra la AWS Glue consola en https://console.aws.amazon.com/glue/.
2. En la barra de navegación, seleccione Rastreadores.
3. Seleccione su bucket de S3 de la lista y, a continuación, elija Añadir rastreador.
4. En la página Añadir rastreador, introduzca el Nombre del rastreador y seleccione Siguiente.
5. Continúe por la página Añadir rastreador y especifique los detalles.
6. En la página Elegir un rol de IAM, seleccione Elegir un rol de IAM existente y luego seleccione Siguiente.

   También puede seleccionar Crear un rol de IAM o pedir a su administrador cree el rol de IAM si es necesario.
7. En Crear una programación para este rastreador, mantenga el valor predeterminado para la Frecuencia (Ejecutar bajo demanda) y, a continuación, seleccione Siguiente.
8. En Configurar la salida del rastreador, introduzca la AWS Glue base de datos y, a continuación, seleccione Siguiente.
9. Revise toda la información y, a continuación, elija Finalizar.
10. En la página Rastreadores, active la casilla de verificación situada junto a su bucket de S3 y, a continuación, elija Ejecutar rastreador.
11. Cuando el rastreador termine de ejecutarse, en la barra de AWS Glue navegación, elija Bases de datos y, a continuación, elija el nombre de la base de datos.

12. En la página Base de datos, elija Tablas de {nombre de su base de datos}.

    a. Vea las tablas de la AWS Glue base de datos.
    b. Para ver el esquema de una tabla, seleccione una tabla.
    c. Anote el nombre de la AWS Glue base de datos y el nombre de AWS Glue la tabla.

Ahora está listo para crear un mapeo de esquemas. Para obtener más información, consulte Crear un esquema de mapeo.

Defina los datos de entrada mediante el mapeo de esquemas

Un mapeo de esquemas define los datos de entrada que desea resolver. También proporciona metadatos sobre los datos de entrada, como los tipos de atributos de las columnas (campos de entrada) y las columnas en las que deben coincidir.

Al crear un esquema de mapeo, primero se definen los campos de entrada y los tipos de atributos y, a continuación, se definen las claves de coincidencia y los datos relacionados con el grupo. El siguiente diagrama resume cómo crear un mapeo de esquema.

Antes de crear un mapeo de esquemas, primero debe configurar AWS Entity Resolution y preparar las tablas de datos. Para obtener más información, consulte Configurar AWS Entity Resolution y Preparar tablas de datos de entrada.

Tras crear una asignación de esquemas, puede realizar una de las siguientes acciones:

- Cree un flujo de trabajo coincidente para buscar coincidencias entre diferentes entradas de datos.
- Cree una fuente de espacio de nombres de ID que pueda usar en un flujo de trabajo de mapeo de ID para traducir los datos de una fuente a un destino.
- Cree un flujo de trabajo de mapeo de ID dentro de la misma Cuenta de AWS utilizando su mapeo de esquemas como fuente.

Temas

- Crear un esquema de mapeo
- Clonar un mapeo de esquemas
- Edición de un mapeo de esquemas

- Eliminar un mapeo de esquemas

Crear un esquema de mapeo

Este procedimiento describe el proceso de creación de un mapeo de esquemas mediante la AWS Entity Resolution consola.

Hay tres formas de crear un mapeo de esquemas:

- Importe los datos de entrada existentes mediante la AWS Glue opción Importar desde: utilice este método de creación para definir los campos de entrada empezando por las columnas rellenadas previamente de una AWS Glue tabla mediante un flujo guiado.
- Definir manualmente los datos de entrada mediante la opción Crear un esquema personalizado: utilice este método de creación para definir manualmente los campos de entrada mediante un flujo guiado.
- Cree manualmente mediante la opción Usar el editor JSON: use un editor JSON para crear, usar una muestra o importar manualmente los datos de entrada existentes.

> **Note**
>
> Los campos de ID único y de entrada no están disponibles con esta opción.

Import from AWS Glue

Para crear un mapeo de esquemas importando los datos de entrada existentes desde AWS Glue

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona Asignaciones de esquemas.
3. En la página de mapeos de esquemas, en la esquina superior derecha, selecciona Crear mapeo de esquemas.
4. Para el paso 1: especificar los detalles del esquema, haga lo siguiente:

    a. En Nombre y método de creación, introduzca un nombre de mapeo del esquema y una descripción opcional.

b. En Método de creación, elija Importar desde AWS Glue.

c. Elija la AWS Glue base de datos en el menú desplegable y, a continuación, elija la AWS Glue tabla en el menú desplegable.

   Para crear una tabla nueva, ve a la AWS Glue consola. https://console.aws.amazon.com/glue/ Para obtener más información, consulte AWS Glue las tablas de la Guía AWS Glue del usuario.

d. En Unique ID, especifique la columna que hace referencia de forma distinta a cada fila de los datos.

   Example

   Por ejemplo: **`Primary_key`**, **`Row_ID`** o **`Record_ID`**.

   > **Note**
   >
   > La columna de ID único es obligatoria. El identificador único debe ser un identificador único dentro de una sola tabla. Sin embargo, en diferentes tablas, el identificador único puede tener valores duplicados. Si no se especifica el identificador único, no es único en la misma fuente o se superpone en términos de nombres de atributos en todas las fuentes, AWS Entity Resolution rechaza el registro cuando se ejecuta el flujo de trabajo coincidente. Si utiliza este esquema de mapeo en un flujo de trabajo de coincidencia basado en reglas, el identificador único no debe superar los 38 caracteres.

e. En el caso de los campos de entrada, elija las columnas que desee utilizar para la coincidencia y para la transferencia opcional.

   Puede elegir un máximo de 34 columnas en total tanto para hacer coincidir como para transferirlas.

   i. En Coincidencia, elija las columnas que desee utilizar como campos de entrada para la coincidencia.

      Puede elegir un máximo de 24 columnas en total para hacer coincidir.

   ii. Seleccione Añadir columnas para transferirlas si desea especificar las columnas que no se utilizan para hacer coincidir.

iii. (Opcional) En Transferir, elige las columnas que deseas incluir como columnas de transferencia.

f. (Opcional) Si desea habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.

g. Elija Siguiente.

5. En el paso 2: mapear los campos de entrada, defina los campos de entrada que desee usar para hacer coincidir y para transferirlos de forma opcional.

a. Para los campos de entrada que deben coincidir, para cada campo de entrada,

- Especifique el tipo de atributo para clasificar los datos.
- Especifique el nombre de la clave de coincidencia para permitir la comparación de los campos de entrada con el flujo de trabajo coincidente. De forma predeterminada, algunos nombres de claves coincidentes se asocian automáticamente a tipos de atributos específicos.
- Seleccione la casilla de verificación Compuesta si el valor de la columna de ese campo de entrada está codificado o deje la casilla en blanco si el valor es texto sin cifrar.

> **Note**
>
> Si va a crear un mapeo de esquemas para usarlo con la técnica de coincidencia basada en los LiveRamp servicios del proveedor, puede:
>
> - Especifique el tipo de atributo para el ID del proveedor como LiveRamp ID.
> - Especifique el tipo de atributo del campo de nombre en varios campos (por ejemplo, nombre o apellidos) o en un campo.
> - Especifique el tipo de atributo del campo de dirección postal en varios campos (por ejemplo, dirección postal 1, dirección postal 2) o en un campo (dirección completa).
>
>   Si coincide con una dirección, se requiere un código postal (código postal).
> - Si incluye el correo electrónico (dirección de correo electrónico) o el teléfono (número de teléfono) con un nombre, esos campos pueden coincidir con la dirección postal.

> **Note**
>
> Si va a crear un esquema de mapeo para usarlo con la técnica de coincidencia basada en los servicios del TransUnion proveedor, puede especificar cualquiera de los siguientes tipos de atributos:
>
> - Nombre completo, nombre y apellido
> - Dirección completa, dirección postal 1, ciudad, estado, país, código postal
> - Número de teléfono
> - Dirección de correo electrónico
> - Fecha
> - Identificadores digitales: IPV4IPV6, o MAID

> **Note**
>
> Si va a crear un mapeo de esquemas para usarlo con el flujo de trabajo de emparejamiento basado en el aprendizaje automático, su conjunto de datos debe contener al menos uno de los siguientes tipos de atributos:
>
> - Nombre completo
> - Dirección completa
> - Teléfono completo
> - Dirección de correo electrónico
> - Fecha con una clave que coincida con el nombre de la fecha de nacimiento
>
> No especifiques el tipo de atributo de ninguno de estos atributos como cadena personalizada.

b. (Opcional) En el caso de los campos de entrada que deban transferirse, añada los campos de entrada que no coincidan y su estado de cifrado correspondiente.

   El estado de cifrado indica si el valor de la columna de ese campo de entrada está codificado o es texto sin cifrar.

c. Elija Siguiente.

6. En el paso 3: Agrupar datos, puede agrupar los campos de entrada de nombre, dirección y número de teléfono si se han separado en varios campos.

   Este paso concatena los campos de entrada relacionados en un solo campo, lo que le permite compararlos como un solo campo en un flujo de trabajo coincidente.

   Si no tiene ningún dato asignado a los campos de entrada de nombre, dirección o número de teléfono, esta sección estará en blanco.

   También puede agregar más grupos si tiene más tipos de datos.

   a. Si quieres agrupar los datos de entrada de Name:

      En Nombre completo, elija dos o más campos de entrada que desee agrupar.

      El nombre del grupo y la clave de coincidencia se asocian automáticamente al tipo de datos.

      Puede actualizar el nombre del grupo y la clave de coincidencia con una clave de coincidencia personalizada que puede contener hasta 255 caracteres, incluidos letras, números, guiones bajos (_) o guiones (-).

      Seleccione Añadir grupo para añadir otro grupo.

      > **Note**
      >
      > La normalización solo se admite para el nombre completo.
      > Si desea normalizar los subtipos de nombre completo, asigne los siguientes subtipos al grupo de nombres completos: nombre, segundo nombre y apellido.

   b. Si desea agrupar los datos de entrada de la dirección:

      En Dirección completa, elija dos o más campos de campos de entrada que desee agrupar.

      El nombre del grupo y la clave de coincidencia se asocian automáticamente al tipo de datos.

Puede actualizar el nombre del grupo y la clave de coincidencia con una clave de coincidencia personalizada que puede contener hasta 255 caracteres, incluidos letras, números, guiones bajos (_) o guiones (-).

Seleccione Añadir grupo para añadir otro grupo.

> **Note**
>
> La normalización solo se admite para la dirección completa.
> Si desea normalizar los subtipos de dirección completa, asigne los siguientes subtipos al grupo de direcciones completo: dirección 1, dirección 2: nombre de la dirección 3, nombre de la ciudad, estado, país y código postal.

c. Si desea agrupar los datos de entrada del teléfono:

En Teléfono completo, elija dos o más campos de entrada que desee agrupar.

El nombre del grupo y la clave de coincidencia se asocian automáticamente al tipo de datos.

Puede actualizar el nombre del grupo y la clave de coincidencia con una clave de coincidencia personalizada que puede contener hasta 255 caracteres, incluidos letras, números, guiones bajos (_) o guiones (-).

Seleccione Añadir grupo para añadir otro grupo.

> **Note**
>
> La normalización solo es compatible con Full Phone.
> Si desea normalizar los subtipos de teléfono completos, asigne los siguientes subtipos al grupo de teléfonos completo: número de teléfono y código de país del teléfono.

d. Elija Siguiente.

7. Para el paso 4: revisar y crear, haga lo siguiente:

a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

b. Seleccione Crear mapeo de esquemas.

> **Note**
>
> No puede modificar un mapeo de esquemas después de asociarlo a un flujo de trabajo. Puede clonar un mapeo de esquema si quiere usar una configuración existente para crear un mapeo de esquema nuevo.

Tras crear el mapeo del esquema, estará listo para crear un flujo de trabajo coincidente o crear un espacio de nombres de ID.

Build custom schema

Para crear un mapeo de esquemas mediante la opción Crear un esquema personalizado

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona Asignaciones de esquemas.
3. En la página de mapeos de esquemas, en la esquina superior derecha, selecciona Crear mapeo de esquemas.
4. Para el paso 1: especificar los detalles del esquema, haga lo siguiente:

   a. Para el nombre y el método de creación, introduzca un nombre de mapeo del esquema y una descripción opcional.

   b. En Método de creación, elija Crear un esquema personalizado.

   c. En ID única, introduce una ID única para identificar cada fila de datos.

      Example

      Por ejemplo: **`Primary_key`**, **`Row_ID`** o **`Record_ID`**.

      > **Note**
      >
      > La columna de ID único es obligatoria. El identificador único debe ser un identificador único dentro de una sola tabla. Sin embargo, en diferentes tablas, el identificador único puede tener valores duplicados. Si no se especifica el identificador único, no es único en la misma fuente o se superpone en términos de nombres de atributos en todas las fuentes, AWS Entity Resolution rechaza

el registro cuando se ejecuta el flujo de trabajo coincidente. Si utiliza este esquema de mapeo en un flujo de trabajo de coincidencia basado en reglas, el identificador único no debe superar los 38 caracteres.

d. (Opcional) Si desea habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.

e. Elija Siguiente.

5. En el paso 2: mapear los campos de entrada, defina los campos de entrada que desee usar para hacer coincidir y para transferirlos de forma opcional.

   Puede definir un máximo de 34 columnas en total tanto para hacer coincidir como para transferirlas.

   a. Si desea que los campos de entrada coincidan, introduzca un campo de entrada.

   b. Seleccione el tipo de atributo para clasificar los datos.

> **Note**
>
> Si va a crear un mapeo de esquemas para usarlo con la técnica de coincidencia basada en los servicios del LiveRamp proveedor, puede especificar el tipo de atributo ProviderID como ID. LiveRamp Si desea incluir datos de PII en la salida, debe especificar el tipo de atributo como cadena personalizada.

> **Note**
>
> Si va a crear un mapeo de esquemas para usarlo con la técnica de coincidencia basada en los servicios del TransUnion proveedor, puede especificar cualquiera de los siguientes tipos de atributos:
>
> - Nombre completo, nombre y apellido
> - Dirección completa, dirección postal 1, ciudad, estado, país, código postal
> - Número de teléfono
> - Dirección de correo electrónico
> - Fecha
> - Identificadores digitales: IPV4IPV6, o MAID

> **Note**
>
> Si va a crear un mapeo de esquemas para usarlo con el flujo de trabajo de emparejamiento basado en el aprendizaje automático, su conjunto de datos debe contener al menos uno de los siguientes tipos de atributos:
>
> - Nombre completo
> - Dirección completa
> - Teléfono completo
> - Dirección de correo electrónico
> - Fecha con una clave que coincida con el nombre de la fecha de nacimiento
>
> No especifiques el tipo de atributo de ninguno de estos atributos como cadena personalizada.

c. Seleccione el nombre de la clave de coincidencia para permitir la comparación de los campos de entrada con su flujo de trabajo coincidente.

   De forma predeterminada, algunos nombres de claves coincidentes se asocian automáticamente a tipos de atributos específicos.

d. Seleccione la casilla de verificación Compuesta si el valor de la columna de ese campo de entrada está codificado o deje la casilla en blanco si el valor es texto sin cifrar.

e. Seleccione Añadir campo de entrada para añadir más campos de entrada.

   Puede añadir un máximo de 24 campos de entrada en total para que coincidan.

f. (Opcional) En el caso de los campos de entrada que deban transferirse, añade los campos de entrada que no coincidan y su estado de cifrado correspondiente.

g. Elija Siguiente.

6. En el paso 3: Agrupar datos, puedes agrupar los campos de entrada de nombre, dirección y número de teléfono si se han separado en varios campos.

   Este paso concatena los campos de entrada relacionados en un solo campo, lo que le permite compararlos como un solo campo en un flujo de trabajo coincidente.

Si no tiene ningún dato asignado a los campos de entrada de nombre, dirección o número de teléfono, esta sección estará en blanco.

También puede agregar más grupos si tiene más tipos de datos.

a. Si quieres agrupar los datos de entrada de Name:

   En Nombre completo, elija dos o más campos de entrada que desee agrupar.

   El nombre del grupo y la clave de coincidencia se asocian automáticamente al tipo de datos.

   Puede actualizar el nombre del grupo y la clave de coincidencia con una clave de coincidencia personalizada que puede contener hasta 255 caracteres, incluidos letras, números, guiones bajos (_) o guiones (-).

   Seleccione Añadir grupo para añadir otro grupo.

   > **Note**
   >
   > La normalización solo se admite para el nombre completo.
   > Si desea normalizar los subtipos de nombre completo, asigne los siguientes subtipos al grupo de nombres completos: nombre, segundo nombre y apellido.

b. Si desea agrupar los datos de entrada de la dirección:

   En Dirección completa, elija dos o más campos de campos de entrada que desee agrupar.

   El nombre del grupo y la clave de coincidencia se asocian automáticamente al tipo de datos.

   Puede actualizar el nombre del grupo y la clave de coincidencia con una clave de coincidencia personalizada que puede contener hasta 255 caracteres, incluidos letras, números, guiones bajos (_) o guiones (-).

   Seleccione Añadir grupo para añadir otro grupo.

> **Note**
>
> La normalización solo se admite para la dirección completa.
> Si desea normalizar los subtipos de dirección completa, asigne los siguientes subtipos al grupo de direcciones completo: dirección 1, dirección 2: nombre de la dirección 3, nombre de la ciudad, estado, país y código postal.

c. Si desea agrupar los datos de entrada del teléfono:

   En Teléfono completo, elija dos o más campos de entrada que desee agrupar.

   El nombre del grupo y la clave de coincidencia se asocian automáticamente al tipo de datos.

   Puede actualizar el nombre del grupo y la clave de coincidencia con una clave de coincidencia personalizada que puede contener hasta 255 caracteres, incluidos letras, números, guiones bajos (_) o guiones (-).

   Seleccione Añadir grupo para añadir otro grupo.

> **Note**
>
> La normalización solo es compatible con Full Phone.
> Si desea normalizar los subtipos de teléfono completos, asigne los siguientes subtipos al grupo de teléfonos completo: número de teléfono y código de país del teléfono.

d. Elija Siguiente.

7. Para el paso 4: revisar y crear, haga lo siguiente:

   a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

   b. Seleccione Crear mapeo de esquemas.

> **Note**
>
> No puede modificar un mapeo de esquemas después de asociarlo a un flujo de trabajo. Puede clonar un mapeo de esquema si quiere usar una configuración existente para crear un mapeo de esquema nuevo.

Tras crear el mapeo del esquema, estará listo para crear un flujo de trabajo coincidente o crear un espacio de nombres de ID.

Use JSON editor

Para crear un mapeo de esquemas mediante el editor JSON

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona Asignaciones de esquemas.
3. En la página de mapeos de esquemas, en la esquina superior derecha, selecciona Crear mapeo de esquemas.
4. Para el paso 1: especificar los detalles del esquema, haga lo siguiente:
    a. Para el nombre y el método de creación, introduzca un nombre de mapeo del esquema y una descripción opcional.
    b. En Método de creación, selecciona Usar el editor JSON.
    c. (Opcional) Si quieres habilitar las etiquetas para el recurso, selecciona Añadir nueva etiqueta y, a continuación, introduce el par clave y valor.
    d. Elija Siguiente.
5. Para el paso 2: especifique el mapeo:
    a. Comience a crear el esquema en el editor JSON o elija una de las siguientes opciones en función de su objetivo:

Su objetivo	Opción recomendada
Comience a crear su mapeo de esquemas	Inserte un ejemplo de JSON y, a continuación, edite la información según sea necesario.
Utilice un archivo JSON existente	Importar desde archivo

> **Note**
>
> La normalización solo se admite para los siguientes tipos: `NAMEADDRESS`,`PHONE`, y`EMAIL_ADRESS`.
> Si desea normalizar los **`NAME`** subtipos, asigne los siguientes subtipos a GroupName:**`NAME`**, y `NAME_FIRST` `NAME_MIDDLE` `NAME_LAST`
> Si desea normalizar los `ADDRESS` subtipos, asigne los siguientes subtipos a `ADDRESS` GroupName:`ADDRESS_STREET1`,,, `ADDRESS_STREET2` `ADDRESS_STREET3``ADDRESS_CITY`, `ADDRESS_STATE` y. `ADDRESS_COUNTRY` `ADDRESS_POSTALCODE`
> Si desea normalizar los **`PHONE`** subtipos, asigne los siguientes subtipos a GroupName: **`PHONE`** y. `PHONE_NUMBER` `PHONE_COUNTRYCODE`

b. Elija Siguiente.

6. Para el paso 3: Revise y cree:

   a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

   b. Seleccione Crear mapeo de esquemas.

> **Note**
>
> No puede modificar un mapeo de esquemas después de asociarlo a un flujo de trabajo. Puede clonar un mapeo de esquema si quiere usar una configuración existente para crear un mapeo de esquema nuevo.

Tras crear el mapeo del esquema, estará listo para crear un flujo de trabajo coincidente o crear un espacio de nombres de ID.

Clonar un mapeo de esquemas

Puede clonar un mapeo de esquema si quiere usar una configuración existente para crear un mapeo de esquema nuevo.

Para clonar un mapeo de esquemas:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona Asignaciones de esquemas.
3. Elija el mapeo de esquemas.
4. Elija Clonar.
5. En la página Especificar los detalles del esquema, realice los cambios necesarios y, a continuación, elija Siguiente.
6. En la página Elegir una técnica coincidente, realice los cambios necesarios y, a continuación, seleccione Siguiente.
7. En la página de campos de entrada del mapa, realice los cambios necesarios y, a continuación, seleccione Siguiente.
8. En la página Datos del grupo, realice los cambios necesarios y, a continuación, seleccione Siguiente.
9. En la página Revisar y guardar, realice los cambios necesarios y, a continuación, seleccione Clonar el mapeo de esquemas.

Edición de un mapeo de esquemas

Solo puede editar una asignación de esquemas antes de asociarla a un flujo de trabajo. Una vez que haya asociado un mapeo de esquema a un flujo de trabajo, no podrá editarlo. Puede clonar un mapeo de esquema si quiere usar una configuración existente para crear un mapeo de esquema nuevo.

Para editar una asignación de esquemas:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona Asignaciones de esquemas.
3. Elija el mapeo de esquemas.
4. Seleccione Editar.
5. En la página Especificar los detalles del esquema, realice los cambios necesarios y, a continuación, elija Siguiente.
6. En la página Elegir una técnica coincidente, realice los cambios necesarios y, a continuación, seleccione Siguiente.
7. En la página de campos de entrada del mapa, realice los cambios necesarios y, a continuación, seleccione Siguiente.
8. En la página Datos del grupo, realice los cambios necesarios y, a continuación, seleccione Siguiente.

> **Note**
>
> La normalización solo se admite para el nombre completo, la dirección completa, el teléfono completo y la dirección de correo electrónico.
> Si desea normalizar los subtipos de nombre completo, asigne los siguientes subtipos al grupo de nombres completos: nombre, segundo nombre y apellido.
> Si desea normalizar los subtipos de dirección completa, asigne los siguientes subtipos al grupo de direcciones completas: dirección 1, dirección 2: nombre de la dirección 3, nombre de la ciudad, estado, país y código postal.
> Si desea normalizar los subtipos de teléfono completos, asigne los siguientes subtipos al grupo de teléfonos completo: número de teléfono y código de país del teléfono.

9. En la página Revisar y guardar, realice los cambios necesarios y, a continuación, seleccione Editar mapeo de esquemas.

Eliminar un mapeo de esquemas

No puede eliminar una asignación de esquemas cuando está asociada a un flujo de trabajo coincidente. Primero debe eliminar la asignación de esquemas de todos los flujos de trabajo coincidentes asociados antes de poder eliminarla.

Para eliminar una asignación de esquemas:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona Asignaciones de esquemas.
3. Elija el mapeo de esquemas.
4. Elija Eliminar.
5. Confirme la eliminación y luego elija Eliminar.

Defina los datos de entrada mediante un espacio de nombres de ID

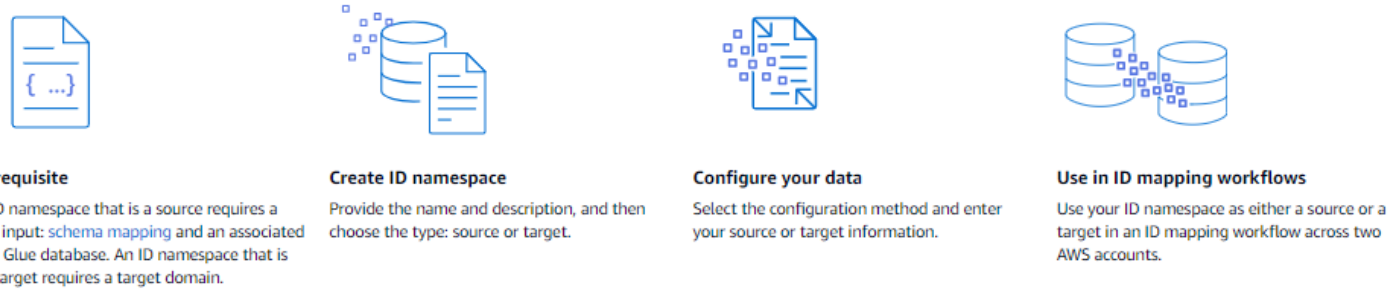
Un espacio de nombres de ID es un envoltorio alrededor de la tabla de datos de entrada. Utiliza un espacio de nombres de ID para proporcionar metadatos que expliquen los datos de entrada y las técnicas de coincidencia y cómo utilizarlos en un flujo de trabajo de mapeo de ID.

Hay dos tipos de espacios de nombres de ID: origen y destino.

- La fuente contiene configuraciones para los datos de origen que se AWS Entity Resolution procesan en un flujo de trabajo de mapeo de ID.
- El destino contiene una configuración de los datos de destino que utilizan todas las fuentes.

Puede definir los datos de entrada que desea resolver Cuentas de AWS en dos en un flujo de trabajo de mapeo de ID. Un participante crea una fuente de espacio de nombres de ID y otro un destino de espacio de nombres de ID. Una vez que los participantes hayan creado la fuente y el destino, puede ejecutar un flujo de trabajo de mapeo de ID para traducir los datos de la fuente al destino.

El siguiente diagrama resume cómo crear un espacio de nombres de ID para usarlo en un flujo de trabajo de mapeo de ID.



En las siguientes secciones se describe cómo crear una fuente de espacio de nombres de ID y un destino de espacio de nombres de ID.

Temas

- Fuente del espacio de nombres de ID
- ID: espacio de nombres: objetivo
- Edición de un espacio de nombres de ID

- Eliminar un espacio de nombres de ID
- Añadir o actualizar una política de recursos para un espacio de nombres de ID

Fuente del espacio de nombres de ID

La fuente del espacio de nombres de ID es la fuente de los datos en un flujo de trabajo de mapeo de ID.

Antes de crear una fuente de espacio de nombres de ID, primero debe crear un esquema de mapeo o un flujo de trabajo coincidente, según su caso de uso. Para obtener más información, consulte Crear un esquema de mapeo y Haga coincidir los datos de entrada mediante un flujo de trabajo coincidente.

Después de crear una fuente de espacio de nombres de ID, puede usarla junto con un destino de espacio de nombres de ID en un flujo de trabajo de mapeo de ID. Para obtener más información, consulte Mapee los datos de entrada mediante un flujo de trabajo de mapeo de ID.

Hay dos formas de crear una fuente de espacio de nombres de ID en la AWS Entity Resolution consola: el método basado en reglas o el método de servicios del proveedor.

Temas

- Crear una fuente de espacio de nombres de ID (basada en reglas)
- Crear una fuente de espacio de nombres de ID (servicios del proveedor)

Crear una fuente de espacio de nombres de ID (basada en reglas)

En este tema se describe el proceso de creación de una fuente de espacio de nombres de ID mediante el método basado en reglas. Este método utiliza reglas de coincidencia para traducir datos propios de una fuente a un destino en un flujo de trabajo de mapeo de ID.

> **Note**
>
> Si los datos de entrada son la fuente, deben tener un esquema de mapeo y una AWS Glue base de datos asociada.

Para crear una fuente de espacio de nombres de ID (basada en reglas)

1. Inicie sesión en AWS Management Console y abra la consola en. AWS Entity Resolution https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona los espacios de nombres de ID.
3. En la página de espacios de nombres de ID, en la esquina superior derecha, selecciona Crear espacio de nombres de ID.
4. Para obtener más información, haz lo siguiente:
   a. Para el nombre del espacio de nombres de ID, introduzca un nombre único.
   b. (Opcional) En Descripción, introduzca una descripción opcional.
   c. Para el tipo de espacio de nombres de ID, elija Fuente.
5. Para el método de espacio de nombres de ID, selecciona Basado en reglas.
6. Para la entrada de datos, elija el tipo de entrada que desee usar y, a continuación, lleve a cabo las acciones recomendadas.

Tipo de entrada	Acciones recomendadas
Un esquema de mapeo existente	1. Elija el mapeo de esquemas. 2. Elija la AWS Glue base de datos, la AWS Glue tabla y el mapeo de esquemas en la lista desplegable. Puede añadir hasta 20 entradas de datos.
Un flujo de trabajo coincidente existente	1. Elija el flujo de trabajo coincidente. 2. Elige la cuenta que está asociada al espacio de nombres de ID: tuya Cuenta de AWS u otra. Cuenta de AWS 3. Según el tipo de cuenta, seleccione el nombre del flujo de trabajo coincidente o introduzca el ARN del flujo de trabajo coincidente.

7. Para los parámetros de la regla, haga lo siguiente.

a. Especifique los controles de la regla eligiendo una de las siguientes opciones en función de su objetivo.

Su objetivo	Opción recomendada
Permita reglas tanto del origen como del destino	Sin preferencia
Elija si una fuente, un destino o ambos pueden proporcionar reglas en un flujo de trabajo de mapeo de ID	Reglas limitadas

Los controles de reglas deben ser compatibles entre el origen y el destino para poder utilizarlos en un flujo de trabajo de mapeo de ID. Por ejemplo, si un espacio de nombres de ID de origen limita las reglas al destino, pero el espacio de nombres de ID de destino limita las reglas al origen, se produce un error.

b. Especifique las reglas de coincidencia eligiendo una de las siguientes opciones en función del tipo de entrada de datos.

Tipo de entrada de datos	Acción recomendada
Mapeo de esquemas	Seleccione Añadir otra regla para añadir una regla coincidente. Puede aplicar hasta 25 reglas de coinciden cia para definir sus criterios de coinciden cia.
Flujo de trabajo correspondiente	Elija Usar reglas del flujo de trabajo coincidente o Proporcionar reglas nuevas para definir sus reglas coincidentes.

8. Para los parámetros de comparación y coincidencia, haga lo siguiente.

a. Especifique el tipo de comparación eligiendo una de las siguientes opciones en función de su objetivo.

Su objetivo	Opción recomendada
Permita que se utilice cualquier tipo de comparación al crear el flujo de trabajo de mapeo de ID.	Sin preferencia
Busque cualquier combinación de coincidencias entre los datos almacenados en varios campos de entrada, independientemente de si los datos están en el mismo campo de entrada o en uno diferente.	Varios campos de entrada
Limite la comparación dentro de un único campo de entrada cuando no deban coincidir datos similares almacenados en varios campos de entrada.	Campo de entrada único

b. Especifique el tipo de registro coincidente eligiendo una de las siguientes opciones en función de su objetivo.

Su objetivo	Opción recomendada
Permita que se utilice cualquier tipo de comparación al crear el flujo de trabajo de mapeo de ID.	Sin preferencia
Limite el tipo de registro coincidente para almacenar solo un registro coincidente en el origen por cada registro coincidente del destino cuando cree el flujo de trabajo de asignación de ID.	Coincidencia de registros limitada y De una fuente a un destino

Su objetivo	Opción recomendada
Limite el tipo de registro coincidente para almacenar solo registros coincidentes en el origen por cada registro coincidente del destino cuando cree el flujo de trabajo de asignación de ID.	Coincidencia de registros limitada y Muchas fuentes para un objetivo

> **Note**
>
> Debe especificar las limitaciones compatibles para los espacios de nombres de los identificadores de origen y destino. Por ejemplo, si un espacio de nombres de ID de origen limita las reglas al destino, pero el espacio de nombres de ID de destino limita las reglas al origen, se produce un error.

9. Especifique los permisos de acceso al servicio eligiendo un nombre de rol de servicio existente en la lista desplegable.
10. (Opcional) Para habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.
11. Elija Creación de un espacio de nombres de ID.

Se crea la fuente del espacio de nombres de ID. Ahora está listo para crear un destino de espacio de nombres de ID.

Crear una fuente de espacio de nombres de ID (servicios del proveedor)

En este tema se describe el proceso de creación de una fuente de espacio de nombres de ID mediante el método Provider Services. Este método usa un servicio de proveedor llamado. LiveRamp LiveRamp traduce datos codificados de terceros de una fuente a un destino durante un flujo de trabajo de mapeo de ID.

> **Note**
>
> Si los datos de entrada son la fuente, deben tener un esquema de mapeo y una AWS Glue base de datos asociada.

Para crear una fuente de espacio de nombres de ID (servicios del proveedor)

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en. https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona los espacios de nombres de ID.
3. En la página de espacios de nombres de ID, en la esquina superior derecha, selecciona Crear espacio de nombres de ID.
4. Para obtener más información, haz lo siguiente:

   a. Para el nombre del espacio de nombres de ID, introduzca un nombre único.

   b. (Opcional) En Descripción, introduzca una descripción opcional.

   c. Para el tipo de espacio de nombres de ID, elija Fuente.
5. Para el método de espacio de nombres de ID, selecciona Provider services.

   > **Note**
   >
   > AWS Entity Resolution actualmente ofrece el servicio del LiveRamp proveedor como un método de espacio de nombres de ID. Si tiene una suscripción a LiveRamp, el estado aparece como Suscrito. Para obtener más información sobre cómo suscribirse LiveRamp, consultePaso 1: Suscríbase a un servicio de proveedor en AWS Data Exchange.
6. Para la entrada de datos, elija la AWS Glue base de datos, la AWS Glue tabla y el mapeo del esquema en la lista desplegable.

   Puede añadir hasta 20 entradas de datos.
7. Para especificar los permisos de acceso al servicio, elija una opción y lleve a cabo la acción recomendada.

Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla.

Opción	Acción recomendada
	• El nombre del rol de servicio predeterminado es `entityresolution-id-mapping-workflow-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, elija la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

8. (Opcional) Para habilitar las etiquetas para el recurso, selecciona Añadir nueva etiqueta y, a continuación, introduce el par clave y valor.
9. Elija Creación de un espacio de nombres de ID.

Se crea la fuente del espacio de nombres de ID. Ahora está listo para crear un destino de espacio de nombres de ID.

ID: espacio de nombres: objetivo

El objetivo del espacio de nombres de ID es el destino de los datos en un flujo de trabajo de mapeo de ID. Todas las fuentes se dirigen al destino.

Antes de crear un destino de espacio de nombres con ID, primero debes crear un flujo de trabajo coincidente o tener una suscripción a un servicio de proveedor (LiveRamp), según tu caso de uso. Para obtener más información, consulte Haga coincidir los datos de entrada mediante un flujo de trabajo coincidente y Paso 1: Suscríbase a un servicio de proveedor en AWS Data Exchange.

Después de crear un objetivo de espacio de nombres de ID, puede usarlo junto con una fuente de espacio de nombres de ID en un flujo de trabajo de mapeo de ID. Para obtener más información, consulte Mapee los datos de entrada mediante un flujo de trabajo de mapeo de ID.

Hay dos formas de crear un destino de espacio de nombres de ID en la AWS Entity Resolution consola: el método basado en reglas o el método de servicios del proveedor.

Temas

- Crear un objetivo de espacio de nombres de ID (método basado en reglas)
- Crear un destino de espacio de nombres de ID (método de servicios del proveedor)

Crear un objetivo de espacio de nombres de ID (método basado en reglas)

En este tema se describe el proceso de creación de un destino de espacio de nombres de ID mediante el método basado en reglas. Este método utiliza reglas de coincidencia para traducir datos propios de una fuente a un destino durante un flujo de trabajo de mapeo de ID.

Para crear un objetivo de espacio de nombres de ID (basado en reglas)

1. Inicie sesión en AWS Management Console y abra la consola en. AWS Entity Resolution https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona los espacios de nombres de ID.
3. En la página de espacios de nombres de ID, en la esquina superior derecha, selecciona Crear espacio de nombres de ID.

4. Para obtener más información, haz lo siguiente:

    a. Para el nombre del espacio de nombres de ID, introduzca un nombre único.

    b. (Opcional) En Descripción, introduzca una descripción opcional.

    c. Para el tipo de espacio de nombres de ID, elija Target.

5. Para el método de espacio de nombres de ID, selecciona Basado en reglas.

6. Para la entrada de datos, en Flujo de trabajo coincidente, haga lo siguiente.

    a. Elige la cuenta que está asociada al espacio de nombres de ID: tuya Cuenta de AWS o de otra. Cuenta de AWS

    b. Según el tipo de cuenta, seleccione el nombre del flujo de trabajo coincidente o introduzca el ARN del flujo de trabajo coincidente.

7. Para los parámetros de la regla, haga lo siguiente.

    a. Especifique los controles de la regla eligiendo una de las siguientes opciones en función de su objetivo.

Su objetivo	Opción recomendada
Permita reglas tanto del origen como del destino	Sin preferencia
Elija si una fuente, un destino o ambos pueden proporcionar reglas en un flujo de trabajo de mapeo de ID	Reglas limitadas

    Los controles de reglas deben ser compatibles entre el origen y el destino para poder utilizarlos en un flujo de trabajo de mapeo de ID. Por ejemplo, si un espacio de nombres de ID de origen limita las reglas al destino, pero el espacio de nombres de ID de destino limita las reglas al origen, se produce un error.

    b. En el caso de las reglas de coincidencia, agrega AWS Entity Resolution automáticamente las reglas del flujo de trabajo de coincidencia.

8. Para los parámetros de comparación y coincidencia, haga lo siguiente.

    a. Especifique el tipo de comparación eligiendo una de las siguientes opciones en función de su objetivo.

Su objetivo	Opción recomendada
Permita que se utilice cualquier tipo de comparación al crear el flujo de trabajo de mapeo de ID.	Sin preferencia
Busque cualquier combinación de coincidencias entre los datos almacenados en varios campos de entrada, independientemente de si los datos están en el mismo campo de entrada o en uno diferente.	Varios campos de entrada
Limite la comparación dentro de un único campo de entrada cuando no deban coincidir datos similares almacenados en varios campos de entrada.	Campo de entrada único

b. Especifique el tipo de registro coincidente eligiendo una de las siguientes opciones en función de su objetivo.

Su objetivo	Opción recomendada
Permita que se utilice cualquier tipo de comparación al crear el flujo de trabajo de mapeo de ID.	Sin preferencia
Limite el tipo de registro coincidente para almacenar solo un registro coincidente en el origen por cada registro coincidente del destino cuando cree el flujo de trabajo de asignación de ID.	Coincidencia de registros limitada y De una fuente a un destino

Su objetivo	Opción recomendada
Limite el tipo de registro coincidente para almacenar solo registros coincidentes en el origen por cada registro coincidente del destino cuando cree el flujo de trabajo de asignación de ID.	Coincidencia de registros limitada y Muchas fuentes para un objetivo

> **Note**
>
> Debe especificar las limitaciones compatibles para los espacios de nombres de los identificadores de origen y destino. Por ejemplo, si un espacio de nombres de ID de origen limita las reglas al destino, pero el espacio de nombres de ID de destino limita las reglas al origen, se produce un error.

9. Especifique los permisos de acceso al servicio eligiendo un nombre de rol de servicio existente en la lista desplegable.
10. (Opcional) Para habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.
11. Elija Creación de un espacio de nombres de ID.

Se crea el objetivo del espacio de nombres ID. Tras crear los espacios de nombres de ID (origen y destino) necesarios para un flujo de trabajo de mapeo de ID, estará listo para crear un flujo de trabajo de mapeo de ID.

Crear un destino de espacio de nombres de ID (método de servicios del proveedor)

En este tema se describe el proceso de creación de un destino de espacio de nombres de ID mediante el método Provider Services. Este método usa un servicio de proveedor llamado. LiveRamp LiveRamp traduce datos codificados de terceros de una fuente a un destino durante un flujo de trabajo de mapeo de ID.

Para crear un objetivo de espacio de nombres de ID (servicios del proveedor)

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en. https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona los espacios de nombres de ID.
3. En la página de espacios de nombres de ID, en la esquina superior derecha, selecciona Crear espacio de nombres de ID.
4. Para obtener más información, haz lo siguiente:
   a. Para el nombre del espacio de nombres de ID, introduzca un nombre único.
   b. (Opcional) En Descripción, introduzca una descripción opcional.
   c. Para el tipo de espacio de nombres de ID, elija Target.
5. Para el método de espacio de nombres de ID, elija Provider services.

> **Note**
>
> AWS Entity Resolution actualmente ofrece el servicio del LiveRamp proveedor como un método de espacio de nombres de ID.
> Si tiene una suscripción a LiveRamp, el estado aparece como Suscrito.
> Para obtener más información sobre cómo suscribirse LiveRamp, consulte Paso 1: Suscríbase a un servicio de proveedor en AWS Data Exchange.

6. Para el dominio de destino, introduzca el identificador del dominio del LiveRamp cliente destinado a la transcodificación que LiveRamp proporciona.
7. (Opcional) Para habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.
8. Elija Creación de un espacio de nombres de ID.

Se crea el objetivo del espacio de nombres ID. Tras crear los espacios de nombres de ID (origen y destino) necesarios para un flujo de trabajo de mapeo de ID, estará listo para crear el flujo de trabajo de mapeo de ID.

Edición de un espacio de nombres de ID

Solo puedes editar un espacio de nombres de ID antes de asociarlo a un flujo de trabajo de mapeo de ID. Una vez que hayas asociado un espacio de nombres de ID a un flujo de trabajo de mapeo de ID, no podrás editarlo.

Para editar un espacio de nombres de ID:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en. https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona los espacios de nombres de ID.
3. Elija el espacio de nombres de ID.
4. Seleccione Editar.
5. En la página Editar el espacio de nombres de ID, realiza los cambios necesarios y, a continuación, selecciona Guardar.

Eliminar un espacio de nombres de ID

No puedes eliminar un espacio de nombres de ID cuando está asociado a un flujo de trabajo de mapeo de ID. Primero debes eliminar el mapeo de esquemas de todos los flujos de trabajo de mapeo de ID asociados antes de poder eliminarlo.

Para eliminar un espacio de nombres de ID:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en. https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona los espacios de nombres de ID.
3. Elija el espacio de nombres de ID.
4. Elija Eliminar.
5. Confirme la eliminación y luego elija Eliminar.

Añadir o actualizar una política de recursos para un espacio de nombres de ID

Una política de recursos permite al creador del recurso de mapeo de ID acceder a tu recurso de espacio de nombres de ID.

Para añadir o actualizar una política de recursos

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona los espacios de nombres de ID.
3. Elija el espacio de nombres de ID.
4. En la página de detalles del espacio de nombres de ID, selecciona la pestaña Permisos.
5. En la sección Política de recursos, selecciona Editar.
6. Agrega o actualiza la política en el editor JSON.
7. Seleccione Save changes (Guardar cambios).

Haga coincidir los datos de entrada mediante un flujo de trabajo coincidente

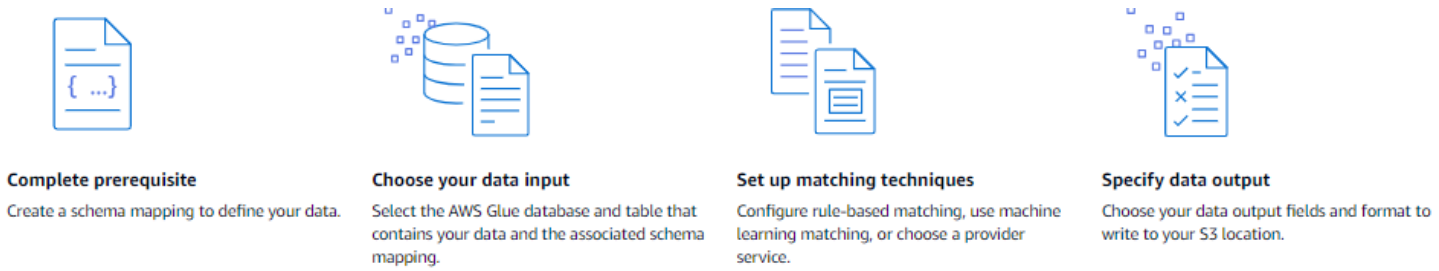
Un flujo de trabajo coincidente es un trabajo de procesamiento de datos que combina y compara datos de diferentes fuentes de entrada y determina cuáles coinciden en función de diferentes técnicas de coincidencia. Genera una tabla de salida de datos.

Al crear un flujo de trabajo coincidente, primero se especifican las entradas de datos y los pasos de normalización y, a continuación, se eligen las técnicas de coincidencia y la salida de datos que desee. AWS Entity Resolution lee los datos de la ubicación o ubicaciones especificadas y busca una coincidencia entre dos o más registros de los datos. A continuación, asigna un identificador de coincidencia a los registros del conjunto de datos coincidente. AWS Entity Resolution a continuación, escribe los archivos de salida de datos en la ubicación que elija. Si lo desea, puede AWS Entity Resolution utilizar el hash de los datos de salida, lo que le ayuda a mantener el control sobre los datos.

Un flujo de trabajo coincidente puede tener varias ejecuciones y los resultados (aciertos o errores) se escriben en una carpeta con el `jobId` nombre.

La salida de datos contiene un archivo para las coincidencias correctas y un archivo para los errores. La salida de datos puede contener varios campos. Los resultados correctos se escriben en una `success` carpeta que contiene varios archivos y cada archivo contiene un subconjunto de los registros correctos. Del mismo modo, los errores se escriben en una `error` carpeta con varios campos, cada uno de los cuales contiene un subconjunto de los registros de errores. Para obtener más información sobre la solución de errores, consulteSolución de problemas de flujos de trabajo.

El siguiente diagrama resume cómo crear un flujo de trabajo coincidente.



Antes de crear un flujo de trabajo coincidente, primero debe crear un mapeo de esquemas. Para obtener más información, consulte Crear un esquema de mapeo.

Hay tres formas de crear un flujo de trabajo coincidente, basado en técnicas de coincidencia: basado en reglas, basado enaprendizaje automático o basado en los servicios del proveedor.

Tras crear y ejecutar un flujo de trabajo coincidente, puede hacer lo siguiente:

- Vea los resultados en la ubicación de S3 que especificó. Los flujos de trabajo coincidentes se generan IDs después de indexar los datos.
- Utilice el resultado del emparejamiento basado en reglas o el emparejamiento mediante aprendizaje automático (ML) como entrada para el emparejamiento basado en los servicios del proveedor o al revés para satisfacer las necesidades de su empresa.

Por ejemplo, para ahorrar costos de suscripción a los proveedores, primero puede ejecutar una búsqueda de coincidencias basada en reglas para encontrar coincidencias en sus datos. A continuación, puede enviar un subconjunto de registros no coincidentes a la búsqueda de coincidencias basada en los servicios del proveedor.

Temas

- Crear un flujo de trabajo de coincidencia basado en reglas
- Crear un flujo de trabajo coincidente basado en el aprendizaje automático
- Crear un flujo de trabajo coincidente basado en los servicios del proveedor
- Edición de un flujo de trabajo coincidente
- Eliminar un flujo de trabajo coincidente
- Modificar o generar un identificador de coincidencia para un flujo de trabajo coincidente basado en reglas
- Búsqueda de un identificador de coincidencia para un flujo de trabajo de coincidencia basado en reglas
- Eliminar registros de un flujo de trabajo coincidente basado en reglas o aprendizaje automático
- Solución de problemas de flujos de trabajo

Crear un flujo de trabajo de coincidencia basado en reglas

La coincidencia basada en reglas es un conjunto jerárquico de reglas de coincidencia en cascada, sugeridas por AWS Entity Resolution, en función de los datos que usted introduce y que usted puede configurar completamente. El flujo de trabajo de coincidencia basado en reglas le permite comparar

texto sin formato o datos cifrados para encontrar coincidencias exactas en función de los criterios que personalice.

Cuando AWS Entity Resolution encuentra una coincidencia entre dos o más registros de los datos, asigna:

- Un identificador de coincidencia para los registros del conjunto de datos coincidente
- La regla de coincidencia que generó la coincidencia.

Para crear un flujo de trabajo de coincidencia basado en reglas

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en. https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.
3. En la página Flujos de trabajo coincidentes, en la esquina superior derecha, selecciona Crear flujo de trabajo coincidente.
4. Para el paso 1: especificar los detalles del flujo de trabajo coincidentes, haga lo siguiente:
   a. Introduzca un nombre de flujo de trabajo coincidente y una descripción opcional.
   b. Para la entrada de datos, elija una AWS Glue base de datos del menú desplegable, seleccione la AWS Glue tabla y, a continuación, el mapeo de esquema correspondiente.

      Puede añadir hasta 19 entradas de datos.
   c. La opción Normalizar datos está seleccionada de forma predeterminada, de modo que las entradas de datos se normalizan antes de que coincidan. Si no desea normalizar los datos, deseleccione la opción Normalizar datos.

      > **Note**
      >
      > La normalización solo se admite en los siguientes escenarios en Crear mapeo de esquemas:
      >
      > - Si se agrupan los siguientes subtipos de nombres: nombre, segundo nombre, apellido.
      > - Si se agrupan los siguientes subtipos de direcciones: dirección 1, dirección 2, dirección 3, ciudad, estado, país, código postal.

- Si los siguientes subtipos de teléfono están agrupados: número de teléfono, código de país del teléfono.

d. Para especificar los permisos de acceso al servicio, elija una opción y lleve a cabo la acción recomendada.

Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-matching-workflow-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.

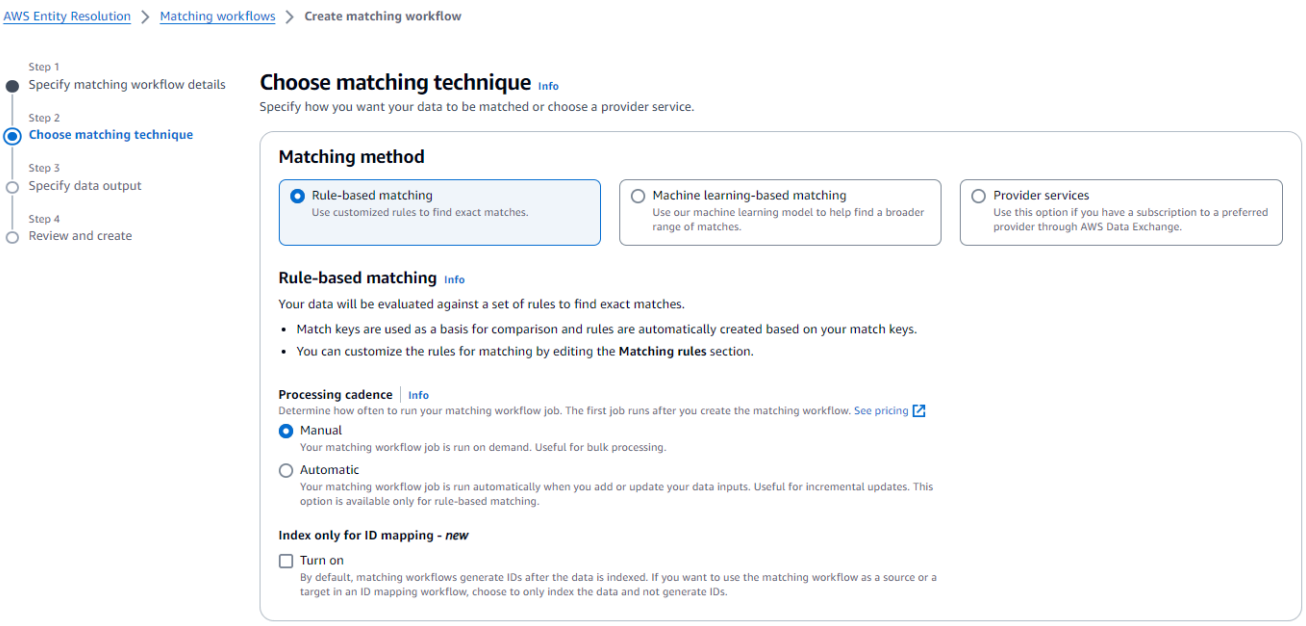
Opción	Acción recomendada
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

e. (Opcional) Para habilitar las etiquetas para el recurso, selecciona Añadir nueva etiqueta y, a continuación, introduce el par clave y valor.

f. Elija Siguiente.

5. Para el paso 2: elija una técnica de coincidencia:

   a. Para el método de coincidencia, elija la coincidencia basada en reglas.



b. En Cadencia de procesamiento, selecciona una de las siguientes opciones:

- Seleccione Manual para ejecutar un flujo de trabajo bajo demanda para una actualización masiva
- Elija Automático para ejecutar un flujo de trabajo en cuanto haya nuevos datos en su bucket de S3

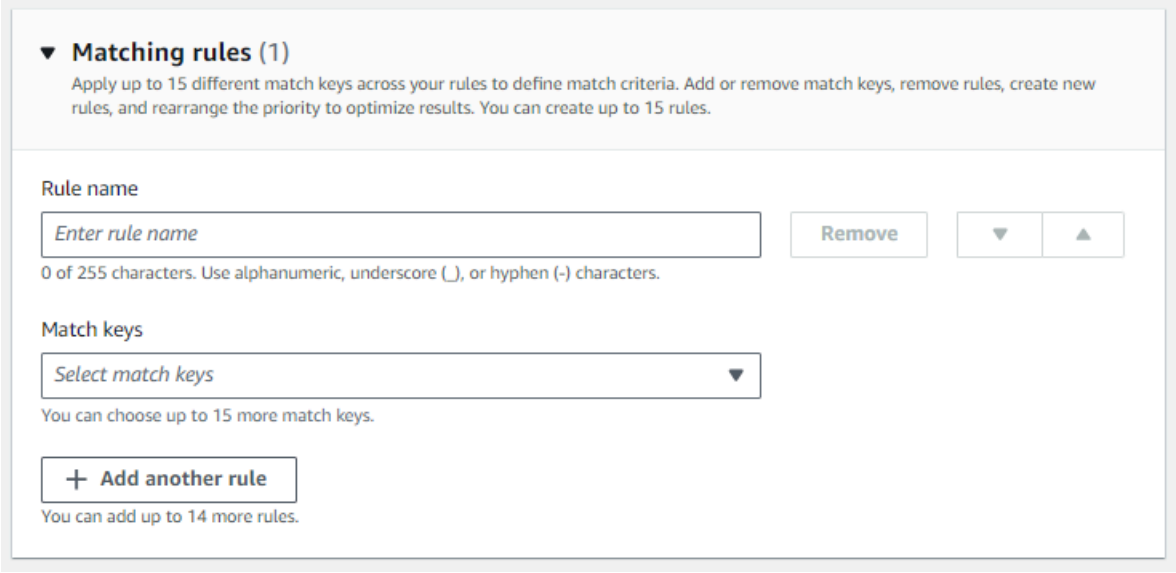
> **Note**
>
> Si eliges Automático, asegúrate de tener activadas EventBridge las notificaciones de Amazon para tu bucket de S3. Para obtener instrucciones sobre cómo habilitar Amazon EventBridge mediante la consola S3, consulte Habilitar Amazon EventBridge en la Guía del usuario de Amazon S3.

c. (Opcional) Seleccione Activar solo para el mapeo de ID si desea utilizar el flujo de trabajo coincidente como origen o destino en un flujo de trabajo de mapeo de ID. AWS Entity Resolution solo indexará los datos y no los generará IDs.

   De forma predeterminada, los flujos de trabajo coincidentes se generan IDs después de indexar los datos.

d. En Reglas de coincidencia, introduzca un nombre de regla y, a continuación, elija las claves de coincidencia para esa regla.

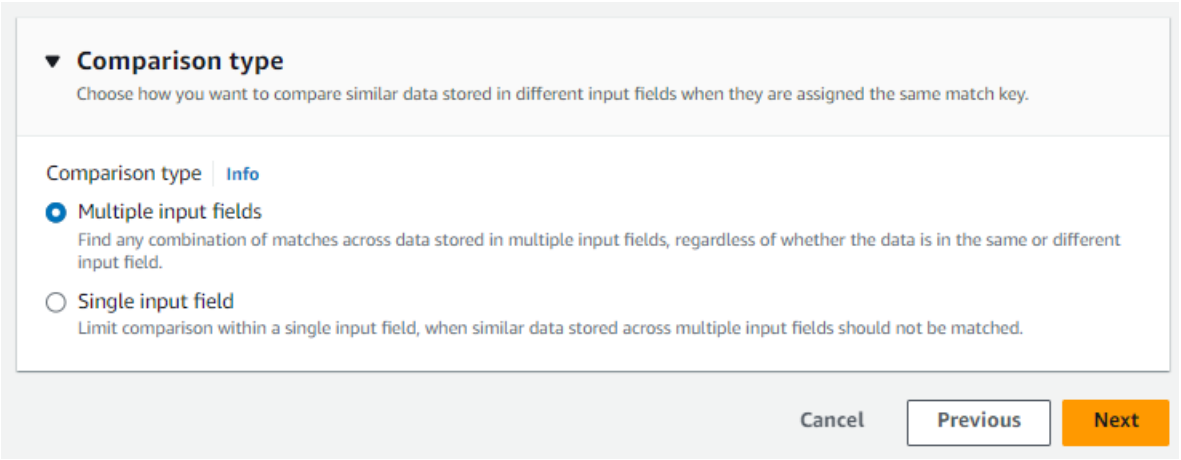
Puede crear hasta 15 reglas y aplicar hasta 15 claves de coincidencia diferentes a sus reglas para definir los criterios de coincidencia.



e. Seleccione Añadir otra regla para crear reglas adicionales según sea necesario.

f. En Tipo de comparación, seleccione una de las siguientes opciones:

- Seleccione Varios campos de entrada para buscar cualquier combinación de coincidencias entre los datos almacenados en varios campos de entrada.
- Elija Campo de entrada único para limitar la comparación a un solo campo de entrada.



g. Elija Siguiente.

6. Para el paso 3: especifique la salida y el formato de los datos:

a. En Destino y formato de salida de datos, elija la ubicación de Amazon S3 para la salida de datos y si el formato de datos será Datos normalizados o Datos originales.

b. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN.

c. Vea la salida generada por el sistema.

d. Para la salida de datos, decida qué campos desea incluir, ocultar o enmascarar y, a continuación, seleccione una de las siguientes opciones:

- Mantenga el estado de salida como Incluido para incluir campos.
- Elija el campo de salida y, a continuación, elija Ocultar para ocultar los campos (excluirlos de la salida)
- Elija el campo de salida y, a continuación, elija la salida Hash para enmascarar los campos.
- Seleccione Restablecer para restablecer la configuración anterior.

e. Elija Siguiente.

7. Para el paso 4: Revisa y crea:

a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

b. Elija Create and run.

Aparece un mensaje que indica que se ha creado el flujo de trabajo correspondiente y que el trabajo ha comenzado.

8. En la página de detalles del flujo de trabajo coincidente, en la pestaña Métricas, consulta lo siguiente en Métricas del último trabajo:

- El identificador del trabajo.
- El estado del trabajo de flujo de trabajo coincidente: en cola, en curso, completado, fallido
- El tiempo de finalización del trabajo de flujo de trabajo.
- El número de registros procesados.
- El número de registros no procesados.
- La coincidencia única IDs generada.
- El número de registros de entrada.

También puede ver las métricas de trabajo para hacer coincidir los trabajos de flujo de trabajo que se han ejecutado anteriormente en el historial de trabajos.

9. Cuando se complete el trabajo del flujo de trabajo correspondiente (el estado es Completado), puede ir a la pestaña Salida de datos y, a continuación, seleccionar su ubicación de Amazon S3 para ver los resultados.
10. (Solo tipo de procesamiento manual) Si ha creado un flujo de trabajo coincidente basado en reglas con el tipo de procesamiento manual, puede ejecutar el flujo de trabajo coincidente en cualquier momento seleccionando Ejecutar flujo de trabajo en la página de detalles del flujo de trabajo coincidente.

Crear un flujo de trabajo coincidente basado en el aprendizaje automático

El emparejamiento basado en el aprendizaje automático es un proceso preestablecido que intenta hacer coincidir los registros de todos los datos que ingresas. El flujo de trabajo de búsqueda de coincidencias basado en el aprendizaje automático le permite comparar datos de texto claro para encontrar una amplia gama de coincidencias mediante un modelo de aprendizaje automático.

> **Note**
>
> El modelo de aprendizaje automático no admite la comparación de datos cifrados.

Cuando AWS Entity Resolution encuentra una coincidencia entre dos o más registros de los datos, asigna:

- Un identificador de coincidencia para los registros del conjunto de datos coincidente
- El porcentaje del nivel de confianza de las coincidencias.

Puede utilizar el resultado de un flujo de trabajo de coincidencia basado en ML como entrada para la búsqueda de proveedores de servicios de datos, o viceversa, para cumplir sus objetivos específicos. Por ejemplo, puede ejecutar una búsqueda basada en ML para buscar primero coincidencias entre sus fuentes de datos en sus propios registros. Si un subconjunto no coincide, puede ejecutar la búsqueda de coincidencias basada en los servicios del proveedor para buscar más coincidencias.

Para crear un flujo de trabajo coincidente basado en ML:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.
3. En la página Flujos de trabajo coincidentes, en la esquina superior derecha, selecciona Crear flujo de trabajo coincidente.
4. Para el paso 1: especificar los detalles del flujo de trabajo coincidentes, haga lo siguiente:

   a. Introduzca un nombre de flujo de trabajo coincidente y una descripción opcional.

   b. Para la entrada de datos, elija una AWS Glue base de datos del menú desplegable, seleccione la AWS Glue tabla y, a continuación, el mapeo de esquema correspondiente.

      Puede añadir hasta 20 entradas de datos.

   c. La opción Normalizar datos está seleccionada de forma predeterminada, de modo que las entradas de datos se normalizan antes de que coincidan. Si no desea normalizar los datos, deseleccione la opción Normalizar datos.

      La coincidencia basada en el aprendizaje automático solo normalizaNombre, y. Teléfono Correo electrónico

   d. Para especificar los permisos de acceso al servicio, elija una opción y tome las medidas recomendadas.

Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-matching-workflow-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se

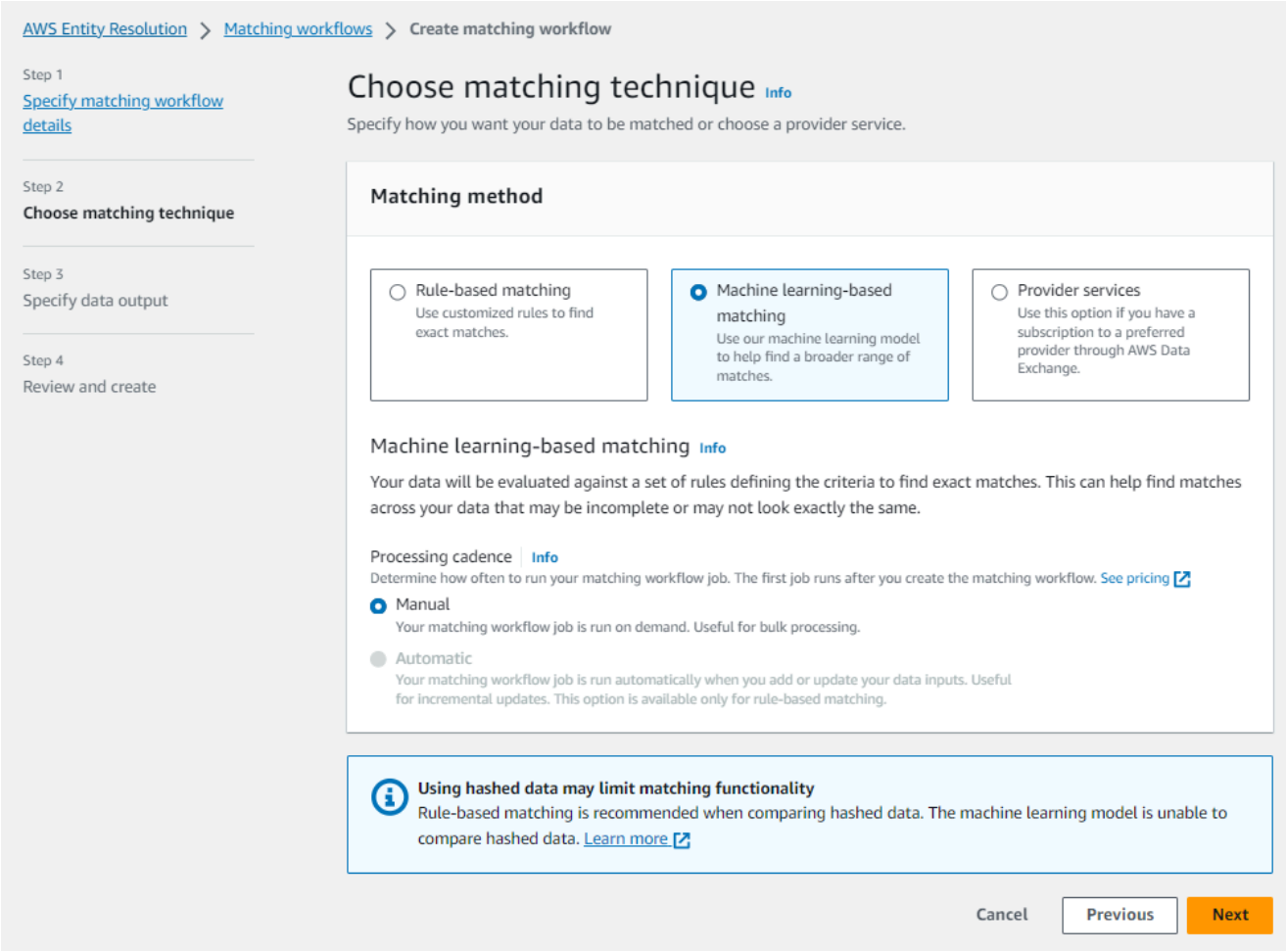
Opción	Acción recomendada
	cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

e. (Opcional) Para habilitar las etiquetas para el recurso, selecciona Añadir nueva etiqueta y, a continuación, introduce el par clave y valor.

f. Elija Siguiente.

5. Para el paso 2: elija una técnica de coincidencia:

   a. Para el método de emparejamiento, elija el emparejamiento basado en el aprendizaje automático.



b. En Cadencia de procesamiento, se selecciona la opción Manual.

   Esta opción le permite ejecutar un flujo de trabajo bajo demanda para realizar una actualización masiva.

> **Note**
>
> El procesamiento automático (incremental) no es compatible con los flujos de trabajo coincidentes basados en el aprendizaje automático.

c. Elija Siguiente.

6. Para el paso 3: especifique la salida y el formato de los datos:

   a. En Destino y formato de salida de datos, elija la ubicación de Amazon S3 para la salida de datos y si el formato de datos será Datos normalizados o Datos originales.

b. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN.

c. Vea la salida generada por el sistema.

d. En el caso de la salida de datos, decide qué campos quieres incluir, ocultar o enmascarar y, a continuación, realiza las acciones recomendadas en función de tus objetivos.

Su objetivo	Opción recomendada
Incluya campos	Mantenga el estado de salida como Incluido.
Ocultar campos (excluirlos de la salida)	Elija el campo de salida y, a continuación, elija Ocultar.
Enmascarar campos	Elija el campo de salida y, a continuación, elija Salida de hash.
Restablece los ajustes anteriores	Elija Restablecer.

e. Elija Siguiente.

7. Para el paso 4: Revisa y crea:

a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

b. Elija Create and run.

Aparece un mensaje que indica que se ha creado el flujo de trabajo correspondiente y que el trabajo ha comenzado.

8. En la página de detalles del flujo de trabajo coincidente, en la pestaña Métricas, consulta lo siguiente en Métricas del último trabajo:

- El identificador del trabajo.
- El estado del trabajo de flujo de trabajo coincidente: en cola, en curso, completado, fallido
- El tiempo de finalización del trabajo de flujo de trabajo.
- El número de registros procesados.
- El número de registros no procesados.
- La coincidencia única IDs generada.

- El número de registros de entrada.

También puede ver las métricas de trabajo para hacer coincidir los trabajos de flujo de trabajo que se han ejecutado anteriormente en el historial de trabajos.

9. Cuando se complete el trabajo del flujo de trabajo correspondiente (el estado es Completado), puede ir a la pestaña Salida de datos y, a continuación, seleccionar su ubicación de Amazon S3 para ver los resultados.
10. (Solo tipo de procesamiento manual) Si ha creado un flujo de trabajo coincidente basado en el aprendizaje automático con el tipo de procesamiento manual, puede ejecutar el flujo de trabajo coincidente en cualquier momento seleccionando Ejecutar flujo de trabajo en la página de detalles del flujo de trabajo coincidente.

Crear un flujo de trabajo coincidente basado en los servicios del proveedor

La coincidencia basada en los servicios de los proveedores le permite hacer coincidir sus identificadores conocidos con los de su proveedor de servicios de datos preferido.

AWS Entity Resolution actualmente admite los siguientes servicios de proveedores de datos:

- LiveRamp
- TransUnion
- ID unificada 2.0

Para obtener más información sobre los servicios de proveedores compatibles, consultePreparar los datos de entrada de terceros.

Puede utilizar una suscripción pública para estos proveedores AWS Data Exchange o negociar una oferta privada directamente con el proveedor de datos. Para obtener más información sobre cómo crear una nueva suscripción o reutilizar una suscripción existente a un servicio de un proveedor, consultePaso 1: Suscríbase a un servicio de proveedor en AWS Data Exchange.

En las siguientes secciones se describe cómo crear un flujo de trabajo coincidente basado en el proveedor.

Temas

- Crear un flujo de trabajo coincidente con LiveRamp
- Crear un flujo de trabajo coincidente con TransUnion
- Crear un flujo de trabajo coincidente con UID 2.0

Crear un flujo de trabajo coincidente con LiveRamp

Si tiene una suscripción al LiveRamp servicio, puede crear un flujo de trabajo que coincida con el LiveRamp servicio para realizar la resolución de identidad.

El LiveRamp servicio proporciona un identificador denominado RampID. El RampID es uno de los más utilizados IDs en las plataformas orientadas a la demanda para crear una audiencia para una campaña publicitaria. Si utilizas un flujo de trabajo coincidente con LiveRamp, puedes resolver direcciones de correo electrónico cifradas en. RAMPIDs

> **Note**
>
> AWS Entity Resolution admite la asignación de RampID basada en PII.

Este flujo de trabajo requiere un depósito de almacenamiento provisional de datos de Amazon S3 en el que desee que se escriba temporalmente la salida del flujo de trabajo coincidente. Antes de crear un flujo de trabajo de mapeo de ID con LiveRamp, añada los siguientes permisos al depósito de almacenamiento provisional de datos.

JSON

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

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

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

Reemplace cada *<user input placeholder>* por su propia información.

staging-bucket	Depósito de Amazon S3 que almacena temporalmente sus datos mientras ejecuta un flujo de trabajo basado en los servicios del proveedor.

Para crear un flujo de trabajo coincidente con LiveRamp:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.

3. En la página Flujos de trabajo coincidentes, en la esquina superior derecha, selecciona Crear flujo de trabajo coincidente.
4. Para el paso 1: especificar los detalles del flujo de trabajo coincidentes, haga lo siguiente:

   a. Introduzca un nombre de flujo de trabajo coincidente y una descripción opcional.

   b. Para la entrada de datos, elija una AWS Glue base de datos del menú desplegable, seleccione la AWS Glue tabla y, a continuación, seleccione el mapeo de esquema correspondiente.

      Puede añadir hasta 20 entradas de datos.

   c. La opción Normalizar datos está seleccionada de forma predeterminada, de modo que las entradas de datos se normalizan antes de que coincidan.

      > **Note**
      >
      > La normalización solo se admite en los siguientes escenarios en Crear mapeo de esquemas:
      >
      > - Si se agrupan los siguientes subtipos de nombres: nombre, segundo nombre, apellido.
      > - Si se agrupan los siguientes subtipos de direcciones: dirección 1, dirección 2: nombre de la dirección 3, nombre, nombre de la ciudad, estado, país, código postal.
      > - Si los siguientes subtipos de teléfono están agrupados: número de teléfono, código de país del teléfono.

      Si está utilizando el proceso de resolución solo por correo electrónico, deseleccione la opción Normalizar datos, ya que solo se utilizan correos electrónicos cifrados para introducir datos.

   d. Para especificar los permisos de acceso al servicio, elige una opción y realiza las acciones recomendadas.

Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-matching-workflow-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.

Opción	Acción recomendada
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

e. (Opcional) Para habilitar las etiquetas para el recurso, selecciona Añadir nueva etiqueta y, a continuación, introduce el par clave y valor.

f. Elija Siguiente.

5. Para el paso 2: elija una técnica de coincidencia:

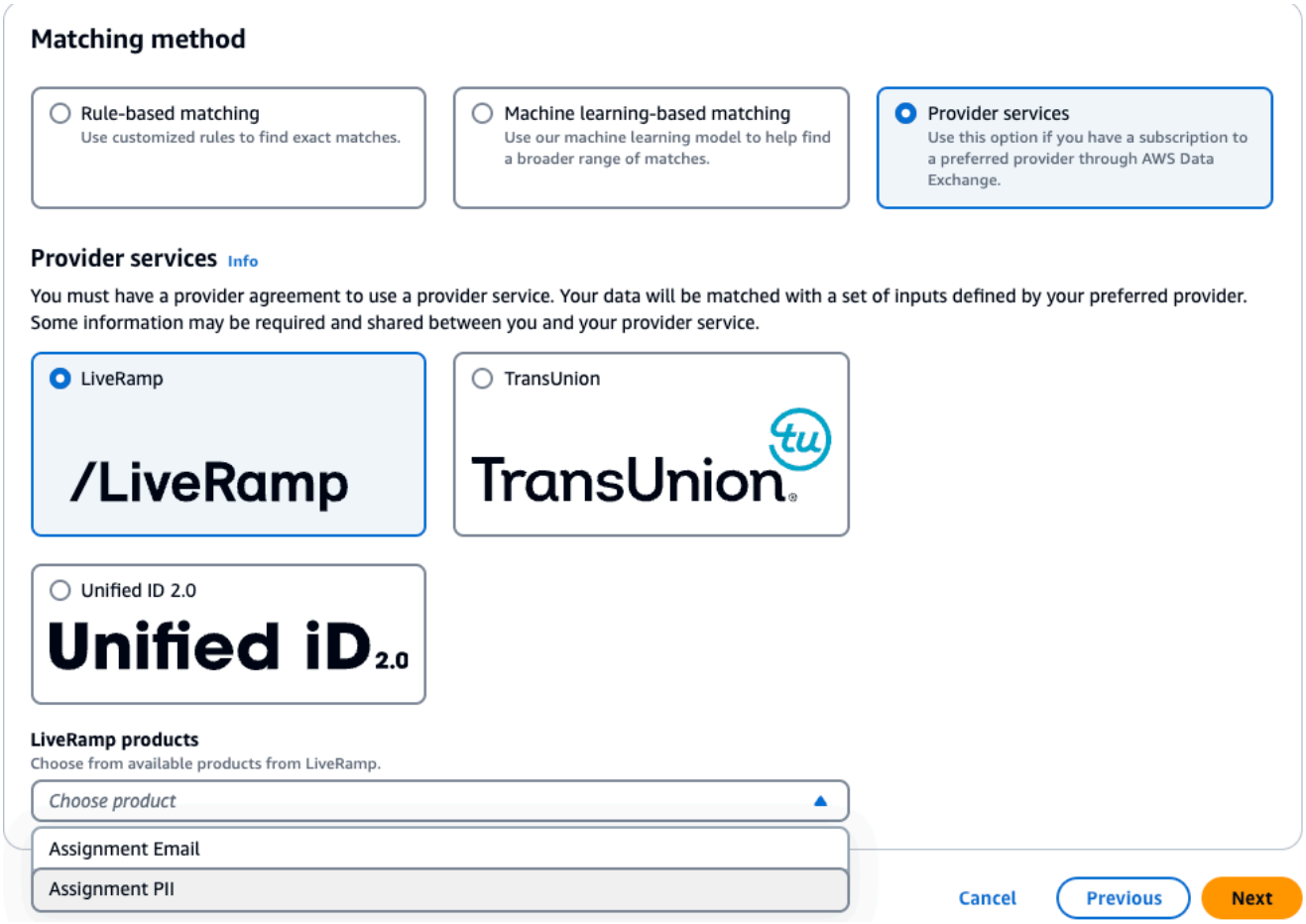
a. Para el método de coincidencia, elija Servicios del proveedor.

b. Para los servicios de proveedores, elija LiveRamp.

> **Note**
>
> Asegúrese de que el formato y la normalización del archivo de entrada de datos estén alineados con las directrices del servicio del proveedor.

Para obtener más información sobre las pautas de formato de los archivos de entrada para el flujo de trabajo correspondiente, consulte Realizar la resolución de identidad mediante ADX en la LiveRamp documentación.

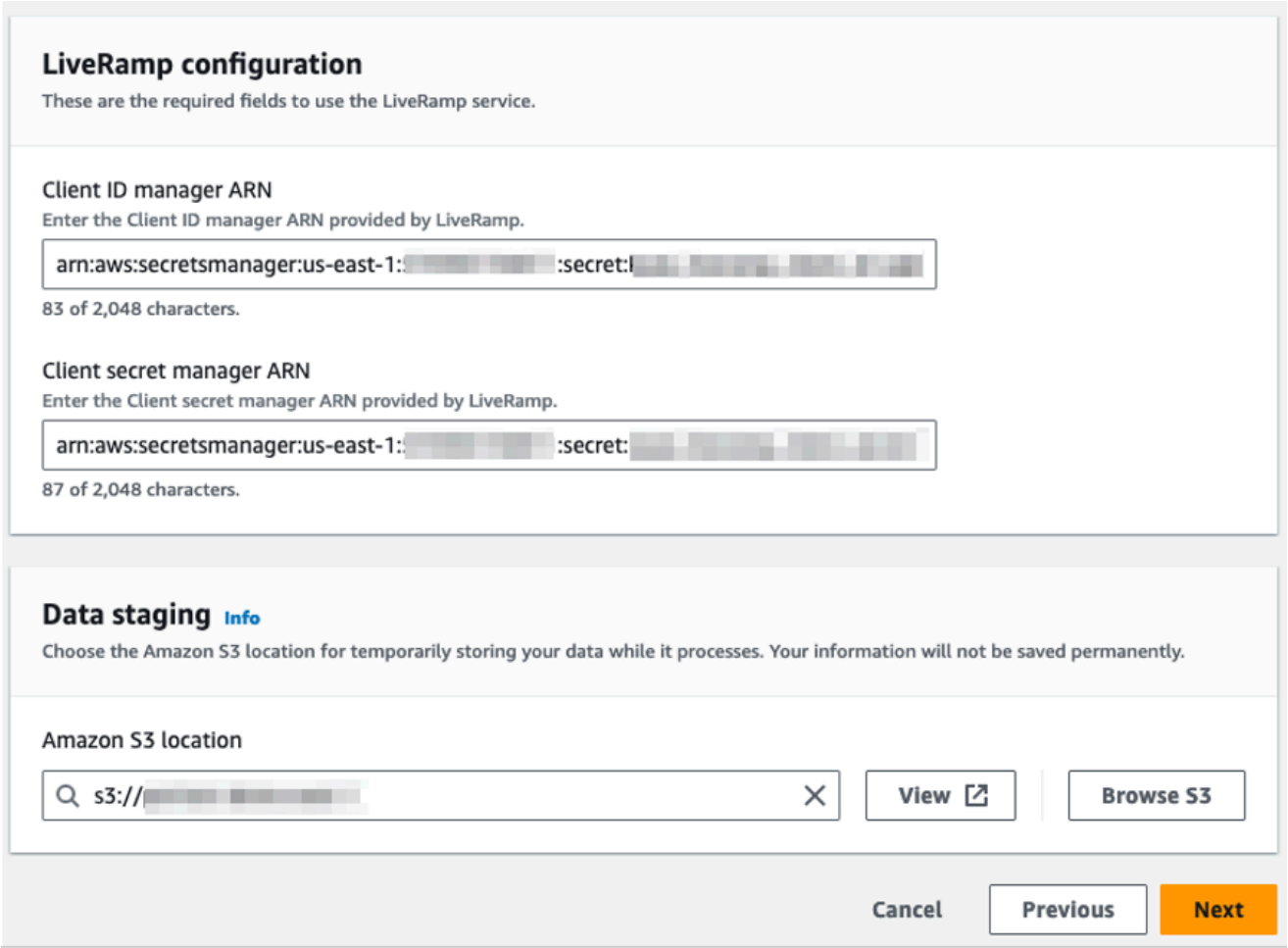
c. Para LiveRamp los productos, elige un producto de la lista desplegable.



Note

Si elige la PII de asignación, debe proporcionar al menos una columna que no sea de identificación al realizar la resolución de la entidad. Por ejemplo, GÉNERO.

d. Para LiveRamp la configuración, introduzca un ARN de administrador de ID de cliente y un ARN de administrador de secretos de cliente.



e. Para la organización de datos, elija la ubicación de Amazon S3 para el almacenamiento temporal de los datos mientras se procesan.

   Debe tener permiso para acceder a la ubicación de almacenamiento de datos de Amazon S3. Para obtener más información, consulte Crear un rol de trabajo de flujo de trabajo para AWS Entity Resolution.

f. Elija Siguiente.

6. Para el paso 3: especifique la salida de datos:

   a. En Destino y formato de salida de datos, elija la ubicación de Amazon S3 para la salida de datos y si el formato de datos será Datos normalizados o Datos originales.

   b. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN.

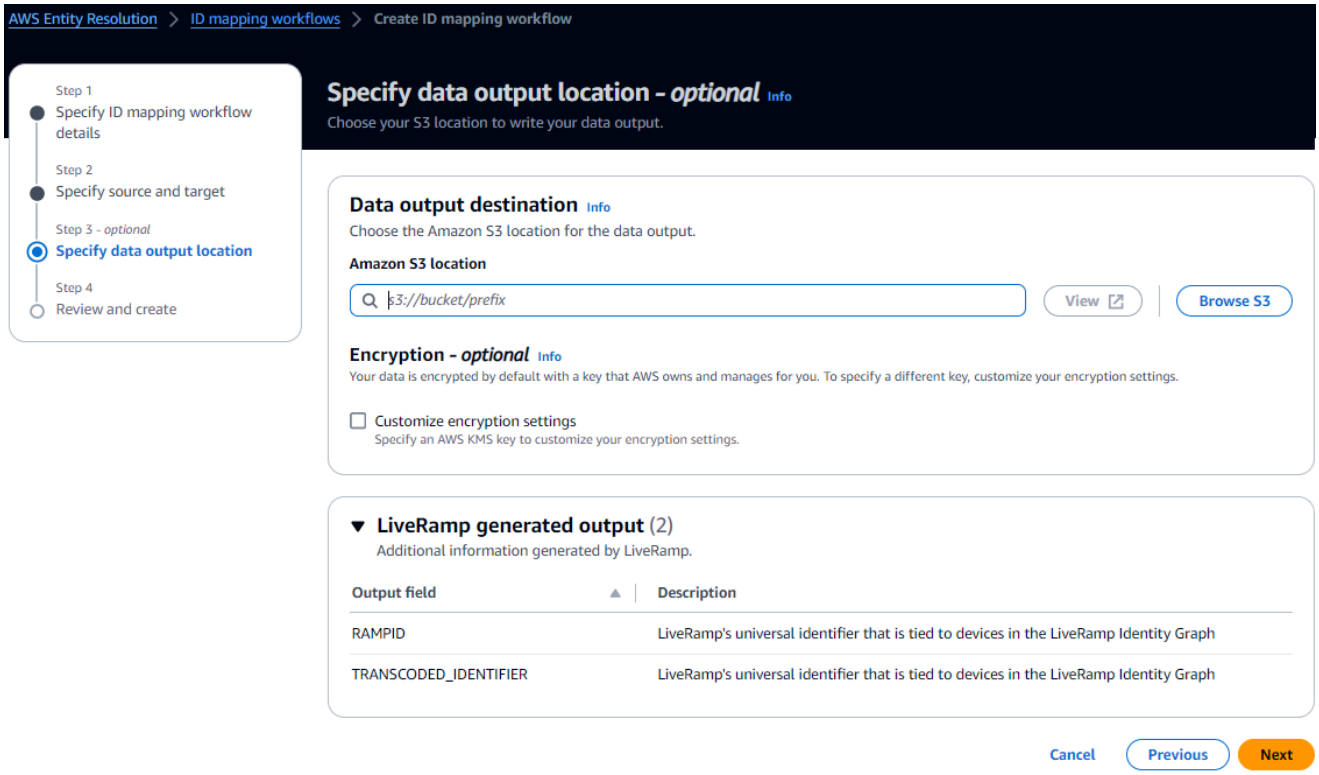
   c. Vea la salida LiveRamp generada.

      Esta es la información adicional generada por LiveRamp.

d. En el caso de la salida de datos, decide qué campos quieres incluir, ocultar o enmascarar y, a continuación, realiza las acciones recomendadas en función de tus objetivos.

> **Note**
>
> Si lo ha elegido LiveRamp, debido a los filtros de LiveRamp privacidad que eliminan la información de identificación personal (PII), algunos campos mostrarán el estado de salida No disponible.

Su objetivo	Opción recomendada
Incluya campos	Mantenga el estado de salida como Incluido.
Ocultar campos (excluirlos de la salida)	Elija el campo de salida y, a continuación, elija Ocultar.
Enmascarar campos	Elija el campo de salida y, a continuación, elija Salida de hash.
Restablece los ajustes anteriores	Elija Restablecer.



e. Elija Siguiente.

7. Para el paso 4: revise y cree:

   a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

   b. Elija Create and run.

      Aparece un mensaje que indica que se ha creado el flujo de trabajo correspondiente y que el trabajo ha comenzado.

8. En la página de detalles del flujo de trabajo coincidente, en la pestaña Métricas, consulta lo siguiente en Métricas del último trabajo:

   - El identificador del trabajo.
   - El estado del trabajo de flujo de trabajo coincidente: en cola, en curso, completado, fallido
   - El tiempo de finalización del trabajo de flujo de trabajo.
   - El número de registros procesados.
   - El número de registros no procesados.
   - La coincidencia única IDs generada.
   - El número de registros de entrada.

También puede ver las métricas de trabajo para hacer coincidir los trabajos de flujo de trabajo que se han ejecutado anteriormente en el historial de trabajos.

9. Cuando se complete el trabajo del flujo de trabajo correspondiente (el estado es Completado), puede ir a la pestaña Salida de datos y, a continuación, seleccionar su ubicación de Amazon S3 para ver los resultados.

Crear un flujo de trabajo coincidente con TransUnion

Si tiene una suscripción al TransUnion servicio, puede mejorar la comprensión de los clientes al vincular, comparar y mejorar los registros relacionados con los clientes almacenados en distintos canales con las claves electrónicas de TransUnion personas y hogares y más de 200 atributos de datos.

El TransUnion servicio proporciona identificadores conocidos como persona y hogar. TransUnion IDs TransUnion proporciona la asignación de ID (también conocida como codificación) de identificadores conocidos, como el nombre, la dirección, el número de teléfono y la dirección de correo electrónico.

Este flujo de trabajo requiere un depósito de almacenamiento provisional de datos de Amazon S3 en el que desee que se escriba temporalmente la salida del flujo de trabajo coincidente. Antes de crear un flujo de trabajo coincidente con TransUnion, añada los siguientes permisos al depósito de almacenamiento provisional de datos.

JSON

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

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

```
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket>",
                "arn:aws:s3:::<staging-bucket>/*"
            ]
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::381491956555:root"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl"
            ],
            "Resource": [
                "arn:aws:s3:::<staging-bucket>",
                "arn:aws:s3:::<staging-bucket>/*"
            ]
        }
    ]
}
```

Reemplace cada *<user input placeholder>* por su propia información.

staging-bucket	Depósito de Amazon S3 que almacena temporalmente sus datos mientras ejecuta un flujo de trabajo basado en los servicios del proveedor.

Para crear un flujo de trabajo coincidente con TransUnion:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.

3. En la página Flujos de trabajo coincidentes, en la esquina superior derecha, selecciona Crear flujo de trabajo coincidente.
4. Para el paso 1: especificar los detalles del flujo de trabajo coincidentes, haga lo siguiente:

   a. Introduzca un nombre de flujo de trabajo coincidente y una descripción opcional.

   b. Para la entrada de datos, elija una AWS Glue base de datos del menú desplegable, seleccione la AWS Glue tabla y, a continuación, seleccione el mapeo de esquema correspondiente.

      Puede añadir hasta 20 entradas de datos.

   c. La opción Normalizar datos está seleccionada de forma predeterminada, de modo que las entradas de datos se normalizan antes de que coincidan. Si no desea normalizar los datos, deseleccione la opción Normalizar datos.

      > **Note**
      >
      > La normalización solo se admite en los siguientes escenarios en Crear mapeo de esquemas:
      >
      > - Si se agrupan los siguientes subtipos de nombres: nombre, segundo nombre, apellido.
      > - Si se agrupan los siguientes subtipos de direcciones: dirección 1, dirección 2: nombre de la dirección 3, nombre, nombre de la ciudad, estado, país, código postal.
      > - Si los siguientes subtipos de teléfono están agrupados: número de teléfono, código de país del teléfono.

   d. Para especificar los permisos de acceso al servicio, elija una opción y lleve a cabo la acción recomendada.

Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-m`

Opción	Acción recomendada
	`atching-workflow-<timestamp > .` • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

e. (Opcional) Para habilitar las etiquetas para el recurso, selecciona Añadir nueva etiqueta y, a continuación, introduce el par clave y valor.

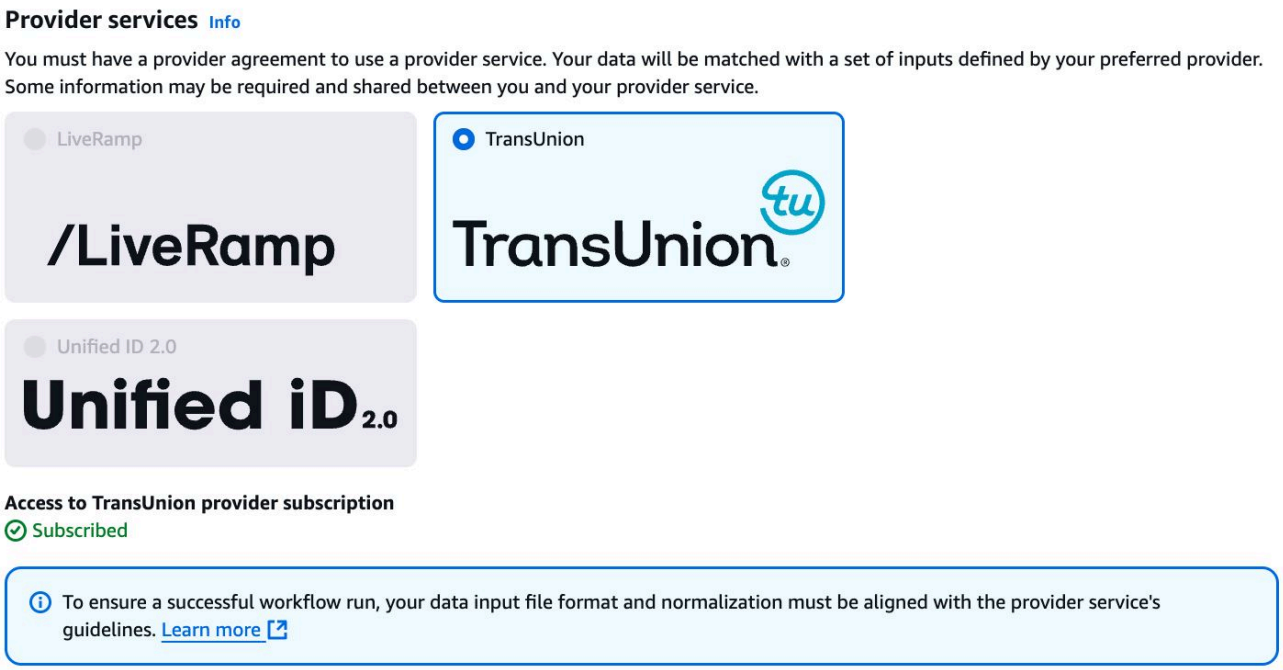
f. Elija Siguiente.

5. Para el paso 2: elija una técnica de coincidencia:

a. Para el método de coincidencia, elija Servicios del proveedor.

b. Para los servicios de proveedores, elija TransUnion.

> **Note**
>
> Asegúrese de que el formato y la normalización del archivo de entrada de datos estén alineados con las directrices del servicio del proveedor.



c. Para la organización de datos, elija la ubicación de Amazon S3 para el almacenamiento temporal de los datos mientras se procesan.

   Debe tener permiso para acceder a la ubicación de almacenamiento de datos de Amazon S3. Para obtener más información, consulte the section called “Crear un rol de trabajo de flujo de trabajo”.

6. Elija Siguiente.

7. Para el paso 3: especifique la salida de datos:

   a. En Destino y formato de salida de datos, elija la ubicación de Amazon S3 para la salida de datos y si el formato de datos será Datos normalizados o Datos originales.

b. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN.

c. Vea la salida TransUnion generada.

   Esta es la información adicional generada por TransUnion.

d. En el caso de la salida de datos, decide qué campos quieres incluir, ocultar o enmascarar y, a continuación, realiza las acciones recomendadas en función de tus objetivos.

Su objetivo	Opción recomendada
Incluya campos	Mantenga el estado de salida como Incluido.
Ocultar campos (excluirlos de la salida)	Elija el campo de salida y, a continuación, elija Ocultar.
Enmascarar campos	Elija el campo de salida y, a continuación, elija Salida de hash.
Restablece los ajustes anteriores	Elija Restablecer.

e. En la salida generada por el sistema, consulte todos los campos incluidos.

f. Elija Siguiente.

8. Para el paso 4: revise y cree:

   a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

   b. Elija Create and run.

      Aparece un mensaje que indica que se ha creado el flujo de trabajo correspondiente y que el trabajo ha comenzado.

9. En la página de detalles del flujo de trabajo coincidente, en la pestaña Métricas, consulta lo siguiente en Métricas del último trabajo:

   - El identificador del trabajo.
   - El estado del trabajo de flujo de trabajo coincidente: en cola, en curso, completado, fallido
   - El tiempo de finalización del trabajo de flujo de trabajo.
   - El número de registros procesados.

- El número de registros no procesados.
- La coincidencia única IDs generada.
- El número de registros de entrada.

También puede ver las métricas de trabajo para hacer coincidir los trabajos de flujo de trabajo que se han ejecutado anteriormente en el historial de trabajos.

10. Cuando se complete el trabajo del flujo de trabajo correspondiente (el estado es Completado), puede ir a la pestaña Salida de datos y, a continuación, seleccionar su ubicación de Amazon S3 para ver los resultados.

Crear un flujo de trabajo coincidente con UID 2.0

Si tiene una suscripción al servicio Unified ID 2.0, puede activar campañas publicitarias con una identidad determinista y aprovechar la interoperabilidad con muchos participantes UID2 habilitados en todo el ecosistema publicitario. Para obtener más información, consulte Descripción general de Unified ID 2.0.

El servicio Unified ID 2.0 proporciona un UID 2 sin procesar, que se utiliza para crear campañas publicitarias en la plataforma The Trade Desk. El UID 2.0 se genera utilizando un marco de código abierto.

En un flujo de trabajo, puede usar uno **`Email Address`** o **`Phone number`** para la UID2 generación sin procesar, pero no ambos. Si ambos están presentes en el mapeo del esquema, el flujo de trabajo seleccionará el campo **`Email Address`** y **`Phone number`** será un campo de transferencia. Para admitir ambos, cree un nuevo esquema de mapeo donde **`Phone number`** esté mapeado pero **`Email Address`** no esté mapeado. A continuación, cree un segundo flujo de trabajo con este nuevo mapeo de esquemas.

> **Note**
>
> UID2s Las sales crudas se crean añadiendo sales de cubos de sal que se giran aproximadamente una vez al año, lo que hace que la materia prima UID2 también se rote con ella. Por lo tanto, se recomienda refrescar el crudo a diario. UID2s Para obtener más información, consulte https://unifiedid.com/docs/how-often-should-uidgetting-started/gs-faqs# 2 -incremental-updates. s-be-refreshed-for

Para crear un flujo de trabajo coincidente con UID 2.0:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.
3. En la página Flujos de trabajo coincidentes, en la esquina superior derecha, selecciona Crear flujo de trabajo coincidente.
4. Para el paso 1: especificar los detalles del flujo de trabajo coincidentes, haga lo siguiente:

   a. Introduzca un nombre de flujo de trabajo coincidente y una descripción opcional.

   b. Para la entrada de datos, elija una AWS Glue base de datos del menú desplegable, seleccione la AWS Glue tabla y, a continuación, seleccione el mapeo de esquema correspondiente.

      Puede añadir hasta 20 entradas de datos.

   c. Deje seleccionada la opción Normalizar datos para que las entradas (**`Email Address`**o**`Phone number`**) de datos se normalicen antes de coincidir.

      Para obtener más información sobre **`Email Address`** la normalización, consulte Normalización de direcciones de correo electrónico en la documentación del UID 2.0.

      Para obtener más información sobre **`Phone number`** la normalización, consulte Normalización de números de teléfono en la documentación del UID 2.0.

   d. Para especificar los permisos de acceso al servicio, elija una opción y lleve a cabo la acción recomendada.

Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-matching-workflow-<timestamp>` .

Opción	Acción recomendada
	• Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

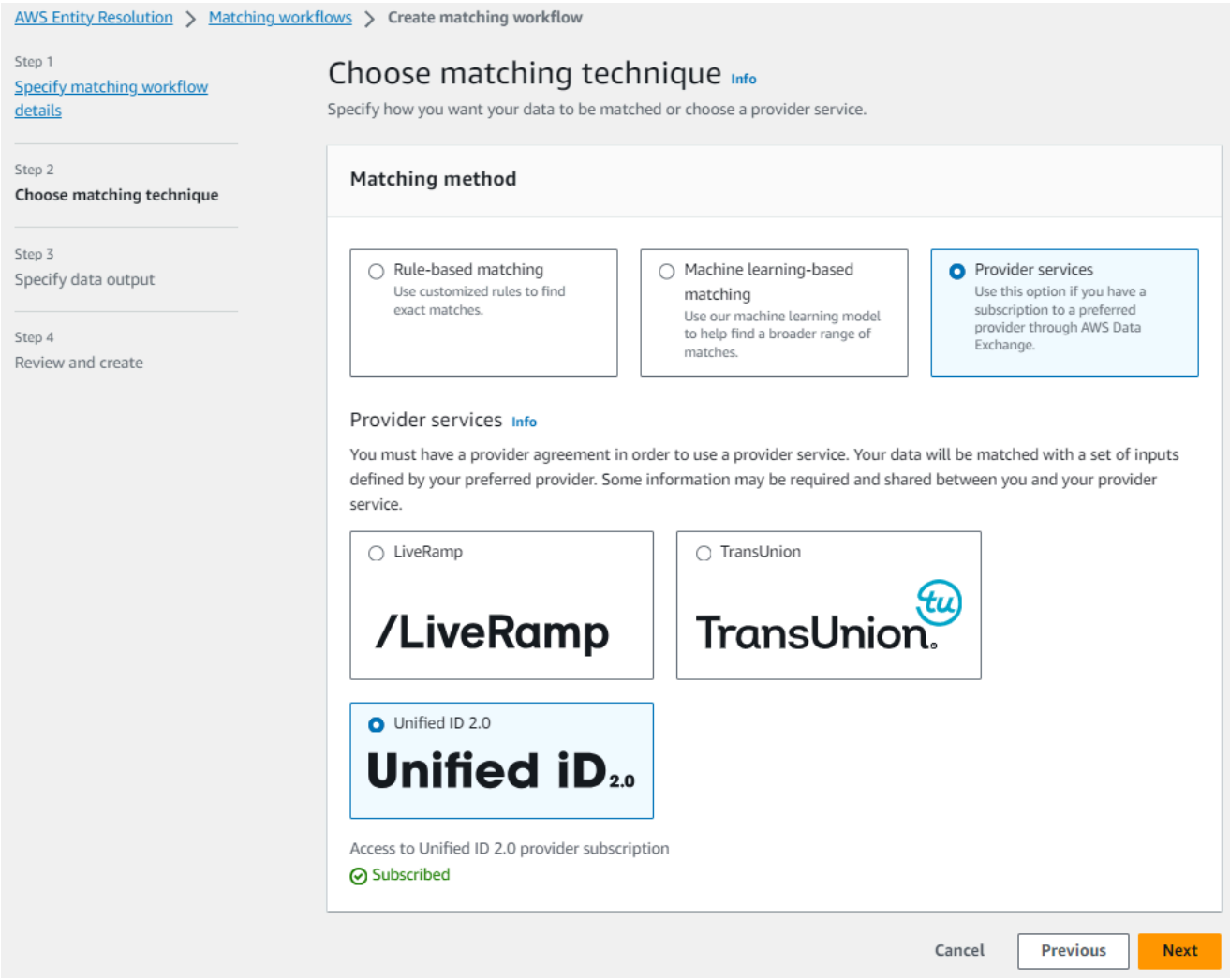
e. (Opcional) Para habilitar las etiquetas para el recurso, selecciona Añadir nueva etiqueta y, a continuación, introduce el par clave y valor.

f. Elija Siguiente.

5. Para el paso 2: elija una técnica de coincidencia:

a. Para el método de coincidencia, elija Servicios del proveedor.

b. Para los servicios de proveedores, elija Unified ID 2.0.



c. Elija Siguiente.

6. Para el paso 3: especifique la salida de datos:

a. En Destino y formato de salida de datos, elija la ubicación de Amazon S3 para la salida de datos y si el formato de datos será Datos normalizados o Datos originales.

b. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN.

c. Vea el resultado generado por Unified ID 2.0.

Esta es una lista de toda la información adicional generada por el UID 2.0

d. Para la salida de datos, decida qué campos quiere incluir, ocultar o enmascarar y, a continuación, tome las medidas recomendadas en función de sus objetivos.

Su objetivo	Opción recomendada
Incluya campos	Mantenga el estado de salida como Incluido.
Ocultar campos (excluirlos de la salida)	Elija el campo de salida y, a continuación, elija Ocultar.
Enmascarar campos	Elija el campo de salida y, a continuación, elija Salida de hash.
Restablece los ajustes anteriores	Elija Restablecer.

e. En la salida generada por el sistema, consulte todos los campos incluidos.

f. Elija Siguiente.

7. Para el paso 4: revise y cree:

   a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

   b. Elija Create and run.

      Aparece un mensaje que indica que se ha creado el flujo de trabajo correspondiente y que el trabajo ha comenzado.

8. En la página de detalles del flujo de trabajo coincidente, en la pestaña Métricas, consulta lo siguiente en Métricas del último trabajo:

   - El identificador del trabajo.
   - El estado del trabajo de flujo de trabajo coincidente: en cola, en curso, completado, fallido
   - El tiempo de finalización del trabajo de flujo de trabajo.
   - El número de registros procesados.
   - El número de registros no procesados.
   - La coincidencia única IDs generada.
   - El número de registros de entrada.

   También puede ver las métricas de trabajo para hacer coincidir los trabajos de flujo de trabajo que se han ejecutado anteriormente en el historial de trabajos.

9. Cuando se complete el trabajo del flujo de trabajo correspondiente (el estado es Completado), puede ir a la pestaña Salida de datos y, a continuación, seleccionar su ubicación de Amazon S3 para ver los resultados.

Edición de un flujo de trabajo coincidente

La edición del flujo de trabajo correspondiente le permite mantener sus procesos de resolución de entidades up-to-date y adaptarlos a los requisitos cambiantes de su organización a lo largo del tiempo. Es posible que desee ajustar los criterios, las técnicas o los resultados de datos coincidentes para mejorar la precisión y la eficiencia del proceso de resolución de entidades. Si identifica problemas o errores en los resultados del flujo de trabajo actual, editarlo puede ayudarle a diagnosticar y resolver esos problemas.

Para editar un flujo de trabajo coincidente:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.
3. Elija el flujo de trabajo correspondiente.
4. En la página de detalles del flujo de trabajo correspondiente, en la esquina superior derecha, selecciona Editar flujo de trabajo.
5. En la página Especificar los detalles del flujo de trabajo coincidentes, realice los cambios necesarios y, a continuación, seleccione Siguiente.
6. En la página Elegir una técnica coincidente, realice los cambios necesarios y, a continuación, seleccione Siguiente.

> **Important**
>
> Puede cambiar la cadencia de procesamiento de manual a automática, pero después de cambiarla a automática, no podrá volver a cambiarla a manual.
> Si la cadencia de procesamiento ya está configurada en Automática, no puedes cambiarla a Manual.

7. En la página Especificar la salida de datos, realice los cambios necesarios y, a continuación, seleccione Siguiente.

8. En la página Revisar y guardar, realice los cambios necesarios y, a continuación, seleccione Guardar.

Eliminar un flujo de trabajo coincidente

Si un flujo de trabajo coincidente ya no se utiliza o ha quedado obsoleto, eliminarlo puede ayudar a mantener el espacio de trabajo organizado y ordenado. Si has desarrollado un flujo de trabajo nuevo y mejorado que reemplaza a uno anterior, eliminar el flujo de trabajo anterior puede ayudarte a garantizar que solo utilizas la mayoría de los procesos. up-to-date

Para eliminar un flujo de trabajo coincidente:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.
3. Elija el flujo de trabajo correspondiente.
4. En la página de detalles del flujo de trabajo coincidente, en la esquina superior derecha, selecciona Eliminar.
5. Confirme la eliminación y luego elija Eliminar.

Modificar o generar un identificador de coincidencia para un flujo de trabajo coincidente basado en reglas

Un ID de coincidencia es el identificador generado AWS Entity Resolution y aplicado a cada conjunto de registros coincidentes después de ejecutar un flujo de trabajo coincidente. Esto forma parte de los metadatos coincidentes del flujo de trabajo que se incluyen en la salida.

Cuando necesites actualizar los registros de un cliente existente o añadir un cliente nuevo a tu conjunto de datos, puedes usar la AWS Entity Resolution consola o la `GenerateMatchID` API. La modificación de una ID de coincidencia existente ayuda a mantener la coherencia a la hora de actualizar la información del cliente, mientras que es necesario generar una nueva ID de coincidencia cuando se añaden al sistema clientes no identificados anteriormente.

> **Note**
>
> Se aplican cargos adicionales, ya sea que utilices la consola o la API. El tipo de procesamiento que elija afecta tanto a la precisión como al tiempo de respuesta de la operación.

> **Important**
>
> Si revoca AWS Entity Resolution los permisos de su bucket de S3 mientras hay un trabajo en curso, AWS Entity Resolution seguirá procesando y cobrando por enviar los resultados a S3, pero no podrá entregarlos a su bucket. Para evitar este problema, asegúrate de tener los AWS Entity Resolution permisos correctos para escribir en tu bucket de S3 antes de iniciar un trabajo. Si los permisos se revocan durante el procesamiento, AWS Entity Resolution intenta volver a entregar los resultados hasta 30 días después de haber completado el trabajo, una vez que hayas restablecido los permisos correctos del bucket.

El siguiente procedimiento le guiará por el proceso de buscar o generar un Match ID, seleccionar un tipo de procesamiento y ver los resultados.

Console

Para modificar o generar un identificador de coincidencia mediante la consola

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.
3. Elija el flujo de trabajo coincidente basado en reglas que se ha procesado (el estado del trabajo es Completado).
4. En la página de detalles del flujo de trabajo coincidente, seleccione la pestaña Coincidencia IDs.
5. Seleccione Modificar o generar el ID de coincidencia.

> **Note**
>
> La opción Modificar o generar el ID de coincidencia solo está disponible para los flujos de trabajo coincidentes que utilizan la cadencia de procesamiento automática. Si ha seleccionado la cadencia de procesamiento manual, esta opción aparecerá inactiva. Para usar esta opción, edite su flujo de trabajo para usar la cadencia de procesamiento automática. Para obtener más información sobre la edición de flujos de trabajo, consulteEdición de un flujo de trabajo coincidente.

6. Seleccione la AWS Glue tabla en la lista desplegable.

   Si solo hay una AWS Glue tabla en el flujo de trabajo, se selecciona de forma predeterminada.

7. Elija el tipo de procesamiento.

   - Coherente: puede buscar una ID de coincidencia existente o generar y guardar una nueva ID de coincidencia inmediatamente. Esta opción tiene la mayor precisión y el tiempo de respuesta más lento.
   - Antecedentes (se muestran como `EVENTUAL` en la API): puedes buscar un identificador de coincidencia existente o generar uno nuevo de forma inmediata. El registro actualizado se guarda en segundo plano. Esta opción tiene una respuesta inicial rápida, y los resultados completos estarán disponibles más adelante en S3.
   - Generación rápida de identificadores (se muestra como `EVENTUAL_NO_LOOKUP` en la API): puedes crear un nuevo identificador de coincidencia sin tener que buscar uno existente. El registro actualizado se guarda en segundo plano. Esta opción tiene la respuesta más rápida. Se recomienda solo para registros únicos.

8. Para los atributos de registro,

   a. Introduzca el valor del identificador único.

   b. Introduzca un valor para cada clave de coincidencia que coincida con los registros existentes en función de las reglas configuradas en su flujo de trabajo.

9. Elija Buscar ID de coincidencia y guarde el registro.

   Aparece un mensaje de confirmación que indica que se ha encontrado el identificador de coincidencia o que se ha generado un nuevo identificador de coincidencia y se ha guardado el registro.

10. Vea el identificador de coincidencia correspondiente y la regla asociada que se guardó en el flujo de trabajo coincidente en el mensaje de confirmación.
11. (Opcional) Para copiar el identificador de coincidencia, selecciona Copiar.

API

Para modificar o generar un identificador de coincidencia mediante la API

> **Note**
>
> Para llamar a esta API correctamente, primero debe haber ejecutado correctamente un flujo de trabajo de coincidencia basado en reglas mediante la StartMatchingJob API. Para obtener una lista completa de los lenguajes de programación compatibles, consulta la sección Vea también del GenerateMatch ID.

1. Abre un terminal o una línea de comandos para realizar la solicitud a la API.
2. Crea una solicitud POST para el siguiente punto final:

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

3. En el encabezado de la solicitud, establece el tipo de contenido en application/json.
4. En el URI de la solicitud, especifique su. `workflowName`

   El `workflowName` debe:

   - Debe tener entre 1 y 255 caracteres
   - Coincide con el patrón [a-zA-z_0-9-] *
5. Para el cuerpo de la solicitud, proporciona el siguiente JSON:

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

```
         "uniqueId": "string"
      }
   ]
}
```

Donde:

- `processingType`(opcional): el valor predeterminado es. `CONSISTENT` Elija uno de estos valores:
  - `CONSISTENT`- Para obtener la máxima precisión con un tiempo de respuesta más lento
  - `EVENTUAL`- Para una respuesta inicial más rápida con procesamiento en segundo plano
  - `EVENTUAL_NO_LOOKUP`- Para una respuesta más rápida cuando se sabe que los registros son únicos
- `records`(obligatorio) - Matriz que contiene exactamente un objeto de registro

6. Envíe la solicitud .

Si se ejecuta correctamente, recibirás una respuesta con el código de estado 200 y un cuerpo JSON que contiene:

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

Si la llamada no se realiza correctamente, es posible que recibas uno de los siguientes errores:

- 403: AccessDeniedException si no tienes acceso suficiente
- 404: ResourceNotFoundException si no se puede encontrar el recurso
- 429: ThrottlingException si la solicitud se ha limitado
- 400: ValidationException si la entrada no pasa la validación
- 500: InternalServerException si hay un fallo en el servicio interno

Búsqueda de un identificador de coincidencia para un flujo de trabajo de coincidencia basado en reglas

Tras completar un flujo de trabajo de coincidencia basado en reglas, puede recuperar el identificador de coincidencia y la regla asociada para cada registro procesado. Esta información le ayuda a comprender cómo se compararon los registros y qué reglas se aplicaron. El siguiente procedimiento muestra cómo acceder a estos datos mediante la AWS Entity Resolution consola o la `GetMatchID` API.

Console

Para buscar un Match ID mediante la consola

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.
3. Elija el flujo de trabajo coincidente basado en reglas que se ha procesado (el estado del trabajo es Completado).
4. En la página de detalles del flujo de trabajo coincidente, seleccione la pestaña Coincidencia IDs.
5. Selecciona Buscar ID de coincidencia.

> **Note**
>
> La opción Buscar ID de coincidencia solo está disponible para los flujos de trabajo coincidentes que utilizan la cadencia de procesamiento automática. Si

ha seleccionado la cadencia de procesamiento manual, esta opción aparecerá inactiva. Para usar esta opción, edite su flujo de trabajo para usar la cadencia de procesamiento automática. Para obtener más información sobre la edición de flujos de trabajo, consulteEdición de un flujo de trabajo coincidente.

6. Realice una de las siguientes acciones:

Si...	Entonces...
Solo hay un mapeo de esquemas asociado a este flujo de trabajo.	Vea el mapeo de esquemas que está seleccionado de forma predeterminada.
Hay más de un mapeo de esquemas asociado a este flujo de trabajo.	Elija el mapeo de esquemas en la lista desplegable.

7. En el caso de los atributos del registro, introduzca el valor de una clave de coincidencia existente para buscar cada registro existente.

> **Tip**
>
> Introduce tantos valores como puedas para ayudarte a encontrar el identificador de coincidencia.

8. La opción Normalizar datos está seleccionada de forma predeterminada, de modo que las entradas de datos se normalizan antes de la coincidencia. Si no desea normalizar los datos, deseleccione la opción Normalizar datos.
9. Si desea ver las reglas de coincidencia, expanda la opción Ver reglas de coincidencia.
10. Elija Look up (Buscar).

    Aparece un mensaje de confirmación que indica que se ha encontrado el identificador de coincidencia.
11. Vea el identificador de coincidencia correspondiente y la regla asociada que se encontró.

API

Para buscar un identificador de coincidencia mediante la API

> **Note**
>
> Para llamar a esta API correctamente, primero debes haber ejecutado correctamente un flujo de trabajo de coincidencia basado en reglas mediante la StartMatchingJob API.
> Para obtener una lista completa de los lenguajes de programación compatibles, consulta la sección Vea también de la API de GetMatchID.

1. Abre un terminal o una línea de comandos para realizar la solicitud de API.
2. Crea una solicitud POST para el siguiente punto final:

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

3. En el encabezado de la solicitud, establece el tipo de contenido en application/json.
4. En el URI de la solicitud, especifique su. `workflowName`

   El `workflowName` debe:

   - Debe tener entre 1 y 255 caracteres
   - Coincide con el patrón [a-zA-z_0-9-] *
5. Para el cuerpo de la solicitud, proporciona el siguiente JSON:

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

   Donde:

   `applyNormalization`(opcional): configúrelo en `true` para normalizar los atributos definidos en el esquema

   `record`(obligatorio): el registro del que se va a buscar el identificador de coincidencia

6. Envíe la solicitud .

   Si se ejecuta correctamente, recibirás una respuesta con el código de estado 200 y un cuerpo JSON que contiene:

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

   El `matchId` es el identificador único de este grupo de registros coincidentes e `matchRule` indica la regla con la que coincide el registro.

   Si la llamada no se realiza correctamente, es posible que recibas uno de los siguientes errores:

   - 403: AccessDeniedException si no tienes acceso suficiente
   - 404: ResourceNotFoundException si no se puede encontrar el recurso
   - 429: ThrottlingException si la solicitud se ha limitado
   - 400: ValidationException si la entrada no pasa la validación
   - 500: InternalServerException si hay un fallo en el servicio interno

Eliminar registros de un flujo de trabajo coincidente basado en reglas o aprendizaje automático

Si necesita cumplir con las normas de gestión de datos, puede eliminar los registros de un flujo de trabajo coincidente basado en reglas o en aprendizaje automático.

Para eliminar registros de un flujo de trabajo coincidente basado en reglas o aprendizaje automático

1. Inicie sesión en AWS Management Console y abra la consola en AWS Entity Resolution . https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Matching.
3. Elija el flujo de trabajo de coincidencia basado en reglas o en ML.
4. En la página de detalles del flujo de trabajo coincidente, seleccione Eliminar de forma única en la IDs lista desplegable Acciones.

5. Introduce el identificador único que deseas eliminar en la IDs sección Único.

   Puedes introducir hasta 10 únicos IDs.

6. Especifique la fuente de entrada desde la que se eliminará el único IDs.

   Si solo hay una fuente de entrada para el flujo de trabajo, la fuente de entrada aparece de forma predeterminada.

   Si solo especifica una fuente de entrada, la única de IDs las demás fuentes de entrada no se verá afectada.

7. Selecciona Eliminar único IDs.

Solución de problemas de flujos de trabajo

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al ejecutar flujos de trabajo coincidentes.

He recibido un archivo de error después de ejecutar un flujo de trabajo coincidente

Causa habitual

Un flujo de trabajo coincidente puede tener varias ejecuciones y los resultados (aciertos o errores) se escriben en una carpeta con el `jobId` nombre.

Los resultados correctos de un flujo de trabajo coincidente se escriben en una `success` carpeta que contiene varios archivos, y cada archivo contiene un subconjunto de los registros correctos.

Los errores de un flujo de trabajo coincidente se escriben en una `error` carpeta con varios campos, cada uno de los cuales contiene un subconjunto de los registros de errores.

El archivo de errores se puede crear por los siguientes motivos:

- El identificador único es:
  - null
  - falta en una fila de datos
  - falta en un registro de la tabla de datos
  - repetido en otra fila de datos de la tabla de datos

- no especificada
- no es único dentro de la misma fuente
- no es único en varias fuentes
- se superpone entre fuentes
- supera los 38 caracteres (solo flujo de trabajo de coincidencia basado en reglas)

- Uno de los campos del mapeo del esquema incluye un nombre reservado:
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - MatchID
  - HashingProtocol
  - ConfidenceLevel
  - Origen

> **Note**
>
> Si el registro del archivo de errores se crea por los motivos enumerados anteriormente, se le cobrará, ya que implica un coste de procesamiento del servicio. Si el registro del archivo de errores se debe a un error interno del servidor, no se te cobrará nada.

Resolución

Para resolver este problema

1. Comprueba si el identificador único es válido.

   Si el identificador único no es válido, actualícelo en la tabla de datos, guarde la nueva tabla de datos, cree un nuevo esquema de mapeo y vuelva a ejecutar el flujo de trabajo correspondiente.
2. Compruebe si uno de los campos de la asignación del esquema incluye un nombre reservado.

   Si uno de los campos incluye un nombre reservado, cree una nueva asignación de esquemas con un nombre nuevo y ejecute de nuevo el flujo de trabajo correspondiente.

Mapee los datos de entrada mediante un flujo de trabajo de mapeo de ID

Un flujo de trabajo de asignación de ID es un trabajo de procesamiento de datos que asigna datos de un origen de datos de entrada a un destino de datos de entrada en función del método de asignación de ID especificado. Produce una tabla de asignación de ID.

Un flujo de trabajo de mapeo de identidad requiere una fuente de datos de entrada y un destino de datos de entrada. La fuente y el destino de entrada de datos dependen del tipo de mapeo de ID que desee realizar. Hay dos formas de realizar el mapeo de ID: mediante reglas o mediante servicios de proveedores:

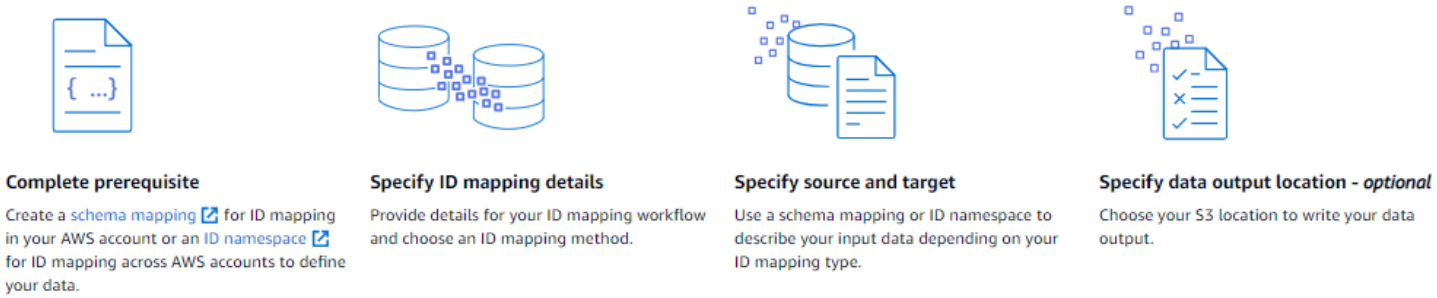
- Asignación de ID basado en reglas: se utilizan reglas de coincidencia para traducir datos propios de un origen a un destino.
- Mapeo de ID de los servicios del proveedor: se utiliza el servicio del LiveRamp proveedor para traducir datos de terceros de una fuente a un destino.

> **Note**
>
> El flujo de trabajo de mapeo de ID de los servicios del proveedor AWS Entity Resolution está integrado actualmente con LiveRamp. Si tiene una suscripción al LiveRamp servicio, puede crear un flujo de trabajo de mapeo de ID con el LiveRamp que realizar la transcodificación. Con la LiveRamp transcodificación, puede traducir un conjunto de Ramp de origen IDs a cualquier RampID de destino. Al utilizar el RampID como símbolo para representar a tus clientes, puedes evitar compartir los datos de los clientes directamente con las plataformas de publicidad.
> Para obtener más información, consulte Realizar traducciones mediante ADX en el sitio web de LiveRamp documentación.

Puede realizar un mapeo de ID entre dos conjuntos de datos en cualquiera de los siguientes escenarios:

- Dentro del tuyo Cuenta de AWS
- A través de dos diferentes Cuentas de AWS

El siguiente diagrama resume cómo configurar un flujo de trabajo de mapeo de ID.



Temas

- Flujo de trabajo de mapeo de ID para una Cuenta de AWS
- Flujo de trabajo de mapeo de ID en dos Cuentas de AWS
- Ejecutar un flujo de trabajo de mapeo de ID
- Ejecutar un flujo de trabajo de mapeo de ID con un nuevo destino de salida
- Edición de un flujo de trabajo de mapeo de ID
- Eliminar un flujo de trabajo de mapeo de ID
- Añadir o actualizar una política de recursos para un flujo de trabajo de mapeo de ID

Flujo de trabajo de mapeo de ID para una Cuenta de AWS

Un flujo de trabajo de mapeo de ID para uno Cuenta de AWS le permite realizar un mapeo de ID entre dos conjuntos de datos por su cuenta. Cuenta de AWS

Antes de crear un flujo de trabajo de mapeo de ID por su cuenta Cuenta de AWS, primero debe cumplir los requisitos previos.

Después de crear y ejecutar un flujo de trabajo de mapeo de ID, puede ver el resultado (la tabla de mapeo de ID) y usarlo para el análisis.

Los siguientes temas lo guían a través de una serie de pasos para crear un flujo de trabajo de mapeo de ID en el mismo Cuenta de AWS.

Temas

- Requisitos previos
- Crear un flujo de trabajo de mapeo de ID (basado en reglas)
- Creación de un flujo de trabajo de mapeo de ID (servicios de proveedores)

Requisitos previos

Antes de crear un flujo de trabajo de mapeo de ID para uno de ellos Cuenta de AWS mediante el método de mapeo de ID basado en reglas o el método de mapeo de ID de Provider Services, primero debe hacer lo siguiente:

- Complete las tareas de Configuración de la resolución de entidades de AWS.
- Complete las tareas en Preparar tablas de datos de entrada función del tipo de datos de entrada que utilice.
- Cree un esquema de mapeo o cree un flujo de trabajo coincidente.
- (Solo mapeo de ID de servicios de proveedores) Antes de crear un flujo de trabajo de mapeo de ID con LiveRamp, debe elegir un depósito de almacenamiento provisional de datos de Amazon Simple Storage Service (Amazon S3) en el que desee escribir temporalmente el resultado del flujo de trabajo de mapeo de ID.

  Si utiliza el servicio del LiveRamp proveedor para traducir datos de terceros, añada la siguiente política de permisos, que le permitirá acceder al depósito de almacenamiento provisional de datos.

  JSON

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

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

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

En la política de permisos anterior, sustituya cada uno *<user input placeholder>* por su propia información.

staging-bucket	El depósito de Amazon S3 que almacena temporalmente sus datos mientras ejecuta un flujo de trabajo basado en los servicios del proveedor.

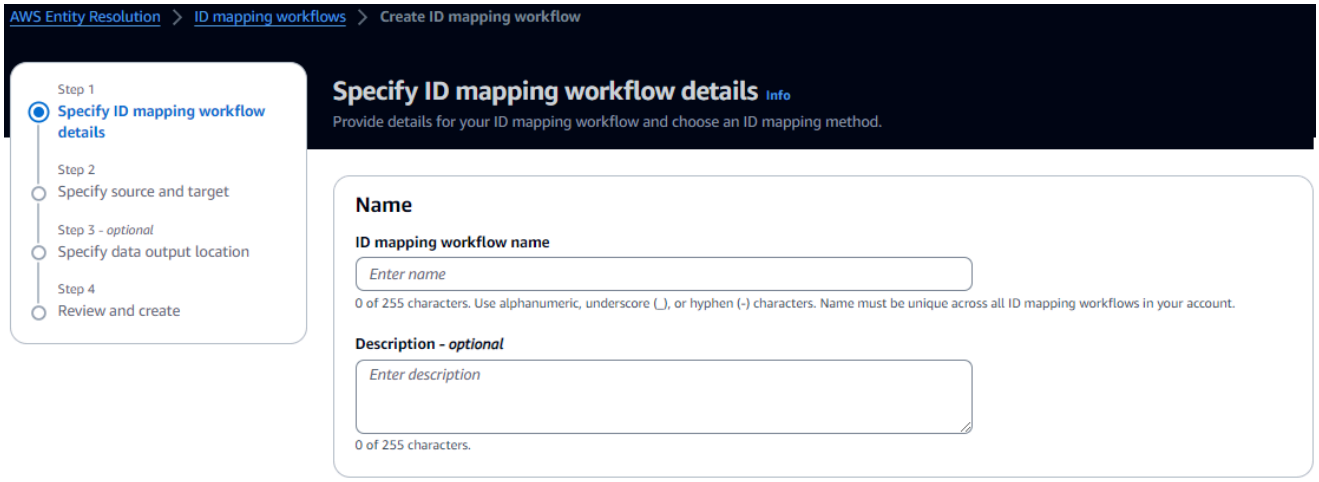
Crear un flujo de trabajo de mapeo de ID (basado en reglas)

En este tema se describe el proceso de creación de un flujo de trabajo de mapeo de ID para uno Cuenta de AWS que utilice reglas de coincidencia para traducir datos propios de una fuente a un destino.

Para crear un flujo de trabajo de mapeo de ID basado en reglas para una Cuenta de AWS

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en. https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Asignación de ID.

3. En la página de flujos de trabajo de mapeo de ID, en la esquina superior derecha, selecciona Crear flujo de trabajo de mapeo de ID.
4. Para el paso 1: especificar los detalles del flujo de trabajo de mapeo de ID, haga lo siguiente.
   a. Introduzca un nombre para el flujo de trabajo de mapeo de ID y una descripción opcional.



   b. Para el método de mapeo de ID, elija Basado en reglas.
   c. (Opcional) Para habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.
   d. Elija Siguiente.
5. Para el paso 2: especificar el origen y el destino, haga lo siguiente.
   a. En Source, elija el escenario que se aplique a su caso y, a continuación, lleve a cabo la acción recomendada.

Escenario	Acción recomendada
Utilice su propia asignación AWS Glue de bases de datos, AWS Glue tablas y esquemas en el flujo de trabajo de mapeo de ID.	1. Elija el mapeo de esquemas. 2. Seleccione una AWS Gluebase de datos del menú desplegable, seleccion e la AWS Glue tabla y, a continuación, seleccione la asignación de esquemas correspondiente. Puede añadir hasta 19 entradas de datos.

Escenario	Acción recomendada
Utilice un flujo de trabajo coincidente existente que apunte a los datos de registro que desee utilizar en el flujo de trabajo de mapeo de ID.	1. Elija un flujo de trabajo coincidente. 2. Seleccione un flujo de trabajo coinciden te existente en la lista desplegable.

b. Para Target, selecciona un flujo de trabajo de Matching existente en la lista desplegable.

c. Para los parámetros de la regla, haga lo siguiente.

i. Especifique los controles de la regla seleccionando una de las siguientes opciones en función del tipo de fuente.

Tipo de origen	Acción recomendada
Flujo de trabajo correspondiente	Especifique los controles de reglas eligiendo si un origen, un destino o ambos pueden proporcionar reglas en un flujo de trabajo de mapeo de ID. Los controles de reglas deben ser compatibles entre el origen y el destino para poder utilizarlos en un flujo de trabajo de mapeo de ID. Por ejemplo, si un espacio de nombres de ID de origen limita las reglas al destino, pero el espacio de nombres de ID de destino limita las reglas al origen, se produce un error.
Mapeo de esquemas	Omita este paso.

ii. Para los parámetros de comparación y coincidencia, el tipo de comparación se establece automáticamente en Varios campos de entrada.

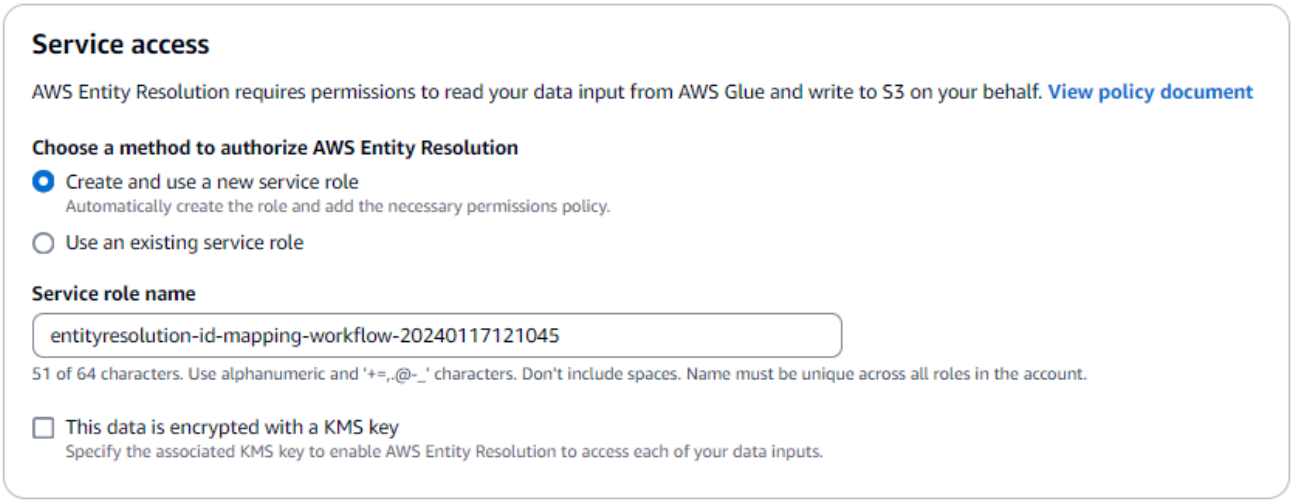
Esto se debe a que ambos participantes habían seleccionado esta opción anteriormente.

d. Especifique el tipo de registro coincidente eligiendo una de las siguientes opciones en función de su objetivo.

Su objetivo	Opción recomendada
Limite el tipo de registro coincidente para almacenar solo un registro coincidente en el origen por cada registro coincidente del destino cuando cree el flujo de trabajo de asignación de ID.	De una fuente a un destino
Limite el tipo de registro coincidente para almacenar solo registros coincidentes en el origen por cada registro coincidente del destino cuando cree el flujo de trabajo de asignación de ID.	Muchas fuentes para un objetivo

> **Note**
>
> Debe especificar las limitaciones compatibles para los espacios de nombres de los identificadores de origen y destino.

e. Para especificar los permisos de acceso al servicio, elija una opción y lleve a cabo la acción recomendada.



Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-id-mapping-workflow-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.

Opción	Acción recomendada
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

6. Elija Siguiente.
7. Para el paso 3: especificar la ubicación de salida de los datos (opcional), haga lo siguiente.
    a. Para el destino de salida de datos, haga lo siguiente:
        i. Elija la ubicación de Amazon S3 para la salida de datos.
        ii. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN o elija Crear una AWS KMS clave.
    b. Elija Siguiente.
8. Para el paso 4: revisar y crear, haga lo siguiente.
    a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.
    b. Seleccione Crear.

    Aparece un mensaje que indica que se ha creado el flujo de trabajo de mapeo de ID.

Tras crear el flujo de trabajo de mapeo de ID, estará listo para ejecutar un flujo de trabajo de mapeo de ID.

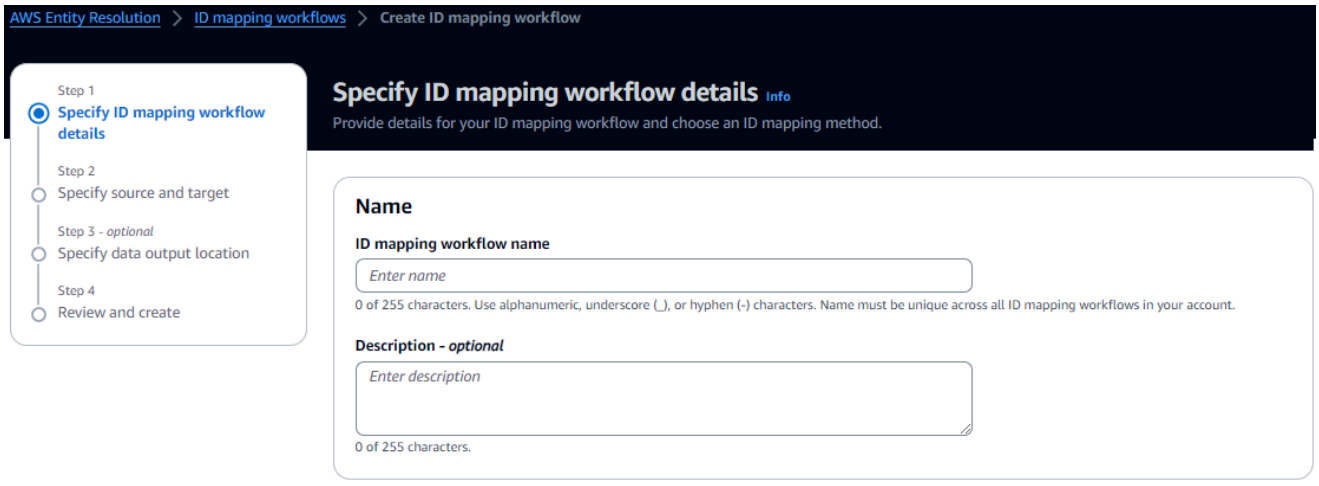
Creación de un flujo de trabajo de mapeo de ID (servicios de proveedores)

En este tema se describe el proceso de creación de un flujo de trabajo de mapeo de ID para una persona Cuenta de AWS mediante un servicio de proveedores denominado LiveRamp. LiveRamp traduce un conjunto de Ramp de origen IDs a otro conjunto utilizando Ramp mantenido o derivadoIDs.

Para crear un flujo de trabajo de mapeo de identidad basado en los servicios del proveedor para uno Cuenta de AWS

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Asignación de ID.
3. En la página de flujos de trabajo de mapeo de ID, en la esquina superior derecha, selecciona Crear flujo de trabajo de mapeo de ID.
4. Para el paso 1: especificar los detalles del flujo de trabajo de mapeo de ID, haga lo siguiente.

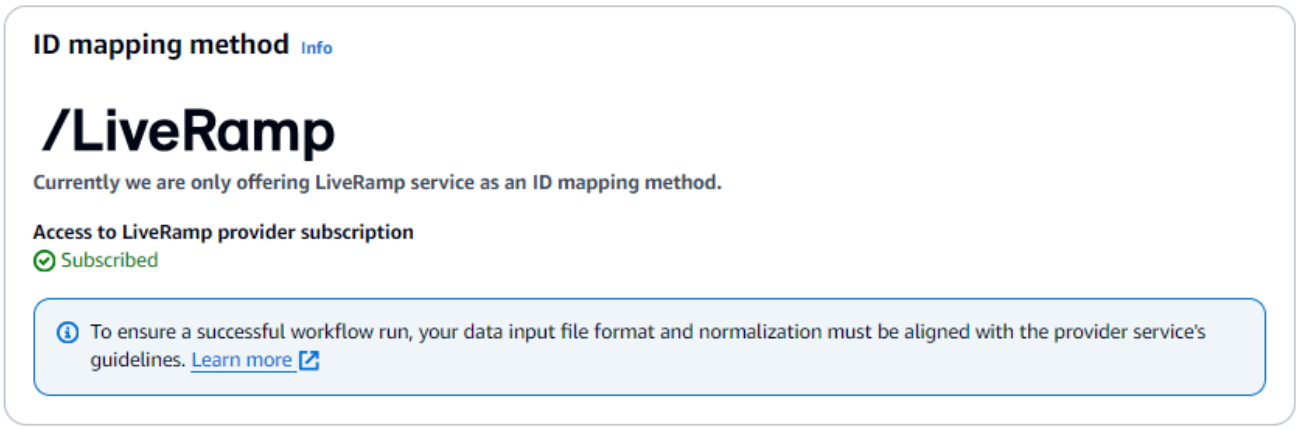
   a. Introduzca un nombre para el flujo de trabajo de mapeo de ID y una descripción opcional.



   b. Para el método de mapeo de ID, elija Provider services.

      AWS Entity Resolution actualmente ofrece el servicio del LiveRamp proveedor como un método de mapeo de ID. Si tiene una suscripción a LiveRamp, el estado aparece como

Suscrito. Para obtener más información sobre cómo suscribirse LiveRamp, consulte[Paso 1: Suscríbase a un servicio de proveedor en AWS Data Exchange](#).



> **Note**
>
> Asegúrese de que el formato del archivo de entrada de datos se ajuste a las directrices del servicio del proveedor. Para obtener más información sobre las pautas LiveRamp de formato de los archivos de entrada, consulte Realizar traducciones mediante ADX en el sitio web de LiveRamp documentación.

c. Para LiveRamp la configuración, introduzca los siguientes valores: LiveRamp

- Administrador de ID de cliente (ARN)
- Administrador de secretos de clientes (ARN)

d. (Opcional) Para habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.

e. Elija Siguiente.

5. Para el paso 2: especificar el origen y el destino, haga lo siguiente.

a. En Source, elija el escenario que se aplique a su caso y, a continuación, lleve a cabo la acción recomendada.

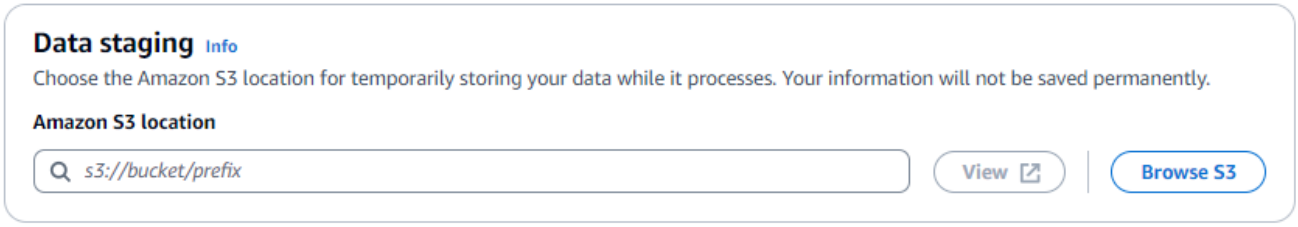
Escenario	Acción recomendada
Utilice su propia asignación AWS Glue de bases de datos, AWS Glue tablas y esquemas en el flujo de trabajo de mapeo de ID.	1. Elija el mapeo de esquemas. 2. Seleccione una AWS Gluebase de datos del menú desplegable, seleccion e la AWS Glue tabla y, a continuación, seleccione la asignación de esquemas correspondiente. Puede añadir hasta 19 entradas de datos.
Utilice un flujo de trabajo coincidente existente que apunte a los datos de registro que desee utilizar en el flujo de trabajo de mapeo de ID.	1. Elija un flujo de trabajo coincidente. 2. Seleccione un flujo de trabajo coinciden te existente en la lista desplegable.

b. En el caso de Target, realice una de las siguientes acciones en función del método de mapeo de ID que haya elegido.

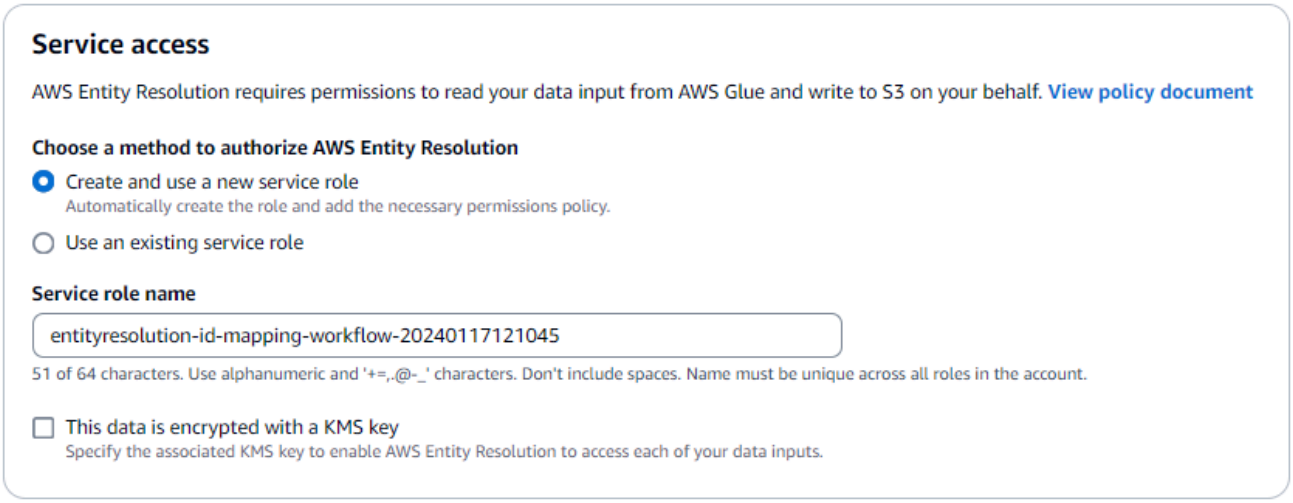
Método de mapeo de ID	Acción recomendada
Basado en reglas	Seleccione un flujo de trabajo coincidente existente en la lista desplegable.
Servicios de proveedores	Introduzca el identificador del dominio del LiveRamp cliente destinado a la transcodi ficación que se LiveRamp proporciona en el dominio de destino.

Método de mapeo de ID	Acción recomendada
	

c. Para la organización de datos, elija la ubicación de Amazon S3 en la que desee escribir temporalmente el resultado del flujo de trabajo de mapeo de ID.



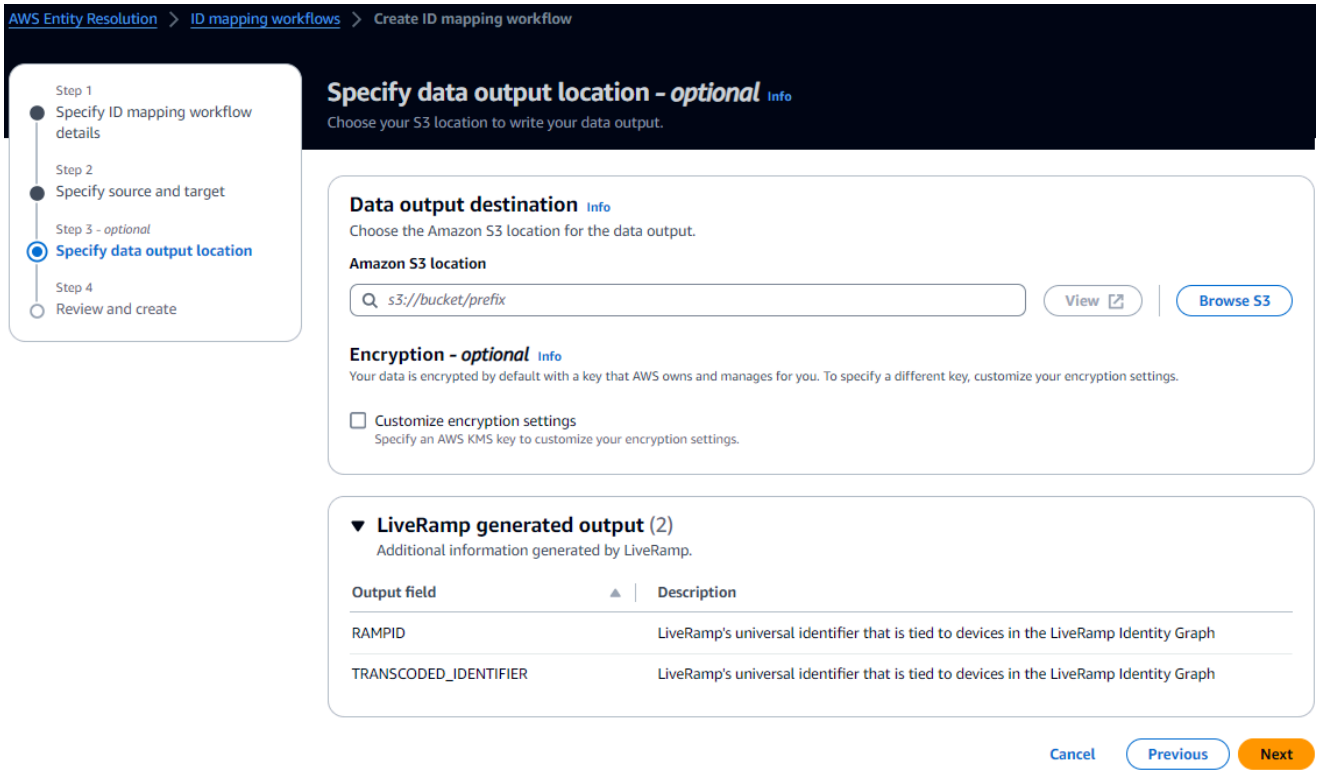
d. Para especificar los permisos de acceso al servicio, elija una opción y lleve a cabo la acción recomendada.



Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-id-mapping-workflow-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.

Opción	Acción recomendada
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

6. Elija Siguiente.
7. Para el paso 3: especificar la ubicación de salida de los datos (opcional), haga lo siguiente.
   a. Para el destino de salida de datos, haga lo siguiente:
      i. Elija la ubicación de Amazon S3 para la salida de datos.
      ii. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN o elija Crear una AWS KMS clave.
   b. Vea la salida LiveRamp generada.
   c. Elija Siguiente.



8. Para el paso 4: revisar y crear, haga lo siguiente.

   a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

   b. Seleccione Crear.

   Aparece un mensaje que indica que se ha creado el flujo de trabajo de mapeo de ID.

9. Tras crear el flujo de trabajo de mapeo de ID, estará listo para ejecutar un flujo de trabajo de mapeo de ID.

Flujo de trabajo de mapeo de ID en dos Cuentas de AWS

Un flujo de trabajo de mapeo de ID a través de dos Cuentas de AWS le permite realizar un mapeo de ID entre dos conjuntos de datos a través de dos Cuentas de AWS. Por lo general, esto se hace entre el suyo Cuenta de AWS y otro Cuenta de AWS.

Por ejemplo, un editor puede crear un flujo de trabajo de mapeo de ID utilizando su propio espacio de nombres de ID de destino (en el suyo propio Cuenta de AWS) y el espacio de nombres de ID de origen de un anunciante (en otro). Cuenta de AWS

Antes de crear un flujo de trabajo de mapeo de ID en dos Cuentas de AWS, primero debes cumplir los requisitos previos.

Después de crear un flujo de trabajo de mapeo de ID, puede ver el resultado (la tabla de mapeo de ID) y usarlo para el análisis.

Los siguientes temas lo guían a través de una serie de pasos para crear un flujo de trabajo de mapeo de ID en dos partes Cuentas de AWS:

Temas

Requisitos previos

Antes de crear un flujo de trabajo de mapeo de ID entre dos Cuentas de AWS personas, primero debe hacer lo siguiente:

- Completar las tareas de Configurar AWS Entity Resolution.
- Cree una fuente de espacio de nombres de ID.
- Crea un objetivo de espacio de nombres de ID.
- Adquiera el ARN del espacio de nombres de ID si utiliza una fuente de espacio de nombres de ID de otra. Cuenta de AWS
- (Solo servicios de proveedores) La creación de un flujo de trabajo de mapeo de ID entre dos Cuentas de AWS requiere permiso para acceder LiveRamp al bucket de S3 y a la AWS Key Management Service ()AWS KMS clave administrada por el cliente.

  Antes de crear un flujo de trabajo de mapeo de ID entre dos Cuentas de AWS LiveRamp, añada la siguiente política de permisos, que permite acceder LiveRamp al depósito de S3 y a la clave gestionada por el cliente.

  JSON

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

En la política de permisos anterior, sustituya cada uno *<user input placeholder>* por su propia información.

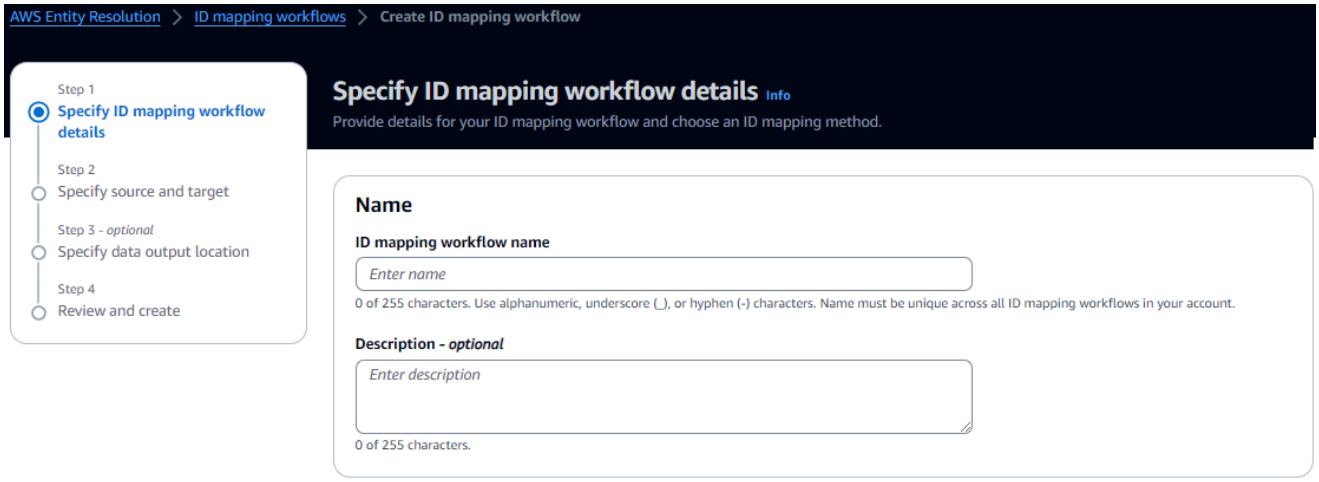
<KMSKeyARN>	El ARN de una clave gestionada por el AWS KMS cliente.

Crear un flujo de trabajo de mapeo de identidades (basado en reglas)

Una vez que haya completado los requisitos previos, puede crear uno o más flujos de trabajo de mapeo de ID para usar reglas de coincidencia para traducir datos propios de una fuente a un destino.

Para crear un flujo de trabajo de mapeo de ID basado en reglas que abarque dos Cuentas de AWS

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en. https://console.aws.amazon.com/entityresolution/
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Asignación de ID.
3. En la página de flujos de trabajo de mapeo de ID, en la esquina superior derecha, selecciona Crear flujo de trabajo de mapeo de ID.
4. Para el paso 1: especificar los detalles del flujo de trabajo de mapeo de ID, haga lo siguiente.
    a. Introduzca un nombre para el flujo de trabajo de mapeo de ID y una descripción opcional.



b. Para el método de mapeo de ID, elija Basado en reglas.

c. (Opcional) Para habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.

d. Elija Siguiente.

5. Para el paso 2: especificar el origen y el destino, haga lo siguiente.

a. Activa las opciones avanzadas.

b. En Origen, selecciona Flujo de trabajo coincidente y, a continuación, selecciona el flujo de trabajo coincidente existente en la lista desplegable.

c. Para Target, elija Flujo de trabajo coincidente y, a continuación, seleccione el flujo de trabajo coincidente existente en la lista desplegable.

d. Para los parámetros de la regla, especifique los controles de la regla eligiendo si una fuente o un destino pueden proporcionar reglas en un flujo de trabajo de mapeo de ID.

Los controles de reglas deben ser compatibles entre el origen y el destino para poder utilizarlos en un flujo de trabajo de mapeo de ID. Por ejemplo, si un espacio de nombres de ID de origen limita las reglas al destino, pero el espacio de nombres de ID de destino limita las reglas al origen, se produce un error.

e. Para los parámetros de comparación y coincidencia, haga lo siguiente.

i. Especifique el tipo de comparación eligiendo una opción en función de su objetivo.

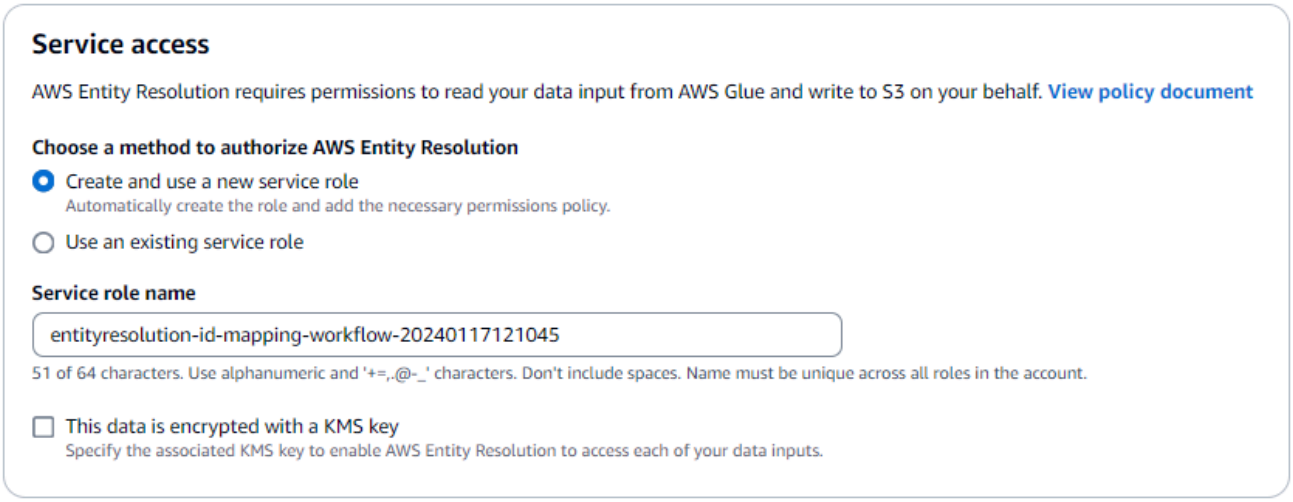
Su objetivo	Opción recomendada
Busque cualquier combinación de coincidencias entre los datos almacenados en varios campos de entrada, independientemente de si los datos están en el mismo campo de entrada o en un campo de entrada diferente.	Múltiples campos de entrada
Limite la comparación dentro de un solo campo de entrada, cuando los datos similares almacenados en varios campos de entrada no deberían coincidir.	Campo de entrada único

ii. Especifique el tipo de registro coincidente eligiendo una opción en función de su objetivo.

Su objetivo	Opción recomendada
Limite el tipo de registro coincidente para almacenar solo un registro coincidente en el origen por cada registro coincidente del destino cuando cree el flujo de trabajo de asignación de ID.	De una fuente a un destino
Limite el tipo de registro coincidente para almacenar solo registros coincidentes en el origen por cada registro coincidente del destino cuando cree el flujo de trabajo de asignación de ID.	Muchas fuentes para un objetivo

> **Note**
>
> Debe especificar las limitaciones compatibles para los espacios de nombres de los identificadores de origen y destino.

f. Para especificar los permisos de acceso al servicio, elija una opción y lleve a cabo la acción recomendada.



Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-id-mapping-workflow-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.

Opción	Acción recomendada
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

6. Elija Siguiente.
7. Para el paso 3: especificar la ubicación de salida de los datos (opcional), haga lo siguiente.
    a. Para el destino de salida de datos, haga lo siguiente.
        i. Elija la ubicación de Amazon S3 para la salida de datos.
        ii. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN o elija Crear una AWS KMS clave.
    b. Vea la salida LiveRamp generada.
    c. Elija Siguiente.
8. Para el paso 4: revisar y crear, haga lo siguiente.
    a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.
    b. Seleccione Crear.

Aparece un mensaje que indica que se ha creado el flujo de trabajo de mapeo de ID.

Tras crear el flujo de trabajo de mapeo de ID, estará listo para ejecutar un flujo de trabajo de mapeo de ID.

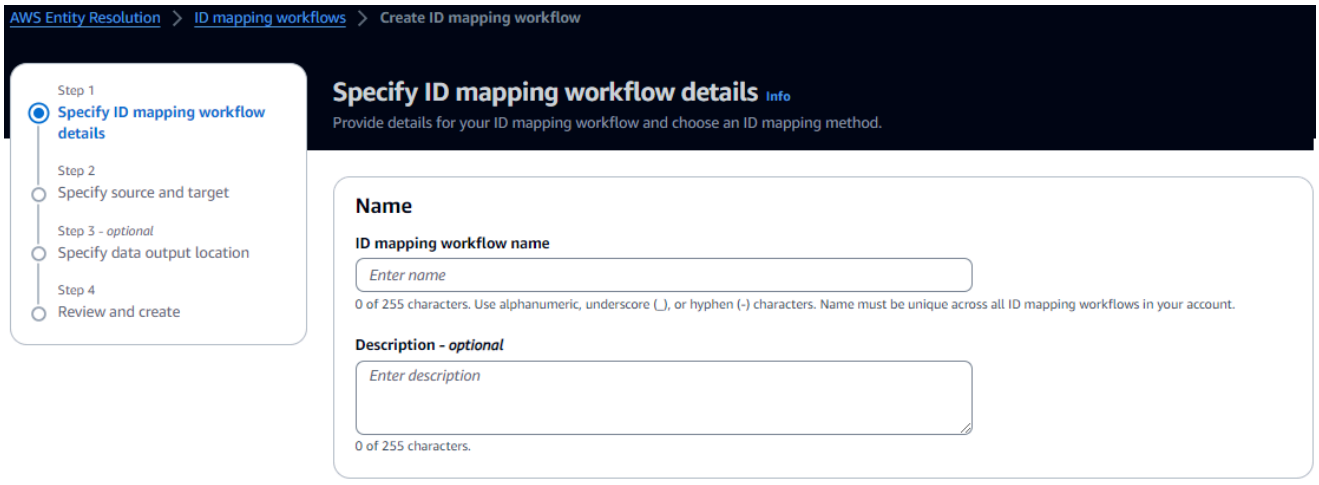
Creación de un flujo de trabajo de mapeo de ID (servicios de proveedores)

Después de completar los requisitos previos, puede crear uno o más flujos de trabajo de mapeo de ID utilizando el servicio del LiveRamp proveedor. LiveRamp convierte un conjunto de Ramp IDs de origen en otro conjunto utilizando Ramp IDs mantenido o derivado.

Para crear un flujo de trabajo de mapeo de ID mediante el servicio del proveedor

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Asignación de ID.
3. En la página de flujos de trabajo de mapeo de ID, en la esquina superior derecha, selecciona Crear flujo de trabajo de mapeo de ID.
4. Para el paso 1: especificar los detalles del flujo de trabajo de mapeo de ID, haga lo siguiente.

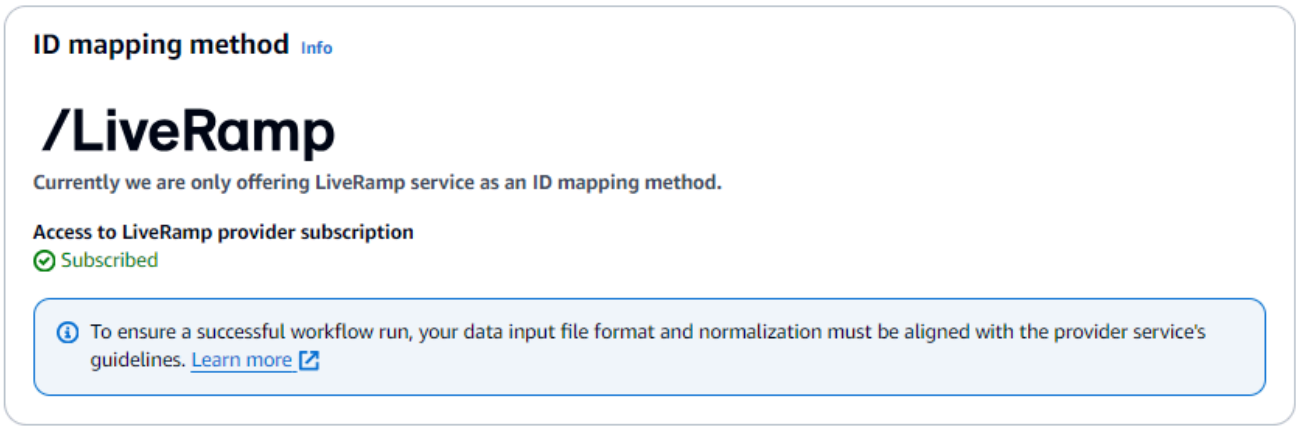
   a. Introduzca un nombre para el flujo de trabajo de mapeo de ID y una descripción opcional.



   b. Para el método de mapeo de ID, elija Provider services.

      AWS Entity Resolution actualmente ofrece el servicio del LiveRamp proveedor como un método de mapeo de ID. Si tiene una suscripción a LiveRamp, el estado aparece como

Suscrito. Para obtener más información sobre cómo suscribirse LiveRamp, consulte[Paso 1: Suscríbase a un servicio de proveedor en AWS Data Exchange](#).



> **Note**
>
> Asegúrese de que el formato del archivo de entrada de datos se ajuste a las directrices del servicio del proveedor. Para obtener más información sobre las pautas LiveRamp de formato de los archivos de entrada, consulte Realizar traducciones mediante ADX en el sitio web de LiveRamp documentación.

c. Para LiveRamp la configuración, introduzca los siguientes valores: LiveRamp

- Administrador de ID de cliente (ARN)
- Administrador de secretos de clientes (ARN)

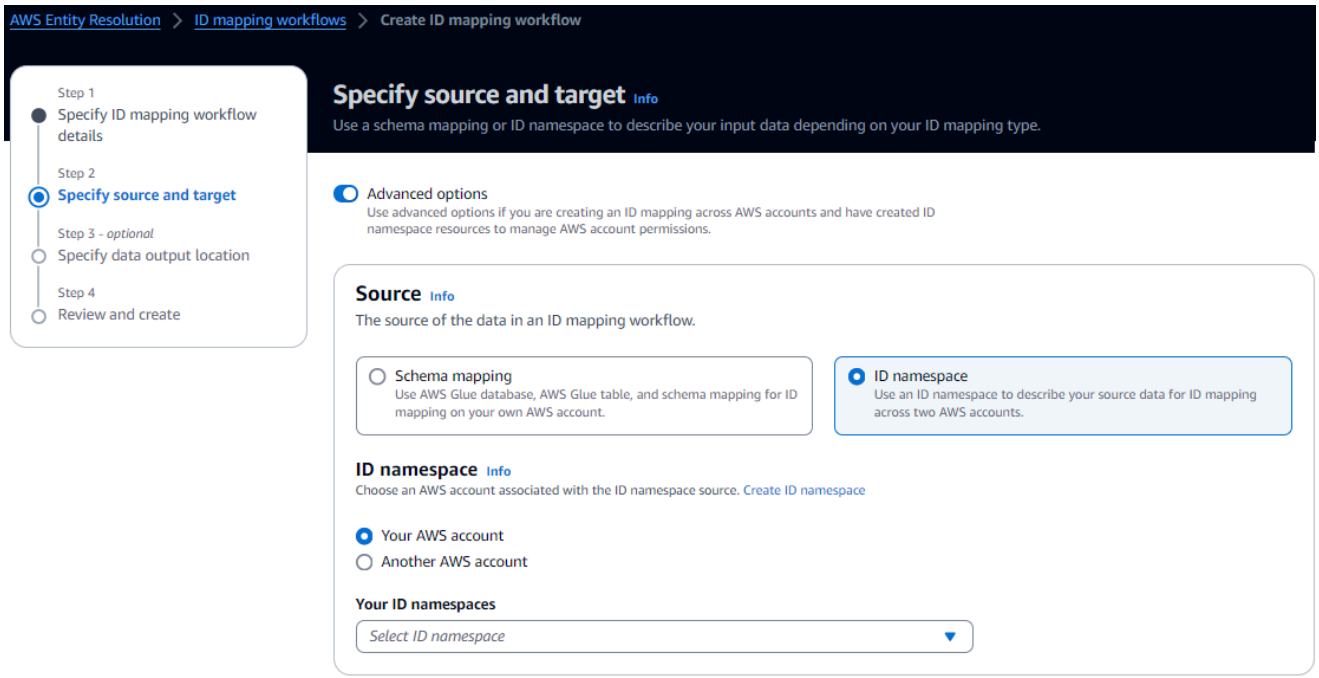
d. (Opcional) Para habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.

e. Elija Siguiente.

5. Para el paso 2: especificar el origen y el destino, haga lo siguiente.

a. Activa las opciones avanzadas.

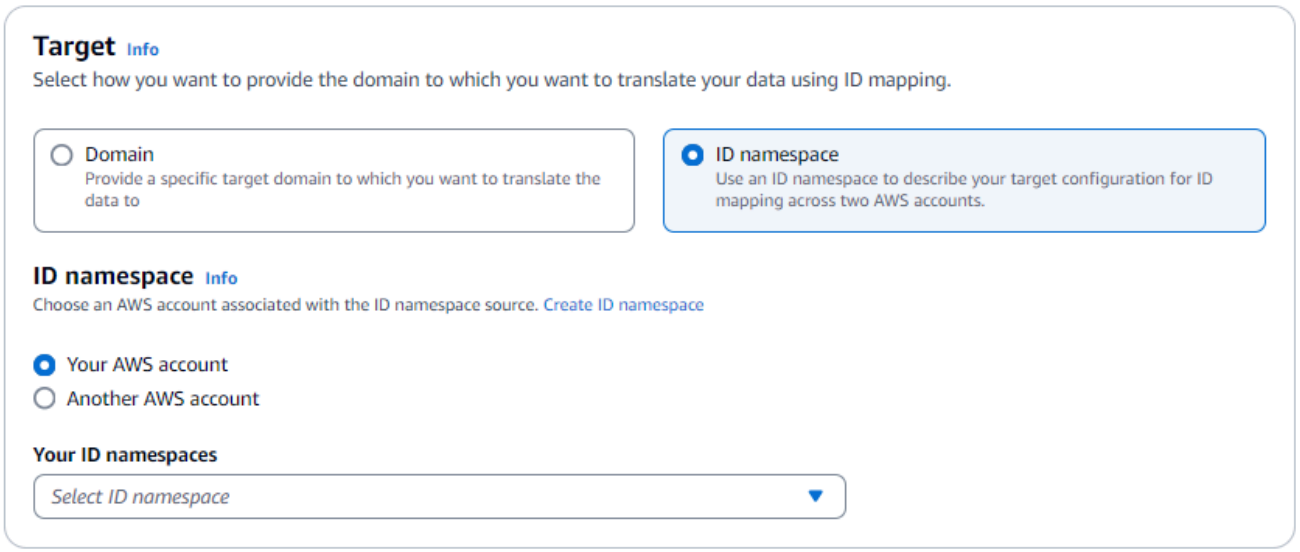
b. En Fuente, selecciona el espacio de nombres de ID.



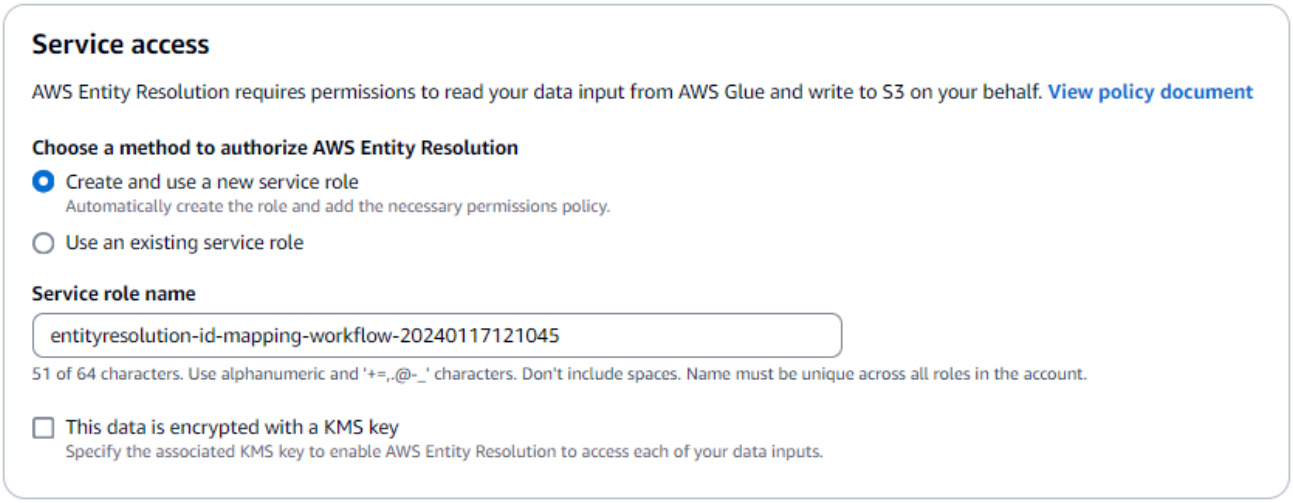
c. Para el espacio de nombres de ID, identifique dónde se encuentra el espacio de nombres de ID y, a continuación, tome las medidas recomendadas.

Ubicación del espacio de nombres de ID	Acción recomendada
El tuyo Cuenta de AWS	1. Elige tu Cuenta de AWS. 2. Seleccione el espacio de nombres de ID en la lista desplegable de espacios de nombres de su ID.
De otra persona Cuenta de AWS	1. Elige otro Cuenta de AWS. 2. Introduzca el ARN del espacio de nombres del ID.

d. En Target, elija el espacio de nombres de ID.



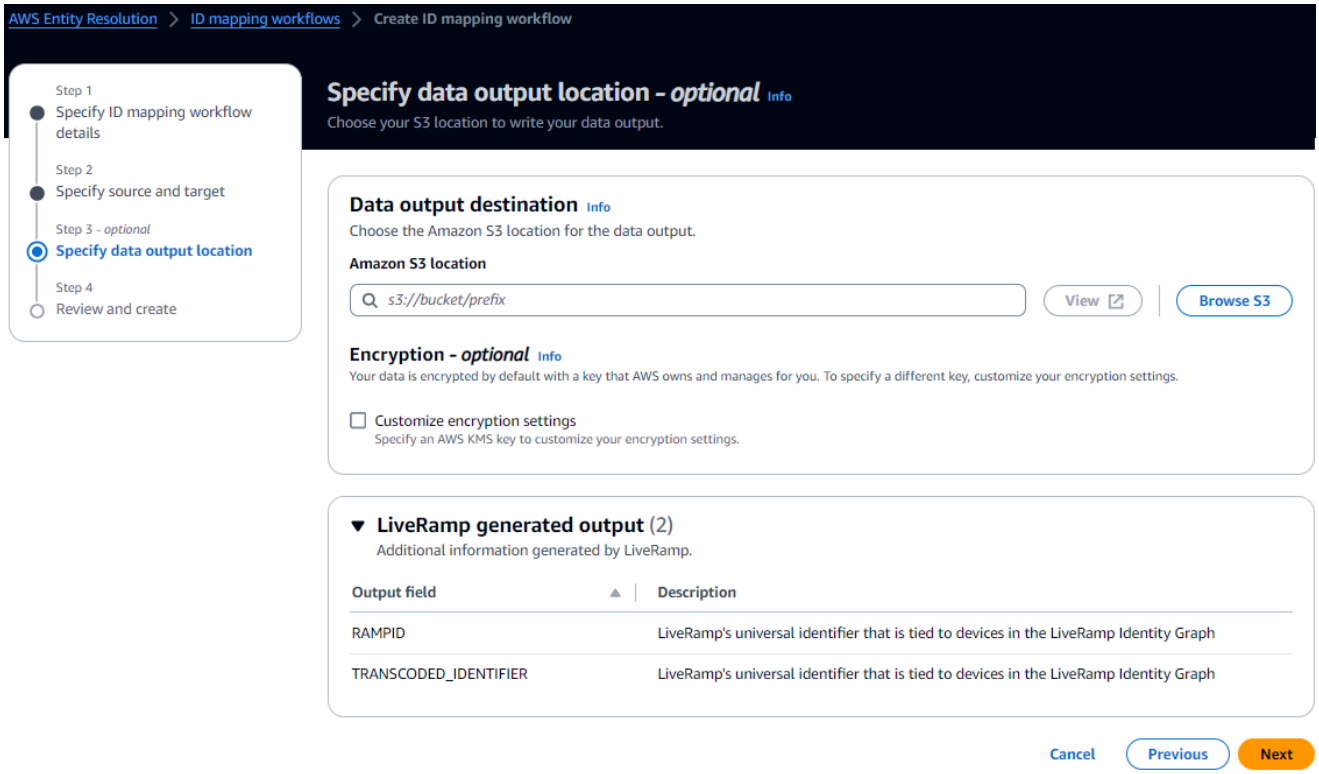
e. Para especificar los permisos de acceso al servicio, elija una opción y lleve a cabo la acción recomendada.



Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-id-mapping-workflow-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.

Opción	Acción recomendada
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

6. Elija Siguiente.
7. Para el paso 3: especificar la ubicación de salida de los datos (opcional), haga lo siguiente.
   a. Para el destino de salida de datos, haga lo siguiente.
      i. Elija la ubicación de Amazon S3 para la salida de datos.
      ii. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN o elija Crear una AWS KMS clave.
   b. Vea la salida LiveRamp generada.
   c. Elija Siguiente.



8. Para el paso 4: revisar y crear, haga lo siguiente.

   a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

   b. Seleccione Crear.

      Aparece un mensaje que indica que se ha creado el flujo de trabajo de mapeo de ID.

Tras crear el flujo de trabajo de mapeo de ID, estará listo para ejecutar un flujo de trabajo de mapeo de ID.

Ejecutar un flujo de trabajo de mapeo de ID

Después de crear un flujo de trabajo de mapeo de ID para uno Cuenta de AWS o crear un flujo de trabajo de mapeo de ID para dos Cuentas de AWS, puede ejecutar el flujo de trabajo de mapeo de ID. El flujo de trabajo de mapeo de ID genera un archivo CSV.

Para ejecutar un flujo de trabajo de mapeo de ID

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.

2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Asignación de ID.
3. Elija el flujo de trabajo de mapeo de ID.
4. En la página de detalles del flujo de trabajo de mapeo de ID, en la esquina superior derecha, selecciona Ejecutar.
5. En la página de detalles del flujo de trabajo correspondiente, en la pestaña Métricas, consulta lo siguiente en Métricas del último trabajo:

   - El identificador del trabajo
   - El tiempo completado para el trabajo del flujo de trabajo
   - El estado del trabajo de flujo de trabajo coincidente: en cola, en curso, completado o fallido
   - El número de registros procesados
   - El número de registros no procesados
   - El número de registros de entrada

   En Historial de trabajos, también puede ver las métricas de los trabajos de flujo de trabajo de mapeo de ID ejecutados anteriormente.
6. Cuando se complete el trabajo del flujo de trabajo de mapeo de ID (el estado es Completado), elija Salida de datos y, a continuación, elija su ubicación de Amazon S3 para ver los resultados.

   Después de obtener el archivo CSV, puede unirlo `RAMPID` con el`TRANSCODED_ID`.

Ejecutar un flujo de trabajo de mapeo de ID con un nuevo destino de salida

Después de crear un flujo de trabajo de mapeo de ID para uno Cuenta de AWS o de crear un flujo de trabajo de mapeo de ID para dos Cuentas de AWS, puede elegir una ubicación S3 diferente para escribir la salida de datos.

Para ejecutar un flujo de trabajo de mapeo de ID con un nuevo destino de salida

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Asignación de ID.
3. Elija el flujo de trabajo de mapeo de ID.

4. En la página de detalles del flujo de trabajo de mapeo de ID, en la esquina superior derecha, seleccione Ejecutar con un nuevo destino de salida en la lista desplegable Ejecutar flujo de trabajo.
5. Para el destino de salida de datos, haga lo siguiente.
   a. Elija la ubicación de Amazon S3 para la salida de datos.
   b. Para el cifrado, si elige personalizar la configuración de cifrado, introduzca la AWS KMS clave ARN o elija Crear una AWS KMS clave.
6. Para especificar los permisos de acceso al servicio, elija una opción y lleve a cabo la acción recomendada.

Opción	Acción recomendada
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `entityresolution-id-mapping-workflow-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, seleccione la opción Estos datos se cifran mediante una clave de KMS. A continuación, introduzca una AWS KMS clave que se utilice para descifrar la entrada de datos.
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles.

Opción	Acción recomendada
	Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Consulte el rol de servicio mediante la elección del enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de funciones existente para añadir los permisos necesarios.

7. Seleccione Ejecutar.
8. En la página de detalles del flujo de trabajo correspondiente, en la pestaña Métricas, consulta lo siguiente en Métricas del último trabajo:

   - El identificador del trabajo
   - El tiempo completado para el trabajo del flujo de trabajo
   - El estado del trabajo de flujo de trabajo coincidente: en cola, en curso, completado o fallido
   - El número de registros procesados
   - El número de registros no procesados
   - El número de registros de entrada

   En Historial de trabajos, también puede ver las métricas de los trabajos de flujo de trabajo de mapeo de ID ejecutados anteriormente.
9. Cuando se complete el trabajo del flujo de trabajo de mapeo de ID (el estado es Completado), elija Salida de datos y, a continuación, elija su ubicación de Amazon S3 para ver los resultados.

   Después de obtener el archivo CSV, puede unirlo `RAMPID` con el`TRANSCODED_ID`.

Edición de un flujo de trabajo de mapeo de ID

La edición del flujo de trabajo de mapeo de identidad le permite mantener sus capacidades de resolución de entidades up-to-date alineadas con las cambiantes necesidades de su empresa a lo largo del tiempo. Si desea ajustar las reglas, las técnicas y los parámetros de mapeo, puede optimizar el flujo de trabajo para proporcionar resultados de coincidencia de identidades más precisos y confiables. Es posible que también desee añadir nuevas fuentes de datos, ampliar los tipos de IDs mapeo o incorporar criterios de coincidencia adicionales en el flujo de trabajo. Si identifica problemas o errores en los resultados del mapeo de ID, editarlos con el flujo de trabajo puede ayudarle a diagnosticar y resolver esos problemas.

Para editar un flujo de trabajo de mapeo de ID:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Asignación de ID.
3. Elija el flujo de trabajo de mapeo de ID.
4. En la página de detalles del flujo de trabajo de mapeo de ID, en la esquina superior derecha, selecciona Editar.
5. En la página Especificar los detalles del flujo de trabajo de mapeo de ID, realice los cambios necesarios y, a continuación, seleccione Siguiente.
6. En la página Especificar la salida de datos, realice los cambios necesarios y, a continuación, seleccione Siguiente.
7. En la página Revisar y guardar, realice los cambios necesarios y, a continuación, seleccione Guardar.

Eliminar un flujo de trabajo de mapeo de ID

Si ya no utilizas un flujo de trabajo de mapeo de identidad, eliminarlo puede ayudarte a agilizar la gestión del flujo de trabajo. Además, eliminar los flujos de trabajo de mapeo de identidad redundantes o menos eficientes que sirven para fines similares puede ayudarle a consolidar sus procesos.

Para eliminar un flujo de trabajo de mapeo de ID:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Asignación de ID.
3. Elija el flujo de trabajo de mapeo de ID.
4. En la página de detalles del flujo de trabajo de mapeo de ID, en la esquina superior derecha, selecciona Eliminar.
5. Confirme la eliminación y luego elija Eliminar.

Añadir o actualizar una política de recursos para un flujo de trabajo de mapeo de ID

Una política de recursos permite al creador del recurso de mapeo de ID acceder a su recurso de flujo de trabajo de mapeo de ID.

Para añadir o actualizar una política de recursos

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona Asignación de ID.
3. Elija el flujo de trabajo de mapeo de ID.
4. En la página de detalles del flujo de trabajo de mapeo de ID, seleccione la pestaña Permisos.
5. En la sección Política de recursos, seleccione Editar.
6. Agrega o actualiza la política en el editor JSON.
7. Seleccione Save changes (Guardar cambios).

AWS Entity Resolution Intégrese como proveedor

AWS Entity Resolution Las integraciones de proveedores externos ayudan a los clientes a proteger la privacidad de los consumidores y a cumplir con las leyes de soberanía de datos. Los proveedores externos, como Ramp LiveRamp IDs y TransUnion Fabrick, traducen los identificadores de los consumidores en publicidad IDs. IDs Estos identificadores de publicidad se utilizan habitualmente en las herramientas de publicidad y marketing para evitar que los datos de los consumidores se exporten a sistemas no gestionados.AWS En esta sección se proporcionan instrucciones para que los proveedores integren la codificación o transcodificación de los identificadores de los consumidores AWS Entity Resolution para convertirlos en publicidad y utilizarlos en un flujo de trabajo de búsqueda de IDs coincidencias basado en los servicios de los proveedores.

Para obtener más información sobre los servicios de proveedores con los que están integrados actualmente, consulte. AWS Entity ResolutionCrear un flujo de trabajo coincidente basado en los servicios del proveedor

Temas

- Requisitos
- Uso de la AWS Entity Resolution especificación OpenAPI
- Probar la integración de un proveedor

Requisitos

Antes de integrarte como proveedor de servicios AWS Entity Resolution, completa los siguientes requisitos.

Temas

- Incluya un servicio de proveedor en AWS Data Exchange
- Identifique sus atributos
- Solicita la especificación de AWS Entity Resolution OpenAPI

Incluya un servicio de proveedor en AWS Data Exchange

Como proveedor externo, debe incluir su producto en el catálogo de productos de AWS Data Exchange (ADX). Una vez que su producto aparezca en el catálogo de AWS Data Exchange productos, los suscriptores pueden suscribirse a él mediante una oferta pública o privada.

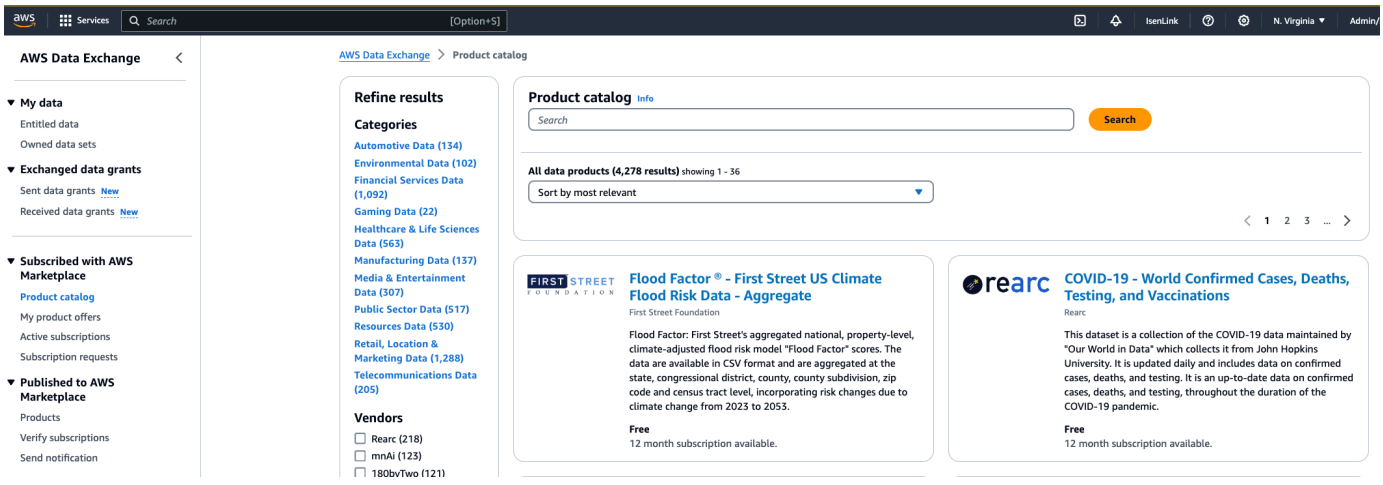
Para incluir un servicio de un proveedor en AWS Data Exchange

1. Si eres un nuevo proveedor de productos de datos en AWS Data Exchange, sigue los pasos de la sección titulada Cómo empezar como proveedor de la Guía del AWS Data Exchange usuario.
2. Cree un conjunto de datos de la API REST y publique un nuevo producto que lo contenga APIs AWS Data Exchange siguiendo los pasos de la sección titulada Cómo publicar un producto que figura APIs en la Guía del AWS Data Exchange usuario. Puede completar el proceso mediante la AWS Data Exchange consola o el AWS Command Line Interface.

   Si has configurado la visibilidad del producto como pública, la oferta pública estará disponible para todos los suscriptores.

   Si has configurado la visibilidad del producto como privada, sigue los pasos de la sección titulada Crear ofertas personalizadas de la Guía del AWS Data Exchange usuario, en función de tu caso de uso.

   La siguiente imagen muestra un ejemplo de un producto disponible en el catálogo de AWS Data Exchange productos.



3. Una vez que el producto esté disponible en el catálogo de AWS Data Exchange productos, el suscriptor puede suscribirse al producto de las siguientes maneras.

- Suscríbase al producto público.
- Utilice una oferta privada (oferta personalizada) emitida por el proveedor de servicios.
- Utilice la oferta Bring Your Own Subscription (BYOS).

Para obtener más información, consulte Suscríbase a un producto incluido APIs en la Guía del AWS Data Exchange usuario y acceda a él.

Identifique sus atributos

Los atributos de los datos de entrada son las definiciones de tipo de las entidades que se van a resolver en un flujo de trabajo. Algunos ejemplos de atributos son `FirstNameLastName`,`Email`, o`Custom String`.

Cuando identifique sus atributos, debe tener en cuenta los requisitos o las directrices.

Example Ejemplo

El siguiente es un ejemplo de validaciones para identificar los atributos del proveedor.

- El `LastName` atributo `FirstName` o es obligatorio.
- Si el `Email` atributo está presente, debe tener un hash.

Como proveedor, debe identificar los atributos del producto de servicio de su proveedor y, a continuación, comunicarlos al equipo de desarrollo AWS Entity Resolution empresarial de `<aws-entity-resolution-bd@amazon .com>` para su posterior validación antes de continuar.

Solicita la especificación de AWS Entity Resolution OpenAPI

AWS Entity Resolution tiene una especificación de OpenAPI que usted, como proveedor, puede usar como un apretón de manos que contiene lo que APIs implica la integración. Para obtener más información, consulte Uso de la AWS Entity Resolution especificación OpenAPI.

Para solicitar la definición de OpenAPI, póngase en contacto con el equipo AWS Entity Resolution de desarrollo empresarial en `<aws-entity-resolution-bd@amazon>` .com.

Uso de la AWS Entity Resolution especificación OpenAPI

La especificación OpenAPI define todos los protocolos asociados a. AWS Entity Resolution Esta especificación es necesaria para implementar la integración.

La definición de OpenAPI contiene las siguientes operaciones de API:

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

Para solicitar la especificación de OpenAPI, póngase en contacto con el equipo AWS Entity Resolution de desarrollo empresarial en `<aws-entity-resolution-bd@amazon>` .com.

La especificación OpenAPI admite dos tipos de integraciones para la codificación y la transcodificación de identificadores de consumo, el procesamiento por lotes y el procesamiento sincrónico. Una vez que haya obtenido la especificación OpenAPI, implemente el tipo de integración de procesamiento para su caso de uso.

Temas

Integración de procesamiento por lotes

La integración del procesamiento por lotes sigue un patrón de diseño asíncrono. Una vez iniciado un flujo de trabajo AWS Data Exchange, envía un trabajo a través de un punto final de integración de proveedores y, a continuación, el flujo de trabajo espera a que finalice el trabajo consultando periódicamente el estado del trabajo. Esta solución es más adecuada para las ejecuciones de tareas que pueden tardar más y en las que el rendimiento del proveedor es menor. El proveedor incluirá la ubicación del conjunto de datos como un enlace de Amazon S3, que podrá procesar por su parte y escribir los resultados en una ubicación S3 de salida predeterminada.

La integración del procesamiento por lotes se habilita mediante tres definiciones de API. AWS Entity Resolution llamará al punto final del proveedor, que está disponible AWS Data Exchange en el siguiente orden:

1. `POST CreateJob`: Esta operación de API envía la información del trabajo al proveedor para que la procese. Esta información se refiere al tipo de trabajo: codificación o transcodificación, las ubicaciones de S3, el esquema proporcionado por el cliente y cualquier propiedad adicional del trabajo requerida.

   Esta API devuelve un`JobId`, y el estado del Job será uno de los siguientes: `PENDINGREADY`,`IN_PROGRESS`,`COMPLETE`, o`FAILED`.

   Ejemplo de solicitud de codificación

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

   Respuesta de ejemplo

```
{
```

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

2. `POST StartJob`: Esta API le permite al proveedor saber cómo iniciar el trabajo en función de lo `JobId` proporcionado. Esto permite al proveedor realizar todas las validaciones necesarias desde hasta`CreateJob`. `StartJob`

   Esta API devuelve un`JobId`, el `Status` for the Job`statusMessage`, el `ystatusCode`.

   Ejemplo de solicitud de codificación

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

   Respuesta de ejemplo

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

3. `GET GetJob`: Esta API informa AWS Entity Resolution si el trabajo se ha completado o si se encuentra en algún otro estado.

   Esta API devuelve un`JobId`, el `Status` for the Job`statusMessage`, el `ystatusCode`.

   Ejemplo de solicitud de codificación

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

   Respuesta de ejemplo

   ```
   {
   ```

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

La definición completa de estos APIs se proporciona en la especificación AWS Entity Resolution OpenAPI.

Integración de procesamiento sincrónico

La solución de procesamiento sincrónico es más deseable para los proveedores que tienen un tiempo de respuesta casi en tiempo real con un tiempo de respuesta en tiempo real con un mayor rendimiento y un mayor TPS. Este AWS Entity Resolution flujo de trabajo divide el conjunto de datos y realiza varias solicitudes de API en paralelo. A continuación, el AWS Entity Resolution flujo de trabajo se encarga de escribir los resultados en la ubicación de salida deseada.

Este proceso se habilita mediante una de las definiciones de la API. AWS Entity Resolution llama al punto final del proveedor, que está disponible a través de AWS Data Exchange:

`POST AssignIdentities`: Esta API envía datos al proveedor mediante un `source_id` identificador y `recordFields` está asociada a ese registro.

Esta API devuelve el`assignedRecords`.

Ejemplo de solicitud de codificación

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

```
  ]
}
```

Respuesta de ejemplo

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

La definición completa de estos APIs se proporciona en la especificación AWS Entity Resolution OpenAPI.

Según el enfoque que elija el proveedor, AWS Entity Resolution creará una configuración para que el proveedor se utilice para iniciar la codificación o la transcodificación. Además, estas configuraciones están disponibles para los clientes mediante las APIs proporcionadas por AWS Entity Resolution.

Se puede acceder a esta configuración mediante un nombre de recurso de Amazon (ARN), que se deriva del lugar donde AWS Data Exchange está alojada la oferta de servicios del proveedor y del tipo de servicio del proveedor. AWS Entity Resolution se refiere a este ARN como. `providerServiceARN`

Probar la integración de un proveedor

Si bien AWS Entity Resolution aloja servicios de búsqueda de datos, la integración de un proveedor es un componente externo crucial para el flujo de trabajo de end-to-end búsqueda de datos. Se AWS Entity Resolution han definido varias pruebas para los proveedores que añaden una protección

en caso de que esta integración falle. Este enfoque brinda a los proveedores la oportunidad de monitorear el estado de sus servicios de acuerdo con estos casos end-to-end de prueba.

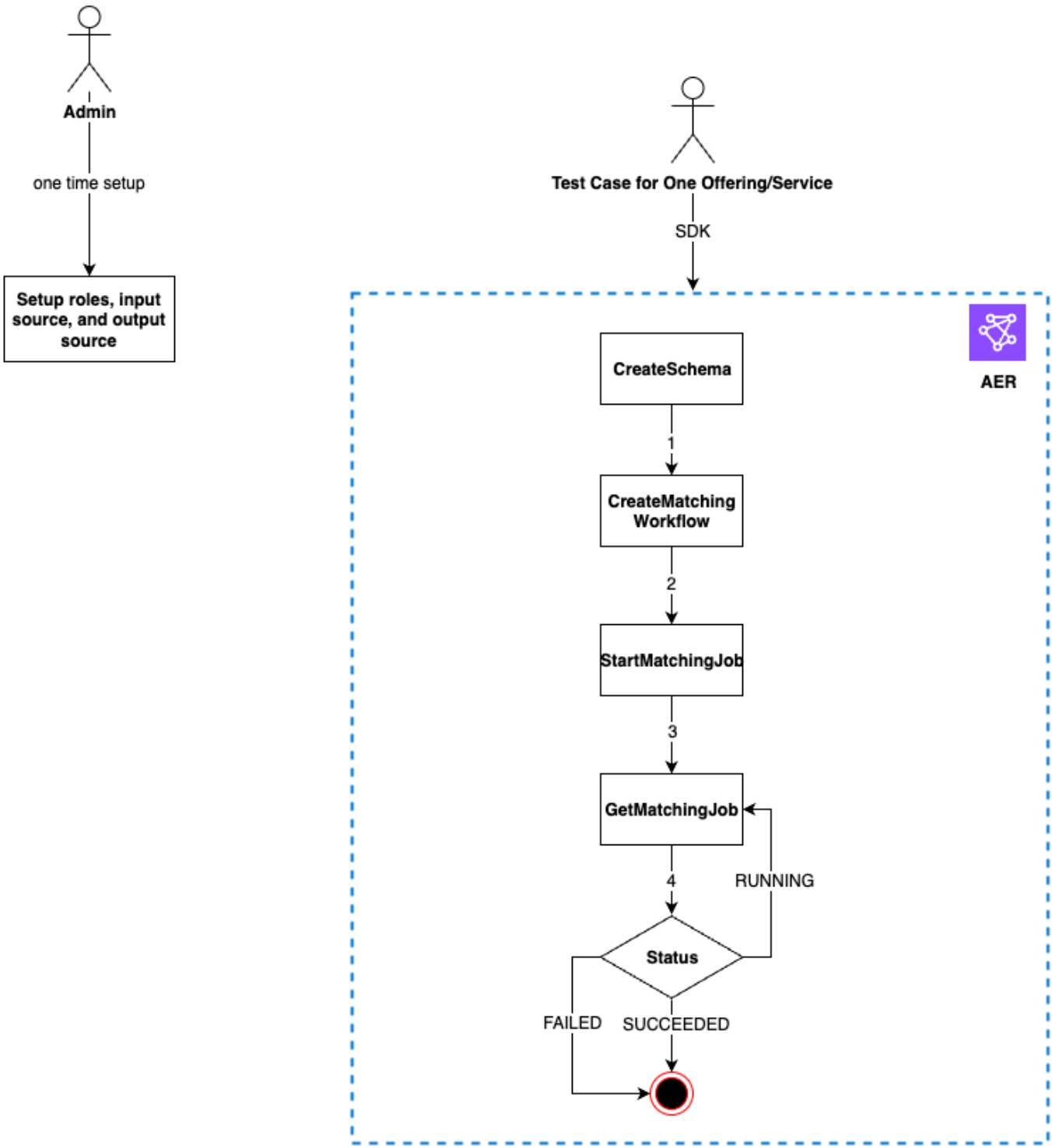
Los proveedores pueden usar sus cuentas de prueba y sus propios datos para ejecutar estos casos de end-to-end prueba mediante el kit de desarrollo de AWS Entity Resolution software (SDK). Si hay algún problema por parte de los proveedores, AWS Entity Resolution utiliza la ruta de escalación preferida para escalar el problema. Además, los proveedores deben implementar su propio monitoreo de los resultados de las pruebas. Los proveedores deben compartir con ellos los Cuenta de AWS IDs que están acostumbrados a realizar estas pruebas AWS Entity Resolution.

Una ejecución correcta significa que el proveedor puede configurar sus datos, utilizar su propio servicio y el AWS Entity Resolution estado del trabajo devuelve el estado Finalizado sin errores. Esto se puede lograr mediante programación utilizando lo APIs proporcionado por. AWS Entity Resolution

Por ejemplo, los proveedores pueden configurar su depósito de S3, la fuente de entrada, las funciones, el esquema y los flujos de trabajo de acuerdo con sus servicios. Una vez completadas estas configuraciones, los proveedores pueden ejecutar estos flujos de trabajo una vez al día con 200 registros para probar su servicio. En este enfoque, los proveedores utilizan el SDK que elijan y realizan una end-to-end prueba para los servicios que ofrecen AWS Data Exchange mediante el uso de sus cuentas de prueba. Se espera que los proveedores realicen estas pruebas para cada una de sus ofertas o servicios.

> **Note**
>
> Los proveedores deben proporcionar AWS Entity Resolution la Cuenta de AWS identificación (`accountId`)que utilizan para ejecutar estos flujos de trabajo) para realizar las pruebas. Además, los proveedores deben monitorear estas pruebas y asegurarse de que se aprueban, lo que significa que los proveedores deben habilitar la notificación en caso de fallas y abordar el problema en consecuencia.

El siguiente diagrama muestra un caso típico de prueba end-to-end de flujo de trabajo.



Para probar la integración de un proveedor

1. (Configuración única) Configure los recursos AWS Entity Resolution siguiendo los procedimientos deConfigurar AWS Entity Resolution.

Una vez que haya completado los procedimientos de configuración únicos, debería tener listos sus funciones, datos y fuente de datos. Ahora está listo para probar la integración del proveedor mediante la AWS Entity Resolution consola o APIs.

2. Pruebe la integración del proveedor mediante la consola AWS Entity Resolution APIs o.

API

Para probar la integración de un proveedor mediante la AWS Entity Resolution APIs

1. Cree un mapeo de esquemas mediante la CreateSchemaMapping API. Para obtener una lista completa de los lenguajes de programación compatibles, consulta la sección Vea también de la CreateSchemaMapping API.

   El mapeo de esquemas es el proceso mediante el cual se indica AWS Entity Resolution cómo interpretar los datos para que coincidan. Usted define el esquema de la tabla de datos de entrada que desea que AWS Entity Resolution lea en un flujo de trabajo coincidente.

   Al crear un mapeo de esquemas, se debe designar y asignar un identificador único a cada fila de datos de entrada que lee AWS Entity Resolution. Por ejemplo, `Primary_key`, `Row_ID`, `Record_ID`.

   Example Crear un esquema de mapeo para una fuente de datos que contenga **`id`** y **`email`**

   El siguiente es un ejemplo de mapeo de esquemas para una fuente de datos que contiene `id` y`email`:

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

Example Crear una asignación de esquemas para una fuente de datos que contenga **`id`** y **`email`** utilice el SDK de Java

El siguiente es un ejemplo de mapeo de esquemas para una fuente de datos que contiene `id` y `email` usa el SDK de Java:

```
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. Cree un flujo de trabajo coincidente mediante la CreateMatchingWorkflow API. Para obtener una lista completa de los lenguajes de programación compatibles, consulta la sección Vea también de la CreateMatchingWorkflow API.

   Example Crear un flujo de trabajo coincidente mediante el SDK de Java

   El siguiente es un ejemplo de un flujo de trabajo coincidente con el SDK de Java:

```
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()

)
```

Una vez configurado el flujo de trabajo correspondiente, puede ejecutar un flujo de trabajo.

3. Ejecute un flujo de trabajo coincidente mediante la StartMatchingJob API. Para ejecutar un flujo de trabajo coincidente, debe haber creado un flujo de trabajo coincidente utilizando el `CreateMatchingWorkflow` punto final.

   Para obtener una lista completa de los lenguajes de programación compatibles, consulta la sección Vea también de la StartMatchingJob API.

   Example Ejecutar un flujo de trabajo coincidente mediante el SDK de Java

   El siguiente es un ejemplo de un flujo de trabajo coincidente en ejecución con el SDK de Java:

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

4. Supervise el estado de un flujo de trabajo mediante la GetMatchingJob API.

   Esta API devuelve el estado, las métricas y los errores (si los hay) asociados a un trabajo.

Example Supervisión de un flujo de trabajo coincidente mediante el SDK de Java

El siguiente es un ejemplo de supervisión de un trabajo de flujo de trabajo coincidente mediante el SDK de Java:

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

La end-to-end prueba se completa si el flujo de trabajo se ha completado correctamente.

Console

Para probar la integración de un proveedor mediante la AWS Entity Resolution consola

1. Cree un mapeo de esquemas siguiendo los pasos que se indican enCrear un esquema de mapeo.

   El mapeo de esquemas es el proceso mediante el cual se indica AWS Entity Resolution cómo interpretar los datos para que coincidan. Usted define el esquema de la tabla de datos de entrada que AWS Entity Resolution desea leer en un flujo de trabajo coincidente.

   Al crear un esquema de mapeo, se debe designar y asignar un identificador único a cada fila de datos de entrada que se AWS Entity Resolution lea. Por ejemplo, `Primary_key`, `Row_ID`, `Record_ID`.

   Example Mapeo de esquemas para una fuente de datos que contiene **`id`** y **`email`**

   El siguiente es un ejemplo de mapeo de esquemas para una fuente de datos que contiene `id` y`email`:

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

```
    "type": "EMAIL_ADDRESS"
  }
]
```

2. Cree y ejecute un flujo de trabajo coincidente siguiendo los pasos que se indican enCrear un flujo de trabajo coincidente basado en los servicios del proveedor.

   La creación de un flujo de trabajo coincidente es el proceso que se configura para especificar los datos de entrada que deben coincidir y cómo se debe realizar la coincidencia. En el flujo de trabajo basado en el proveedor, si una cuenta está suscrita a un proveedor a través del servicio AWS Data Exchange, puedes hacer coincidir tus identificadores conocidos con los de tu proveedor preferido. Según el proveedor y el servicio que utilice para realizar una prueba integral, puede configurar el flujo de trabajo correspondiente en consecuencia.

   La AWS Entity Resolution consola combina las acciones de crear y ejecutar en un solo botón. Tras seleccionar Crear y ejecutar, aparece un mensaje que indica que se ha creado el flujo de trabajo correspondiente y que se ha iniciado el trabajo.
3. Supervise el estado del flujo de trabajo en la página Flujos de trabajo coincidentes.

   La end-to-end prueba se completa si el flujo de trabajo se ha completado correctamente (el estado del trabajo es Completado).

   En la pestaña Métricas de la página de detalles del flujo de trabajo correspondiente, puedes ver lo siguiente en las métricas del último trabajo:

   - El identificador del trabajo.
   - El estado del trabajo de flujo de trabajo coincidente: en cola, en curso, completado, fallido
   - El tiempo de finalización del trabajo de flujo de trabajo.
   - El número de registros procesados.
   - El número de registros no procesados.
   - La coincidencia única IDs generada.
   - El número de registros de entrada.

   También puede ver las métricas de trabajo para hacer coincidir los trabajos de flujo de trabajo que se han ejecutado anteriormente en el historial de trabajos.

Seguridad en AWS Entity Resolution

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Entity Resolution, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por lo Servicio de AWS que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Entity Resolution. Los siguientes temas muestran cómo configurarlo AWS Entity Resolution para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayuden a supervisar y proteger sus AWS Entity Resolution recursos.

Temas

- Protección de datos en AWS Entity Resolution
- Administración de identidad y acceso para AWS Entity Resolution
- Validación de conformidad para AWS Entity Resolution
- Resiliencia en AWS Entity Resolution

Protección de datos en AWS Entity Resolution

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Entity Resolution. Como se describe en este modelo, AWS es responsable de proteger la

infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS Entity Resolution o Servicios de AWS utiliza la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos en reposo para AWS Entity Resolution

AWS Entity Resolution proporciona cifrado de forma predeterminada para proteger los datos confidenciales de los clientes en reposo mediante claves AWS de cifrado propias.

Claves propiedad de AWS: AWS Entity Resolution utiliza estas claves de forma predeterminada para cifrar automáticamente los datos de identificación personal. No puede ver, administrar ni usar las llaves propiedad de AWS ni auditar su uso. Sin embargo, no es necesario que tome ninguna medida para proteger las claves que cifran sus datos. Para obtener más información, consulte las claves propiedad de AWS en la Guía para desarrolladores de AWS Key Management Service .

El cifrado de los datos en reposo de forma predeterminada ayuda a reducir la sobrecarga operativa y la complejidad que implica la protección de los datos confidenciales. Al mismo tiempo, puede utilizarla para crear aplicaciones seguras que cumplan con los estrictos requisitos normativos y de conformidad con el cifrado.

Como alternativa, también puede proporcionar una clave de cifrado de KMS administrada por el cliente al crear el recurso de flujo de trabajo correspondiente.

Claves administradas por el cliente: AWS Entity Resolution admite el uso de una clave KMS simétrica administrada por el cliente que usted crea, posee y administra para permitir el cifrado de sus datos confidenciales. Como usted tiene el control total de este cifrado, puede realizar dichas tareas como:

- Establecer y mantener políticas de claves
- Establecer y mantener concesiones y políticas de IAM
- Habilitar y deshabilitar políticas de claves
- Rotar el material criptográfico
- Agregar etiquetas.
- Crear alias de clave
- Programar la eliminación de claves

Para obtener más información, consulta la clave gestionada por el cliente en la Guía para AWS Key Management Service desarrolladores.

Para obtener más información AWS KMS, consulte ¿Qué es AWS Key Management Service?

Administración de claves

¿Cómo se AWS Entity Resolution utilizan las subvenciones en AWS KMS

AWS Entity Resolution requiere una concesión para utilizar la clave gestionada por el cliente. Al crear un flujo de trabajo coincidente cifrado con una clave gestionada por el cliente, AWS Entity Resolution crea una concesión en tu nombre enviando una CreateGrantsolicitud a AWS KMS. Las concesiones in se AWS KMS utilizan para dar AWS Entity Resolution acceso a una clave de KMS en la cuenta de un cliente. AWS Entity Resolution requiere la autorización para utilizar la clave gestionada por el cliente en las siguientes operaciones internas:

- Envíe GenerateDataKeysolicitudes AWS KMS para generar claves de datos cifradas por su clave gestionada por el cliente.
- Envíe solicitudes de descifrado AWS KMS a para descifrar las claves de datos cifrados para que puedan usarse para cifrar sus datos.

Puede revocar el acceso a la concesión o eliminar el acceso del servicio a la clave administrada por el cliente en cualquier momento. Si lo hace, AWS Entity Resolution no podrá acceder a ninguno de los datos cifrados por la clave gestionada por el cliente, lo que afectará a las operaciones que dependen de esos datos. Por ejemplo, si eliminas el acceso de servicio a tu clave mediante la concesión e intentas iniciar un trabajo para un flujo de trabajo coincidente cifrado con una clave de cliente, la operación devolverá un `AccessDeniedException` error.

Creación de una clave administrada por el cliente

Puede crear una clave simétrica gestionada por el cliente mediante el AWS Management Console, o el AWS KMS APIs.

Para crear una clave simétrica administrada por el cliente

AWS Entity Resolution admite el cifrado mediante claves KMS de cifrado simétrico. Siga los pasos para crear una clave simétrica gestionada por el cliente que se indican en la Guía para desarrolladores de AWS Key Management Service .

Declaración de política clave

Las políticas de clave controlan el acceso a la clave administrada por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave

administrada por el cliente, puede especificar una política de clave. Para obtener más información, consulte Administrar el acceso a las claves administradas por el cliente en la Guía para AWS Key Management Service desarrolladores.

Para utilizar la clave gestionada por el cliente con AWS Entity Resolution los recursos, la política de claves debe permitir las siguientes operaciones de API:

- `kms:DescribeKey`— Proporciona información como el ARN de la clave, la fecha de creación (y la fecha de eliminación, si corresponde), el estado de la clave y la fecha de origen y caducidad (si la hubiera) del material clave. Incluye campos que, por ejemplo`KeySpec`, ayudan a distinguir los distintos tipos de claves de KMS. También muestra el uso de las claves (cifrado, firma o generación y verificación MACs) y los algoritmos que admite la clave KMS. AWS Entity Resolution valida que `KeySpec` es `SYMMETRIC_DEFAULT` y es. `KeyUsage` `ENCRYPT_DECRYPT`
- `kms:CreateGrant`: añade una concesión a una clave administrada por el cliente. Otorga el acceso de control a una clave de KMS específica, que permite el acceso a las operaciones de concesión necesarias AWS Entity Resolution . Para obtener más información sobre el uso de concesiones, consulte la Guía para desarrolladores de AWS Key Management Service .

Esto permite AWS Entity Resolution hacer lo siguiente:

- Llamar a `GenerateDataKey` para generar una clave de datos cifrada y almacenarla, ya que la clave de datos no se utiliza inmediatamente para cifrar.
- Llamar a `Decrypt` para usar la clave de datos cifrados almacenada para acceder a los datos cifrados.
- Configurar una entidad principal que se retire para permitir que el servicio `RetireGrant`.

Los siguientes son ejemplos de declaraciones de política que puede añadir para AWS Entity Resolution:

```
{
      "Sid" : "Allow access to principals authorized to use AWS Entity Resolution",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "*"
      },
      "Action" : ["kms:DescribeKey","kms:CreateGrant"],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "kms:ViaService" : "entityresolution.region.amazonaws.com",
          "kms:CallerAccount" : "111122223333"
        }
      }
}
```

Permisos para los usuarios

Al configurar una clave de KMS como clave de cifrado predeterminada, la política de claves de KMS predeterminada permite a cualquier usuario con acceso a las acciones de KMS necesarias utilizar esta clave de KMS para cifrar o descifrar recursos. Debe conceder a los usuarios permiso para realizar las siguientes acciones a fin de utilizar el cifrado de claves de KMS administrado por el cliente:

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

Durante una `CreateMatchingWorkflow`solicitud, AWS Entity Resolution enviará una DescribeKeyy otra CreateGrantsolicitud AWS KMS en tu nombre. Esto requerirá que la entidad de IAM que realice la `CreateMatchingWorkflow` solicitud con una clave de KMS administrada por el cliente disponga de `kms:DescribeKey` los permisos establecidos en la política de claves de KMS.

Durante una `CreateIdMappingWorkflow` `StartIdMappingJob`solicitud de venta, AWS Entity Resolution enviará una DescribeKeyy una CreateGrantsolicitud a AWS KMS en tu nombre. Para ello, será necesario que la entidad de IAM que realice la `CreateIdMappingWorkflow` `StartIdMappingJob` solicitud con una clave de KMS gestionada por el cliente disponga de `kms:DescribeKey` los permisos establecidos en la política de claves de KMS. Los proveedores podrán acceder a la clave gestionada por el cliente para descifrar los datos del bucket de AWS Entity Resolution Amazon S3.

Los siguientes son ejemplos de declaraciones de políticas que puede añadir para que los proveedores descifren los datos del bucket de AWS Entity Resolution Amazon S3:

JSON

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

Reemplace cada *<user input placeholder>* por su propia información.

<KMSKeyARN>	AWS KMS Nombre del recurso de Amazon.

Del mismo modo, la entidad de IAM que invoca la `StartMatchingJobAPI` debe tener la clave de KMS gestionada por el cliente `kms:Decrypt` y los `kms:GenerateDataKey` permisos correspondientes proporcionados en el flujo de trabajo correspondiente.

Para obtener más información sobre cómo especificar los permisos en una política, consulta la Guía para AWS Key Management Service desarrolladores.

Para obtener más información sobre la solución de problemas de acceso a las claves, consulta la Guía para AWS Key Management Service desarrolladores.

Especificar una clave gestionada por el cliente para AWS Entity Resolution

Puede especificar una clave administrada por el cliente como cifrado de segunda capa para los siguientes recursos:

Flujo de trabajo coincidente: al crear un recurso de flujo de trabajo coincidente, puede especificar la clave de datos introduciendo una KMSArn, que se AWS Entity Resolution utiliza para cifrar los datos personales identificables almacenados en el recurso.

KMSArn— Introduzca una clave ARN, que es un identificador clave para una clave gestionada por el AWS KMS cliente.

Puede especificar una clave gestionada por el cliente como cifrado de segunda capa para los siguientes recursos si va a crear o ejecutar un flujo de trabajo de mapeo de ID en dos de ellos: Cuentas de AWS

Flujo de trabajo de mapeo de ID o flujo de trabajo de mapeo de ID inicial: al crear un recurso de flujo de trabajo de mapeo de ID o iniciar un trabajo de flujo de trabajo de mapeo de ID, puede especificar la clave de datos introduciendo una KMSArn, que se AWS Entity Resolution utiliza para cifrar los datos personales identificables almacenados en el recurso.

KMSArn— Introduzca una clave ARN, que es un identificador clave para una clave gestionada por el AWS KMS cliente.

Supervisión de las claves de cifrado para el servicio AWS Entity Resolution

Cuando utiliza una clave gestionada por el AWS KMS cliente con sus recursos de AWS Entity Resolution servicio, puede utilizar AWS CloudTrail o Amazon CloudWatch Logs para realizar un seguimiento de las solicitudes que se AWS Entity Resolution envía a AWS KMS.

Los siguientes ejemplos son AWS CloudTrail eventos para `CreateGrant` `GenerateDataKeyDecrypt`, y para monitorear AWS KMS las operaciones solicitadas `DescribeKey` para acceder AWS Entity Resolution a los datos cifrados por su clave administrada por el cliente:

Temas

- CreateGrant
- DescribeKey
- GenerateDataKey
- Decrypt

CreateGrant

Cuando utilizas una clave gestionada por el AWS KMS cliente para cifrar el recurso de flujo de trabajo correspondiente, AWS Entity Resolution envía una `CreateGrant` solicitud en tu nombre para acceder a la clave KMS que contiene. Cuenta de AWS La concesión que se AWS Entity Resolution crea es específica del recurso asociado a la clave gestionada por el AWS KMS cliente. Además, AWS Entity Resolution utiliza la `RetireGrant` operación para eliminar una concesión al eliminar un recurso.

El siguiente evento de ejemplo registra la operación `CreateGrant`:


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

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

DescribeKey

AWS Entity Resolution utiliza la `DescribeKey` operación para comprobar si la clave gestionada por el AWS KMS cliente asociada al recurso coincidente existe en la cuenta y la región.

El siguiente evento de ejemplo registra la operación `DescribeKey`.

```
{
    "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

Cuando habilita una clave gestionada por el AWS KMS cliente para el recurso de flujo de trabajo correspondiente, AWS Entity Resolution envía una `GenerateDataKey` solicitud a través de Amazon Simple Storage Service (Amazon S3) AWS KMS en la que se especifica AWS KMS la clave gestionada por el cliente para el recurso.

El siguiente evento de ejemplo registra la operación `GenerateDataKey`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "sharedEventID": "57f5dbee-16da-413e-979f-2c4c6663475e"
}
```

Decrypt

Cuando habilita una clave gestionada por el AWS KMS cliente para el recurso de flujo de trabajo correspondiente, AWS Entity Resolution envía una `Decrypt` solicitud a través de Amazon Simple Storage Service (Amazon S3) AWS KMS en la que se especifica AWS KMS la clave gestionada por el cliente para el recurso.

El siguiente evento de ejemplo registra la operación `Decrypt`.

```
{
    "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"
}
```

Consideraciones

AWS Entity Resolution no admite la actualización de un flujo de trabajo coincidente con una nueva clave de KMS administrada por el cliente. En esos casos, puede crear un nuevo flujo de trabajo con la clave de KMS administrada por el cliente.

Más información

Los siguientes recursos proporcionan más información sobre cifrado de datos en reposo.

Para obtener más información sobre los conceptos básicos de AWS Key Management Service, consulte la Guía para AWS Key Management Service desarrolladores.

Para obtener más información sobre las prácticas recomendadas de seguridad de AWS Key Management Service, consulte la Guía para AWS Key Management Service desarrolladores.

Acceda AWS Entity Resolution mediante un punto final de interfaz (AWS PrivateLink)

Puede usarlo AWS PrivateLink para crear una conexión privada entre su VPC y. AWS Entity Resolution Puede acceder AWS Entity Resolution como si estuviera en su VPC, sin el uso de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect una conexión. Las instancias de la VPC no necesitan direcciones IP públicas para acceder a AWS Entity Resolution.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a AWS Entity Resolution.

Para obtener más información, consulte Acceso Servicios de AWS directo AWS PrivateLink en la AWS PrivateLink Guía.

Consideraciones sobre AWS Entity Resolution

Antes de configurar un punto final de interfaz para AWS Entity Resolution, consulte las consideraciones de la AWS PrivateLink guía.

AWS Entity Resolution permite realizar llamadas a todas sus acciones de API a través del punto final de la interfaz.

Se admiten las políticas de puntos finales de VPC. AWS Entity Resolution De forma predeterminada, se concede acceso completo a AWS Entity Resolution a través del punto de conexión de interfaz. Como alternativa, puede asociar un grupo de seguridad a las interfaces de red del punto de conexión para controlar el tráfico a AWS Entity Resolution a través del punto de conexión de interfaz.

Cree un punto final de interfaz para AWS Entity Resolution

Puede crear un punto final de interfaz para AWS Entity Resolution usar la consola de Amazon VPC o AWS Command Line Interface ()AWS CLI. Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Cree un punto final de interfaz para AWS Entity Resolution usar el siguiente nombre de servicio:

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

Si habilita DNS privado para el punto de conexión de interfaz, puede realizar solicitudes a la API para AWS Entity Resolution usando su nombre de DNS predeterminado para la región. Por ejemplo, `entityresolution.us-east-1.amazonaws.com`.

Creación de una política de puntos de conexión para el punto de conexión de interfaz

Una política de punto de conexión es un recurso de IAM que puede adjuntar al punto de conexión de su interfaz. La política de punto final predeterminada permite el acceso total a AWS Entity Resolution través del punto final de la interfaz. Para controlar el acceso permitido AWS Entity Resolution desde su VPC, adjunte una política de punto final personalizada al punto final de la interfaz.

Una política de punto de conexión especifica la siguiente información:

- Las entidades principales que pueden llevar a cabo acciones (Cuentas de AWS, usuarios de IAM y roles de IAM).
- Las acciones que se pueden realizar.
- El recurso en el que se pueden realizar las acciones.

Para obtener más información, consulte Control del acceso a los servicios con políticas de punto de conexión en la Guía del usuario de AWS PrivateLink .

Ejemplo: política de puntos finales de VPC para acciones AWS Entity Resolution

El siguiente es un ejemplo de una política de un punto de conexión personalizado. Al adjuntar esta política al punto final de la interfaz, se concede acceso a las AWS Entity Resolution acciones enumeradas a todos los principales de todos los recursos.

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

Administración de identidad y acceso para AWS Entity Resolution

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Entity Resolution La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

> **Note**
>
> AWS Entity Resolution admite políticas de cuentas cruzadas. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Temas

- Público

- Autenticación con identidades
- Administración de acceso mediante políticas
- ¿Cómo AWS Entity Resolution funciona con IAM
- Ejemplos de políticas basadas en identidades de AWS Entity Resolution
- AWS políticas gestionadas para AWS Entity Resolution
- Solución de problemas de AWS Entity Resolution identidad y acceso

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS Entity Resolution

Usuario del servicio: si utiliza el AWS Entity Resolution servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS Entity Resolution funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS Entity Resolution, consulte Solución de problemas de AWS Entity Resolution identidad y acceso.

Administrador de servicios: si estás a cargo de AWS Entity Resolution los recursos de tu empresa, probablemente tengas acceso total a ellos AWS Entity Resolution. Su trabajo consiste en determinar a qué AWS Entity Resolution funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM AWS Entity Resolution, consulte¿Cómo AWS Entity Resolution funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS Entity Resolution. Para ver ejemplos de políticas AWS Entity Resolution basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en identidades de AWS Entity Resolution

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor AWS en IAM en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulta Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario

a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puedes crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puedes acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puedes asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puedes utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para

obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulta Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puedes asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades puedes clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas puedes establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puedes conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades

del rol y las políticas de la sesión. Los permisos también puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Entity Resolution funciona con IAM

Antes de utilizar IAM para gestionar el acceso AWS Entity Resolution, infórmese sobre las funciones de IAM disponibles para su uso. AWS Entity Resolution

Funciones de IAM que puede utilizar con AWS Entity Resolution

Característica de IAM	AWS Entity Resolution soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí

Característica de IAM	AWS Entity Resolution soporte
Roles vinculados al servicio	No

Para obtener una visión general de cómo AWS Entity Resolution funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AWS Entity Resolution

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para AWS Entity Resolution

Para ver ejemplos de políticas AWS Entity Resolution basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS Entity Resolution

Políticas basadas en recursos incluidas AWS Entity Resolution

Compatibilidad con las políticas basadas en recursos: sí

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los

administradores de servicios puedes utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para AWS Entity Resolution

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puedes utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de AWS Entity Resolution acciones, consulte las acciones definidas por AWS Entity Resolution en la Referencia de autorización del servicio.

Las acciones políticas AWS Entity Resolution utilizan el siguiente prefijo antes de la acción:

```
entityresolution
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas AWS Entity Resolution basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS Entity Resolution

Recursos de políticas para AWS Entity Resolution

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de AWS Entity Resolution recursos y sus tipos ARNs, consulte los recursos definidos por AWS Entity Resolution en la Referencia de autorización del servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Entity Resolution.

Para ver ejemplos de políticas AWS Entity Resolution basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS Entity Resolution

Claves de condición de la política para AWS Entity Resolution

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una sola clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de AWS Entity Resolution condición, consulte las claves de condición AWS Entity Resolution en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Entity Resolution.

Para ver ejemplos de políticas AWS Entity Resolution basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS Entity Resolution

ACLs in AWS Entity Resolution

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AWS Entity Resolution

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulta Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AWS Entity Resolution

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes

AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS Entity Resolution

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWSél, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

Roles de servicio para AWS Entity Resolution

Compatibilidad con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio puede interrumpir AWS Entity Resolution la funcionalidad. Edite las funciones de servicio solo cuando se AWS Entity Resolution proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AWS Entity Resolution

Compatibilidad con roles vinculados al servicio: no

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya Yes en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades de AWS Entity Resolution

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de AWS Entity Resolution . Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puedes crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos AWS Entity Resolution, incluido el formato ARNs de cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de AWS Entity Resolution la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Mediante la consola de AWS Entity Resolution
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS Entity Resolution recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la

MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de AWS Entity Resolution

Para acceder a la AWS Entity Resolution consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS Entity Resolution recursos de su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la AWS Entity Resolution consola, adjunte también la política *`ReadOnly`* AWS gestionada AWS Entity Resolution *`ConsoleAccess`* o la política gestionada a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "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 políticas gestionadas para AWS Entity Resolution

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSEntity ResolutionConsoleFullAccess

Puede adjuntar la política `AWSEntityResolutionConsoleFullAccess` a las identidades de IAM.

Esta política otorga acceso total a los AWS Entity Resolution puntos finales y los recursos.

Esta política también permite cierto acceso de lectura a temas relacionados, Servicios de AWS como el S3 o el etiquetado AWS Glue, AWS KMS para que la consola pueda mostrar las opciones y utilizar las seleccionadas para realizar acciones de resolución de entidades. Algunos recursos están restringidos para incluir el nombre del servicio. `entityresolution`

Como AWS Entity Resolution se basa en un rol transferido para realizar acciones en AWS los recursos relacionados, esta política también otorga los permisos para seleccionar y transferir el rol deseado.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `EntityResolutionAccess`— Permite a los directores el acceso total a los AWS Entity Resolution puntos finales y los recursos.
- `GlueSourcesConsoleDisplay`— Otorga el acceso a AWS Glue las tablas de listas como opciones de fuentes de datos e importa el esquema de tablas de una fuente de datos para la experiencia del usuario.
- `S3BucketsConsoleDisplay`— Otorga el acceso para enumerar todos los cubos de S3 como opciones de fuente de datos.
- `S3SourcesConsoleDisplay`— Otorga el acceso para mostrar los cubos de S3 como opciones de fuente de datos.
- `TaggingConsoleDisplay`— Otorga el acceso para leer las claves y valores del etiquetado.
- `KMSConsoleDisplay`— Otorga el acceso para describir las claves y enumerar los alias AWS Key Management Service para descifrar y cifrar las fuentes de datos.
- `ListRolesToPickForPassing`— Otorga el acceso a una lista de todos los roles para que el usuario pueda elegir el rol que desea transferir.
- `PassRoleToEntityResolutionService`— Otorga el acceso para transferir un rol reducido al AWS Entity Resolution servicio.

- `ManageEventBridgeRules`— Otorga el acceso para crear, actualizar y eliminar la EventBridge regla de Amazon para recibir notificaciones de S3.
- `ADXReadAccess`— Otorga el acceso AWS Data Exchange para verificar si el cliente tiene un derecho o una suscripción.

Para ver los permisos de esta política, consulte AWSEntityResolutionConsoleFullAccess en la Referencia de la política administrada de AWS .

AWS política gestionada: AWSEntity ResolutionConsoleReadOnlyAccess

Puede adjuntar `AWSEntityResolutionConsoleReadOnlyAccess` a sus entidades de IAM.

Esta política otorga acceso de solo lectura a los AWS Entity Resolution puntos finales y los recursos.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `EntityResolutionRead`— Permite a los directores el acceso de solo lectura a los puntos finales y los recursos. AWS Entity Resolution

Para ver los permisos de esta política, consulte AWSEntityResolutionConsoleReadOnlyAccess en la Referencia de la política administrada de AWS .

AWS Entity Resolution actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Entity Resolution desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS Entity Resolution documento.

Cambio	Descripción	Fecha
`AWSEntityResolutionConsoleFullAccess` : actualización de una política actual	Se agregó `ADXReadAccess` y `ManageEventBridgeRules` habilitó la opción de	16 de octubre de 2023

Cambio	Descripción	Fecha
	servicios del proveedor en el flujo de trabajo correspon diente.	
AWS Entity Resolution comenzó a rastrear los cambios	AWS Entity Resolution comenzó a rastrear los cambios de sus políticas AWS gestionadas.	18 de agosto de 2023

Solución de problemas de AWS Entity Resolution identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con un AWS Entity Resolution IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AWS Entity Resolution
- No estoy autorizado a realizar lo siguiente: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Entity Resolution recursos

No estoy autorizado a realizar ninguna acción en AWS Entity Resolution

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `entityresolution:`*`GetWidget`*.

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

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-widget`* mediante la acción `entityresolution:`*`GetWidget`*.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS Entity Resolution.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Entity Resolution. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Entity Resolution recursos

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan las políticas basadas en recursos o las listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS Entity Resolution es compatible con estas funciones, consulte. ¿Cómo AWS Entity Resolution funciona con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de conformidad para AWS Entity Resolution

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).

- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

AWS Entity Resolution mejores prácticas de cumplimiento

En esta sección se proporcionan las mejores prácticas y recomendaciones para garantizar el cumplimiento cuando se utiliza AWS Entity Resolution.

Normas de seguridad de datos del sector de pagos con tarjeta (PCI DSS)

AWS Entity Resolution admite el procesamiento, el almacenamiento y la transmisión de datos de tarjetas de crédito por parte de un comerciante o proveedor de servicios, y se ha comprobado que cumple con el estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI). Para obtener más información sobre PCI DSS, incluida la forma de solicitar una copia del PCI AWS Compliance Package, consulte PCI DSS Level 1.

Controles del Sistema y Organizaciones (System and Organization Controls, SOC)

AWS Entity Resolution cumple con las medidas de control de sistemas y organizaciones (SOC), incluidas las normas SOC 1, SOC 2 y SOC 3. Los informes del SOC son informes de examen independientes realizados por terceros que demuestran cómo se AWS logran los principales controles y objetivos de cumplimiento. Estas auditorías garantizan que contamos con los mecanismos de seguridad y los procedimientos adecuados para protegernos frente a los riesgos que puedan afectar a la seguridad, la confidencialidad y la disponibilidad de los datos de clientes

y negocios. Los resultados de estas auditorías de terceros están disponibles en el sitio web de cumplimiento del AWS SOC, donde puede consultar los informes publicados para obtener más información sobre los controles que respaldan AWS las operaciones y el cumplimiento.

Resiliencia en AWS Entity Resolution

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, AWS Entity Resolution ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos.

Supervisión AWS Entity Resolution

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS Entity Resolution AWS las demás soluciones. AWS proporciona las siguientes herramientas de monitoreo para observar AWS Entity Resolution, informar cuando algo anda mal y tomar medidas automáticas cuando sea apropiado:

- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por usted o en su nombre Cuenta de AWS y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.
- Amazon CloudWatch Logs te permite comprobar, almacenar y acceder a tus registros desde EC2 instancias de Amazon y otras fuentes. CloudTrail CloudWatch Los registros pueden comprobar la información de los archivos de registro e indicarle cuándo se alcanzan determinados umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.

Temas

Registrar llamadas a la AWS Entity Resolution API mediante AWS CloudTrail

AWS Entity Resolution está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Entity Resolution. CloudTrail captura todas las llamadas a la API AWS Entity Resolution como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Entity Resolution consola y llamadas en código a las operaciones de la AWS Entity Resolution API. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Entity Resolution. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar el destinatario de la

solicitud AWS Entity Resolution, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

AWS Entity Resolution información en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS Entity Resolution, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos para AWS Entity Resolution ti, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas AWS Entity Resolution las acciones se registran CloudTrail y se documentan en la referencia de la AWS Entity Resolution API.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.

- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas de los archivos de AWS Entity Resolution registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Supervisión y registro de flujos de trabajo mediante Amazon CloudWatch Logs

AWS Entity Resolution proporciona funciones de registro completas que le ayudan a comprobar y analizar sus flujos de trabajo de mapeo de coincidencias y de identificación. Mediante la integración con Amazon CloudWatch Logs, puede capturar información detallada sobre la ejecución del flujo de trabajo, incluidos los tipos de eventos, las marcas de tiempo, las estadísticas de procesamiento y los recuentos de errores. Puede elegir enviar estos CloudWatch registros a los destinos de Logs, Amazon S3 o Amazon Data Firehose. Al analizar estos registros, puede evaluar el rendimiento del servicio, solucionar problemas, obtener información sobre su base de clientes y comprender mejor su AWS Entity Resolution uso y facturación. Si bien el registro está desactivado de forma predeterminada, puedes habilitarlo tanto para los flujos de trabajo nuevos como para los existentes a través de la consola o la API.

Cuando habilitas el registro de AWS Entity Resolution flujos de trabajo, se aplican cargos por CloudWatch venta estándar de Amazon, incluidos los costes asociados a la ingesta, el almacenamiento y el análisis de registros. Para obtener información detallada sobre los precios, visita la página de CloudWatch precios. .

Temas

- Configuración de entrega de registros
- Deshabilitar el registro (consola)

- Leyendo los registros

Configuración de entrega de registros

En esta sección se explican los permisos necesarios para utilizar el AWS Entity Resolution registro y cómo habilitar la entrega de registros mediante la consola y APIs.

Temas

- Permisos
- Habilitar el registro para un nuevo flujo de trabajo (consola)
- Habilitar el registro para un nuevo flujo de trabajo (API)
- Habilitar el registro para un flujo de trabajo existente (consola)

Permisos

AWS Entity Resolution utiliza los CloudWatch registros vendidos para entregar el registro del flujo de trabajo. Para entregar los registros del flujo de trabajo, necesita permisos para el destino del registro que especifique.

Para ver los permisos necesarios para cada destino de registro, elige uno de los siguientes AWS servicios en la Guía del usuario de Amazon CloudWatch Logs.

- Amazon CloudWatch Logs
- Amazon Simple Storage Service (Amazon S3)
- Amazon Data Firehose

Para crear, ver o cambiar la configuración de registro AWS Entity Resolution, debe tener los permisos necesarios. Su función de IAM debe incluir los siguientes permisos mínimos para gestionar el registro del flujo de trabajo en la AWS Entity Resolution consola.

JSON

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

```
            "Sid": "AllowLogDeliveryActionsConsoleCWL",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:log-group:*"
            ]
        },
        {
            "Sid": "AllowLogDeliveryActionsConsoleS3",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "AllowLogDeliveryActionsConsoleFH",
            "Effect": "Allow",
            "Action": [
                "firehose:ListDeliveryStreams",
                "firehose:DescribeDeliveryStream"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Para obtener más información sobre los permisos para gestionar el registro del flujo de trabajo, consulte Habilitar el registro desde AWS los servicios en la Guía del usuario de Amazon CloudWatch Logs.

Habilitar el registro para un nuevo flujo de trabajo (consola)

Después de configurar los permisos para el destino del registro, puede habilitar el registro para un nuevo flujo de trabajo AWS Entity Resolution mediante la consola.

Para habilitar el registro de un nuevo flujo de trabajo (consola)

1. Abre la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/casa.
2. En Flujos de trabajo, selecciona Flujos de trabajo coincidentes o Flujos de trabajo de mapeo de ID.
3. Siga los pasos para crear uno de los siguientes flujos de trabajo:
   - Flujo de trabajo de coincidencia basado en reglas
   - Flujo de trabajo de emparejamiento basado en el aprendizaje automático
   - Flujo de trabajo de emparejamiento basado en servicios de proveedores
   - Flujo de trabajo de mapeo de ID para una cuenta
   - Flujo de trabajo de mapeo de ID en dos cuentas
4. En el paso 1, especifique los detalles del flujo de trabajo coincidentes, en Entregas de registros: registros del EntityResolution flujo de trabajo, elija Agregar.
   - Elija uno de los siguientes destinos de registro.
     - A Amazon CloudWatch Logs
     - A Amazon S3
     - Hacia Amazon Data Firehose

> **Tip**
>
> Si eliges Amazon S3 o Firehose, puedes enviar tus registros a una cuenta Cross o a una cuenta corriente In.
> Para habilitar la entrega entre cuentas, ambas Cuentas de AWS deben tener los permisos necesarios. Para obtener más información, consulta el ejemplo de entrega entre cuentas en la Guía del usuario de Amazon CloudWatch Logs.

5. En el caso del grupo de registros de destino, los grupos de registros que tienen el prefijo «/aws/vendedlogs/» se crean automáticamente. Si utiliza otros grupos de registros, selecciónelos antes de configurar una entrega de registros. Para obtener más información, consulte Trabajar con grupos de registros y transmisiones de CloudWatch registros en la Guía del usuario de Amazon Logs.
6. Para ver más ajustes (opcional), elige lo siguiente:
   a. En Selección de campos, seleccione los campos de registro que desee incluir en cada registro de registro.
   b. (CloudWatch Registros) En el formato de salida, elija el formato de salida del registro.
   c. En Delimitador de campos, elija cómo separar cada campo de registro.
   d. (Amazon S3) En Sufijo, especifique la ruta del sufijo para particionar los datos.
   e. (Amazon S3) Si es compatible con HIVE, seleccione Activar si desea utilizar rutas S3 compatibles con HIVE.
7. Para crear otro destino de registro, elija Agregar y repita los pasos 4 a 6.
8. Complete los pasos restantes para configurar y ejecutar el flujo de trabajo.
9. Una vez finalizados los trabajos del flujo de trabajo, compruebe los registros del flujo de trabajo en el destino de entrega de registros que especificó.

Habilitar el registro para un nuevo flujo de trabajo (API)

Después de configurar los permisos para el destino del registro, puede habilitar el registro para un nuevo flujo de trabajo AWS Entity Resolution mediante Amazon CloudWatch Logs APIs.

Para habilitar el registro de un nuevo flujo de trabajo (API)

1. Tras crear un flujo de trabajo en la AWS Entity Resolution consola, obtenga el nombre de recurso de Amazon (ARN) del flujo de trabajo.

   Puede encontrar el ARN en la página de flujo de trabajo de la AWS Entity Resolution consola o puede llamar a la operación `GetMatchingWorkflow` o `GetIdMappingWorkflow` API.

   Un ARN de flujo de trabajo sigue este formato:

   ```
   arn:(aws|aws-us-gov|aws-cn):entityresolution:[a-z]{2}-[a-z]{1,10}-[0-9]:[0-9]{12}:(matchingworkflow/[a-zA-Z_0-9-]{1,255})
   ```

Un ARN de mapeo de ID sigue este formato:

```
arn:(aws|aws-us-gov|aws-cn):entityresolution:[a-z]{2}-[a-z]{1,10}-
[0-9]:[0-9]{12}:(idmappingworkflow/[a-zA-Z_0-9-]{1,255})
```

Para obtener más información consulte GetMatchingWorkflow o GetIdMappingWorkflow en la Referencia de la API de AWS Entity Resolution .

2. Utilice la operación de la `PutDeliverySource` API de CloudWatch registros para crear una fuente de entrega para los registros del flujo de trabajo.

   Para obtener más información, consulta PutDeliverySourcela referencia de la API CloudWatch de Amazon Logs.

   a. Pase el`resourceArn`.

   b. Pues`logType`, los tipos de registros que se recopilan son`WORKFLOW_LOGS`:

   Example

   Ejemplo de operación `PutDeliverySource` de API

   ```
   {
       "logType": "WORKFLOW_LOGS",
       "name": "my-delivery-source",
       "resourceArn": "arn:aws:entityresolution:region:accoungId:matchingworkflow/
   XXXWorkflow"
   }
   ```

3. Utilice la operación de `PutDeliveryDestination` API para configurar dónde almacenar los registros.

   Puede elegir CloudWatch Logs, Amazon S3 o Firehose como destino. Debe especificar el ARN de una de las opciones de destino en las que se almacenarán los registros.

   Para obtener más información, consulta PutDeliveryDestinationla referencia de la API CloudWatch de Amazon Logs.

   Example

   Ejemplo de operación `PutDeliveryDestination` de API

```
{
   "delivery-destination-configuration": {
      "destinationResourceArn": "arn:aws:logs:region:accountId:log-group:my-log-
group"
   },
   "name": "my-delivery-destination",
   "outputFormat": "json",
   }
}
```

> **Note**
>
> Si entrega registros entre cuentas, debe usar la PutDeliveryDestinationPolicyAPI para asignar una política AWS Identity and Access Management (IAM) a la cuenta de destino. La política de IAM permite la entrega de una cuenta a otra.

4. Usa la operación de la `CreateDelivery` API para vincular la fuente de entrega al destino que creaste en los pasos anteriores. Esta operación de la API asocia el origen de la entrega con el destino final.

   Para obtener más información, consulta PutDeliveryDestinationla referencia de la API CloudWatch de Amazon Logs.

   Example

   Ejemplo de operación `CreateDelivery` de API

   ```
   {
      "delivery-destination-arn": "arn:aws:logs:region:accountId:log-group:my-log-
   group",
      "delivery-source-name": "my-delivery-source",
      "tags": {
         "string" : "string"
      }
   }
   ```

5. Ejecute el flujo de trabajo.
6. Una vez finalizados los trabajos del flujo de trabajo, compruebe los registros del flujo de trabajo en el destino de entrega de registros que especificó.

Habilitar el registro para un flujo de trabajo existente (consola)

Después de configurar los permisos para el destino del registro, puede habilitar el registro para un flujo de trabajo existente AWS Entity Resolution mediante la pestaña Entregas de registros de la consola.

Para habilitar el registro de un flujo de trabajo existente mediante la pestaña Entregas de registros (consola)

1. Abre la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/casa.
2. En Flujos de trabajo, selecciona Flujos de trabajo coincidentes o Flujos de trabajo de mapeo de ID y, a continuación, selecciona tu flujo de trabajo actual.
3. En la pestaña Entregas de registros, en Entrega de registros, selecciona Agregar y, a continuación, elige uno de los siguientes destinos de registro.

   - A Amazon CloudWatch Logs
   - A Amazon S3
     - Entre cuentas
     - En la cuenta actual
   - Hacia Amazon Data Firehose
     - Entre cuentas
     - En la cuenta actual

   > **Tip**
   >
   > Si eliges Amazon S3 o Firehose, puedes enviar tus registros a una cuenta Cross o a una cuenta corriente In.
   > Para habilitar la entrega entre cuentas, ambas Cuentas de AWS deben tener los permisos necesarios. Para obtener más información, consulta el ejemplo de entrega entre cuentas en la Guía del usuario de Amazon CloudWatch Logs.

4. En el modo modal, haz lo siguiente, según el tipo de entrega de registros que hayas elegido.

   a. Vea el tipo de registro: WORKFLOW_LOGS.

      El tipo de registro no se puede cambiar.

b. (CloudWatch Registros) Para el grupo de registros de destino, los grupos de registros que tienen el prefijo '/aws/vendedlogs/' se crean automáticamente. Si utiliza otros grupos de registros, selecciónelos antes de configurar la entrega de registros. Para obtener más información, consulte Trabajar con grupos de registros y transmisiones de CloudWatch registros en la Guía del usuario de Amazon Logs.

   (Amazon S3 en la cuenta corriente) Para el bucket S3 de Destination, seleccione un bucket o introduzca un ARN.

   (Cuenta cruzada de Amazon S3) Para el ARN de destino de entrega, introduzca un ARN de destino de entrega.

   (Firehose en la cuenta corriente) En el flujo de entrega de destino, introduzca el ARN del recurso de destino de entrega que se creó en otra cuenta.

   (Cuenta cruzada de Firehose) Para el ARN de destino de entrega, introduzca un ARN de destino de entrega.

5. Para obtener más ajustes (opcional), elija lo siguiente:

   a. En Selección de campos, seleccione los campos de registro que desee incluir en cada registro de registro.

   b. (CloudWatch Registros) En el formato de salida, elija el formato de salida del registro.

   c. En Delimitador de campos, elija cómo separar cada campo de registro.

   d. (Amazon S3) En Sufijo, especifique la ruta del sufijo para particionar los datos.

   e. (Amazon S3) Si es compatible con HIVE, seleccione Activar si desea utilizar rutas S3 compatibles con HIVE.

6. Elija Agregar.

7. En la página del flujo de trabajo, elija Ejecutar.

8. Una vez finalizados los trabajos del flujo de trabajo, compruebe los registros del flujo de trabajo en el destino de entrega de registros que especificó.

Deshabilitar el registro (consola)

Puede deshabilitar el registro de su AWS Entity Resolution flujo de trabajo en cualquier momento en la consola.

Para deshabilitar el registro del flujo de trabajo (consola)

1. Abre la AWS Entity Resolution consola en https://console.aws.amazon.com/entityresolution/casa.
2. En Flujos de trabajo, selecciona Flujos de trabajo coincidentes o Flujos de trabajo de mapeo de ID y, a continuación, selecciona tu flujo de trabajo.
3. En la pestaña Entregas de registros, en Entrega de registros, selecciona el destino y, a continuación, selecciona Eliminar.
4. Revisa los cambios y, a continuación, ve al paso siguiente para guardarlos.

Leyendo los registros

La lectura de Amazon CloudWatch Logs le ayuda a mantener AWS Entity Resolution flujos de trabajo eficientes. Los registros ofrecen una visibilidad detallada de la ejecución del flujo de trabajo, incluidas métricas importantes, como la cantidad de registros procesados y los errores encontrados, lo que le ayuda a garantizar que el procesamiento de datos se ejecute sin problemas. Además, los registros ofrecen un seguimiento en tiempo real de la progresión del flujo de trabajo mediante marcas de tiempo y tipos de eventos, lo que le permite identificar rápidamente los cuellos de botella o los problemas en su proceso de procesamiento de datos. La completa información sobre el seguimiento de errores y el recuento de registros le ayuda a mantener la calidad y la integridad de los datos, ya que muestra exactamente cuántos registros se procesaron correctamente y si alguno quedó sin procesar.

Si usa CloudWatch Logs como destino, puede usar Logs Insights para leer CloudWatch los registros del flujo de trabajo. Se aplican CloudWatch los cargos típicos de Logs. Para obtener más información, consulte Análisis de datos de registro con CloudWatch Logs Insights en la Guía del usuario de Amazon CloudWatch Logs.

> **Note**
>
> Los registros del flujo de trabajo pueden tardar unos minutos en aparecer en su destino. Si no ve los registros, espere unos minutos y actualice la página.

Los registros del flujo de trabajo constan de una secuencia de registros formateados, en la que cada registro representa un flujo de trabajo. El orden de los campos en el registro puede variar.

```
{
  "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-ingress-point/inp-
xxxxx",
  "event_type": "JOB_START",
  "event_timestamp": 1728562395042,
  "job_id": "b01eea4678d4423a4b43eeada003f6",
  "workflow_name": "TestWorkflow",
  "workflow_start_time": "2025-03-11 10:19:56",
  "data_procesing_progression": "Matching Job Starts ...",
  "total_records_processed": 1500,
  "total_records_unprocessed": 0,
  "incremental_records_processed": 0,
  "error_message": "sample error that caused workflow failure"
}
```

En la siguiente lista, se describen los campos de entrada de registro en orden:

`resource_arn`

El nombre del recurso de Amazon (ARN) que identifica de forma exclusiva el AWS recurso que se utiliza en el flujo de trabajo.

`event_type`

El tipo de evento que se produjo durante la ejecución del flujo de trabajo. AWS Entity Resolution actualmente admite:

`JOB_START`

`DATA_PROCESSING_STEP_START`

`DATA_PROCESSING_STEP_END`

`JOB_SUCCESS`

`JOB_FAILURE`

`event_timestamp`

La marca de tiempo de Unix que indica cuándo se produjo el evento durante el flujo de trabajo.

`job_id`

Un identificador único asignado a la ejecución de un trabajo de flujo de trabajo específico.

`workflow_name`

El nombre dado al flujo de trabajo que se está ejecutando.

`workflow_start_time`

La fecha y la hora en que se inició la ejecución del flujo de trabajo.

`data_procesing_progression`

Descripción de la etapa actual del flujo de trabajo de procesamiento de datos. Ejemplos: `"Matching Job Starts"`, `"Loading Step Starts"`, `"ID_Mapping Job Ends Successfully"`.

`total_records_processed`

El número total de registros que se procesaron correctamente durante el flujo de trabajo.

`total_records_unprocessed`

El número de registros que no se procesaron durante la ejecución del flujo de trabajo.

`incremental_records_processed`

El número de registros nuevos procesados en una actualización incremental del flujo de trabajo.

`error_message`

La causa principal del error del flujo de trabajo.

Cree recursos de resolución de entidades de AWS con AWS CloudFormation

AWS Entity Resolution está integrado con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Cree una plantilla que describa todos los AWS recursos que desee (por ejemplo, AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace y AWS::EntityResolution::PolicyStatement) y los AWS CloudFormation aprovisione y configure automáticamente.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar los recursos de AWS Entity Resolution de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos una y otra vez en varias Cuentas de AWS regiones.

Resolución y AWS CloudFormation plantillas de entidades de AWS

Para aprovisionar y configurar recursos para AWS Entity Resolution y los servicios relacionados, debe conocer AWS CloudFormation las plantillas. Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus AWS CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar AWS CloudFormation Designer para ayudarte a empezar con AWS CloudFormation las plantillas. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation ? en la Guía del usuario de AWS CloudFormation .

AWS Entity Resolution admite la creación AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace y AWS::EntityResolution::PolicyStatement el ingreso AWS CloudFormation. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace y AWS::EntityResolution::PolicyStatement, consulte la referencia de tipos de recursos de AWS Entity Resolution en la Guía del AWS CloudFormation usuario.

Están disponibles las siguientes plantillas:

- Flujo de trabajo correspondiente

Cree un `MatchingWorkflow` objeto que almacene la configuración del trabajo de procesamiento de datos que se va a ejecutar.

Para obtener más información, consulte los temas siguientes:

AWS::EntityResolution::MatchingWorkflow en la Guía del usuario de AWS CloudFormation .

CreateMatchingWorkflow en la Referencia de la API de AWS Entity Resolution

- Mapeo de esquemas

  Cree un mapeo de esquemas, que defina el esquema de la tabla de registros de clientes de entrada.

  Para obtener más información, consulte los temas siguientes:

  AWS::EntityResolution::SchemaMapping en la Guía del usuario de AWS CloudFormation .

  CreateSchemaMapping en la Referencia de la API de AWS Entity Resolution

- Flujo de trabajo de mapeo

  Cree un `IdMappingWorkflow` objeto que almacene la configuración del trabajo de procesamiento de datos que se va a ejecutar.

  Para obtener más información, consulte los temas siguientes:

  AWS::EntityResolution::IdMappingWorkflow en la Guía del usuario de AWS CloudFormation .

  CreateIdMappingWorkflow en la Referencia de la API de AWS Entity Resolution

- ID (espacio de nombres)

  Cree un `IdNamespace` objeto que almacene los metadatos que explican el conjunto de datos y cómo usarlo.

  Para obtener más información, consulte los temas siguientes:

  AWS::EntityResolution::IdNamespace en la Guía del usuario de AWS CloudFormation .

  CreateIdNamespace en la Referencia de la API de AWS Entity Resolution

- PolicyStatement

Cree un objeto `PolicyStatement`.

Para obtener más información, consulte los temas siguientes:

AWS::EntityResolution::PolicyStatement en la Guía del usuario de AWS CloudFormation .

AddPolicyStatement en la Referencia de la API de AWS Entity Resolution

Obtenga más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormation Guía del usuario
- Referencia de la API de AWS CloudFormation
- AWS CloudFormation Guía del usuario de la interfaz de línea de comandos

Cuotas para AWS Entity Resolution

Cuenta de AWS Tiene cuotas predeterminadas, antes denominadas límites, para cada una de ellas Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región. Puedes solicitar aumentos para algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas AWS Entity Resolution, abra la consola Service Quotas. En el panel de navegación, elija Servicios de AWS y seleccione AWS Entity Resolution.

Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si la cuota aún no se encuentra disponible en Service Quotas, utilice el formulario de aumento del límite.

Cuenta de AWS Tiene las siguientes cuotas relacionadas con AWS Entity Resolution.

Nombre	Valor predeterminado	Ajusta	Descripción
Trabajos de mapeo de ID simultáneos	Cada región admitida: 1	No	El número máximo de flujos de trabajo de mapeo de ID que se pueden procesar simultáneamente en la región actual AWS .
Trabajos coincidentes simultáneos	Cada región admitida: 1	No	El número máximo de flujos de trabajo coincidentes que se pueden procesar simultáneamente en la región actual AWS .
Servicios de proveedores simultáneos que coinciden con los trabajos	Cada región admitida: 1	No	El número máximo de flujos de trabajo coincidentes con los servicios del proveedor que se pueden procesar simultáne

Nombre	Valor predeterminado	Ajusta	Descripción
			amente en la región actual AWS .
Flujos de trabajo de mapeo	Cada región admitida: 10	Sí	El número máximo de flujos de trabajo de mapeo de ID que puede crear en esta cuenta en la AWS región actual.
Espacios de nombres de ID	Cada región admitida: 10	Sí	El número máximo de espacios de nombres de ID que puedes crear en esta cuenta en la región actual AWS .
Flujos de trabajo compatibles	Cada región admitida: 10	Sí	El número máximo de flujos de trabajo coincidentes que puede crear en esta cuenta en la AWS región actual.
Tasa de solicitudes de GenerateMatchId API	Cada región admitida: 10	Sí	El número máximo de solicitudes de GenerateMatchId API por segundo
Tasa de solicitudes a GetMatchId la API	Cada región admitida: 50	Sí	El número máximo de solicitudes de GetMatchId API por segundo.

Nombre	Valor predeterminado	Ajustable	Descripción
Registros por flujo de trabajo coincidente basado en el aprendizaje automático	Cada región compatible: 150 000 000	Sí	El número máximo de registros que puede procesar un flujo de trabajo de emparejamiento basado en el aprendizaje automático en esta cuenta en AWS las regiones de af-south-1, ap-northeast-2 y eu-west-2.
Registros por flujo de trabajo coincidente basado en el aprendizaje automático	Cada región compatible: 600 000 000	Sí	El número máximo de registros que puede procesar un flujo de trabajo de coincidencia basado en el aprendizaje automático en esta cuenta en las AWS regiones de ap-northeast-1, ap-southeast-1, ap-southeast-2, ca-central-1, eu-central-1, eu-central-1, eu-west-1, us-east-1, us-east-1, us-east-1, us-east-1, us-Este-2, us-west-2.

Nombre	Valor predeterminado	Ajusta	Descripción
Flujo de trabajo de mapeo de ID de registros por proveedor	Cada región compatible: 150 000 000	Sí	El número máximo de registros que se pueden procesar para la asignación de ID de proveedor en esta cuenta en AWS las regiones af-south-1, ap-northeast-2 y eu-west-2.
Flujo de trabajo de mapeo de ID de registros por proveedor	Cada región compatible: 250 000 000	Sí	El número máximo de registros que se pueden procesar para la asignación de ID de proveedor en esta cuenta en AWS las regiones de ap-northeast-1, ap-southeast-1, ap-southeast-2, ca-central-1, eu-central-1, eu-central-1, eu-west-1, us-east-1, us-east-1, us-east-2, us-west-2.
Flujo de trabajo coincidente basado en el servicio de cada proveedor	Cada región admitida: 100 000 000	Sí	El número máximo de registros que puede procesar un flujo de trabajo coincidente basado en el servicio del proveedor en esta cuenta en la región actual AWS .

Nombre	Valor predeterminado	Ajusta	Descripción
Registros por flujo de trabajo de mapeo de ID basado en reglas	Cada región compatible: 1 000 000 000	Sí	El número máximo de registros que se pueden procesar para la asignación de ID basada en reglas en esta cuenta en AWS las regiones de ap-northeast-1, ap-southeast-1, ap-southeast-2, ca-central-1, eu-central-1, eu-central-1, eu-west-1, us-east-1, us-east-1, us-east-2 us-west-2, us-west-2.
Registros por flujo de trabajo de mapeo de ID basado en reglas	Cada región compatible: 150 000 000	Sí	El número máximo de registros que se pueden procesar para el mapeo de ID basado en reglas en esta cuenta en AWS las regiones af-south-1, ap-northeast-2 y eu-west-2.
Registros por flujo de trabajo coincidente basado en reglas	Cada región admitida: 100 000 000	Sí	El número máximo de registros que puede procesar un flujo de trabajo de coincidencia basado en reglas en esta cuenta en la región actual. AWS

Nombre	Valor predeterminado	Ajusta	Descripción
Mapeos de esquemas	Cada región admitida: 50	Sí	El número máximo de mapeos de esquemas que puede crear en esta cuenta en la región actual. AWS

Cuotas de limitación controlada de la API

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `CreateMatchingWorkflow`	5 TPS	Número máximo de llamadas a la `CreateMatchingWorkflow` API por segundo.
Tasa de solicitudes `DeleteMatchingWorkflow`	5 TPS	Número máximo de llamadas a la `DeleteMatchingWorkflow` API por segundo.
Tasa de solicitudes `GetMatchingWorkflow`	5 TPS	Número máximo de llamadas a la `GetMatchingWorkflow` API por segundo.
Tasa de solicitudes `ListMatchingWorkflows`	5 TPS	Número máximo de llamadas a la `ListMatchingWorkflows` API por segundo.
Tasa de solicitudes `UpdateMatchingWorkflow`	5 TPS	Número máximo de llamadas a la `UpdateMatchingWorkflow` API por segundo.
Tasa de solicitudes `CreateSchemaMapping`	5 TPS	Número máximo de llamadas a la `CreateSchemaMapping` API por segundo.

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `DeleteSchemaMapping`	5 TPS	Número máximo de llamadas a la `DeleteSchemaMapping` API por segundo.
Tasa de solicitudes `GetSchemaMapping`	5 TPS	Número máximo de llamadas a la `GetSchemaMapping` API por segundo.
Tasa de solicitudes `ListSchemaMappings`	5 TPS	Número máximo de llamadas a la `ListSchemaMappings` API por segundo.
Tasa de solicitudes `UpdateSchemaMapping`	5 TPS	Número máximo de llamadas a la `UpdateSchemaMapping` API por segundo.
Tasa de solicitudes `GetPartnerComponent`	5 TPS	Número máximo de llamadas a la `GetPartnerComponent` API por segundo.
Tasa de solicitudes `ListPartnerComponents`	5 TPS	Número máximo de llamadas a la `ListPartnerComponents` API por segundo.
Tasa de solicitudes `TagResource`	5 TPS	Número máximo de llamadas a la `TagResource` API por segundo.
Tasa de solicitudes `UntagResource`	5 TPS	Número máximo de llamadas a la `UntagResource` API por segundo.
Tasa de solicitudes `ListTagsForResource`	5 TPS	Número máximo de llamadas a la `ListTagsForResource` API por segundo.

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `CreateIdMappingWorkflow`	5 TPS	Número máximo de llamadas a la `CreateIdMappingWorkflow` API por segundo.
Tasa de solicitudes `DeleteIdMappingWorkflow`	5 TPS	Número máximo de llamadas a la `DeleteIdMappingWorkflow` API por segundo.
Tasa de solicitudes `GetIdMappingWorkflow`	5 TPS	Número máximo de llamadas a la `GetIdMappingWorkflow` API por segundo.
Tasa de solicitudes `ListIdMappingWorkflow`	5 TPS	Número máximo de llamadas a la `ListIdMappingWorkflow` API por segundo.
Tasa de solicitudes `UpdateIdMappingWorkflow`	5 TPS	Número máximo de llamadas a la `UpdateIdMappingWorkflow` API por segundo.
Tasa de solicitudes `ListProviderServices`	5 TPS	Número máximo de llamadas a la `ListProviderServices` API por segundo.
Tasa de solicitudes `GetProviderService`	5 TPS	Número máximo de llamadas a la `GetProviderService` API por segundo.
Tasa de solicitudes `CreateIdNamespace`	5 TPS	Número máximo de llamadas a la `CreateIdNamespace` API por segundo.
Tasa de solicitudes `DeleteIdNamespace`	5 TPS	Número máximo de llamadas a la `DeleteIdNamespace` API por segundo.

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `GetIdNamespace`	5 TPS	Número máximo de llamadas a la `GetIdNamespace` API por segundo.
Tasa de solicitudes `ListIdNamespaces`	5 TPS	Número máximo de llamadas a la `ListIdNamespaces` API por segundo.
Tasa de solicitudes `UpdateIdNamespace`	5 TPS	Número máximo de llamadas a la `UpdateIdNamespace` API por segundo.
Tasa de solicitudes `AddPolicyStatement`	5 TPS	Número máximo de llamadas a la `AddPolicyStatement` API por segundo.
Tasa de solicitudes `DeletePolicyStatement`	5 TPS	Número máximo de llamadas a la `DeletePolicyStatement` API por segundo.
Tasa de solicitudes `GetPolicy`	5 TPS	Número máximo de llamadas a la `GetPolicy` API por segundo.
Tasa de solicitudes `PutPolicy`	5 TPS	Número máximo de llamadas a la `PutPolicy` API por segundo.
Tasa de solicitudes `GetMatchingJob`	10 TPS	Número máximo de llamadas a la `GetMatchingJob` API por segundo.
Tasa de solicitudes `ListMatchingJobs`	5 TPS	Número máximo de llamadas a la `ListMatchingJobs` API por segundo.

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `StartMatchingJob`	5 TPS	Número máximo de llamadas a la `StartMatchingJob` API por segundo.
Tasa de solicitudes `GetMatchId`	50 TPS	Número máximo de llamadas a la `GetMatchId` API por segundo.
Tasa de solicitudes `GetIdMappingJob`	10 TPS	Número máximo de llamadas a la `GetIdMappingJob` API por segundo.
Tasa de solicitudes `ListIdMappingJobs`	5 TPS	Número máximo de llamadas a la `ListIdMappingJobs` API por segundo.
Tasa de solicitudes `StartIdMappingJob`	5 TPS	Número máximo de llamadas a la `StartIdMappingJob` API por segundo.
Tasa de solicitudes `BatchDeleteUniqueId`	5 TPS	Número máximo de llamadas a la `BatchDeleteUniqueId` API por segundo.

Historial de documentos de la Guía AWS Entity Resolution del usuario

En la siguiente tabla se describen las versiones de la documentación de AWS Entity Resolution.

Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a la fuente RSS. Para suscribirse a las actualizaciones RSS, debe tener un complemento de RSS habilitado para el navegador que esté utilizando.

Cambio	Descripción	Fecha
Clarificación del procesamiento de Match ID	Se ha añadido una aclaración de que las opciones Modificar o generar el ID de coincidencia y Buscar el ID de coincidencia requieren una cadencia de procesamiento automática en los flujos de trabajo coincidentes.	17 de julio de 2025
Genera un nuevo identificador de coincidencia	Los clientes ahora pueden buscar y modificar una ID de coincidencia existente o generar una nueva ID de coincidencia al utilizar un flujo de trabajo de coincidencia basado en reglas.	2 de junio de 2025
Flujo de trabajo de búsqueda de coincidencias basado en el servicio del proveedor	Los clientes ahora pueden usar identificadores digitales como IPV4 IPV6, y MAID cuando utilizan el flujo de trabajo de búsqueda de coincidencias basado en los servicios del TransUnion proveedor.	21 de abril de 2025

Amazon CloudWatch Logs	AWS Entity Resolution ahora es compatible con la integración de CloudWatch Logs, lo que le permite habilitar un registro detallado del flujo de trabajo que captura las métricas de ejecución de tareas, los tiempos y las estadísticas de procesamiento que se pueden enviar a CloudWatch los destinos de Logs, Amazon S3 o Amazon Data Firehose.	14 de abril de 2025
Flujo de trabajo de mapeo de ID: actualización	Los clientes ahora pueden configurar la AWS Glue partición cuando utilizan un flujo de trabajo de mapeo de ID.	25 de marzo de 2025
Cuotas: actualización	Actualización de la documentación unicamente. Los flujos de trabajo de coincidencia basados en reglas pueden procesar hasta 100 millones de registros, mientras que los flujos de trabajo de coincidencia basados en el aprendizaje automático pueden procesar hasta 250 millones de registros. Los clientes que necesiten límites más altos deben ponerse en contacto con el equipo de servicio.	7 de febrero de 2025

Mapeo de esquemas: actualización	Actualización solo de la documentación para aclarar que la normalización es compatible con los tipos de atributos de nombre completo, dirección completa y teléfono completo.	17 de enero de 2025
Integración de proveedores	Actualización de la documentación unicamente. Los clientes pueden aprender cómo integrarse como un proveedor de servicios con AWS Entity Resolution.	8 de agosto de 2024
Flujo de trabajo de mapeo de identidad: actualización	Los clientes ahora pueden usar reglas de coincidencia para traducir datos propios en un flujo de trabajo de mapeo de identidades.	23 de julio de 2024
Flujo de trabajo coincidente: actualización	Los clientes ahora pueden eliminar los registros de un flujo de trabajo coinciden te basado en reglas o en aprendizaje automático para ayudar a cumplir con las normas de administración de datos.	8 de abril de 2024
Flujo de trabajo de mapeo de identidad: actualización	Los clientes ahora pueden usar un flujo de trabajo de mapeo de ID en varios Cuentas de AWS.	2 de abril de 2024

AWS CloudFormation Recursos: recursos nuevos y actualizados	AWS Entity Resolution ha agregado los siguiente s recursos: `AWS::Enti tyResolution::IdNa mespace` `AWS::Enti tyResolution::Poli cyStatement` y ha actualizado el siguiente recurso:`AWS::Enti tyResolution::IdMa ppingWorkflow` .	2 de abril de 2024
Encuentra el ID de coinciden cia	Los clientes ahora pueden encontrar el ID de coinciden cia correspondiente y la regla asociada para un flujo de trabajo procesado basado en reglas.	25 de marzo de 2024
Flujo de trabajo coincidente: actualización	AWS Entity Resolution ahora admite la asignación de RAMPID basada en la PII en el flujo de trabajo de correspondencia basado en los LiveRamp servicios del proveedor.	12 de febrero de 2024
AWS PrivateLink	AWS Entity Resolution ahora admite una seguridad de datos adicional, lo AWS PrivateLi nk que ayuda a los clientes a acceder de forma privada a los servicios alojados en ellos. AWS	20 de octubre de 2023

AWS CloudFormation Recursos: recursos nuevos y actualizados	AWS Entity Resolution ha agregado el siguiente recurso: `AWS::EntityResolution:IdMappingWorkflow` y ha actualizado los siguientes recursos: `AWS::EntityResolution::MatchingWorkflow` y `AWS::EntityResolution::Schemamapping` .	19 de octubre de 2023
Actualización de una política existente	Se han agregado los siguientes permisos nuevos a la política administrada: `AWSEntityResolutionConsoleFullAccess` `ADXReadAccess` y `ManageEventBridgeRules` .	16 de octubre de 2023
Mapeo de esquemas: actualización	Los clientes ahora tienen la posibilidad de editar y actualizar un esquema de datos existente.	16 de octubre de 2023
Flujo de trabajo coincidente: actualización	Los clientes ahora pueden seleccionar un servicio de proveedor de datos preferido para ayudarlos a comparar y vincular sus datos.	16 de octubre de 2023

Flujo de trabajo de mapeo	Los clientes pueden usar este nuevo flujo de trabajo para especificar los detalles del mapeo de ID, elegir el método de mapeo de ID que prefieran y especificar los campos de entrada y salida de datos.	16 de octubre de 2023
AWS CloudFormation integration	AWS Entity Resolution ahora se integra con AWS CloudFormation.	24 de agosto de 2023
AWS actualización gestionada de políticas: nuevas políticas	AWS Entity Resolution agregó dos nuevas políticas administradas.	18 de agosto de 2023
Versión inicial	Versión inicial de la Guía AWS Entity Resolution del usuario	26 de julio de 2023

AWS Entity Resolution Glosario

Nombre de recurso de Amazon (ARN)

Un identificador único de los recursos. AWS ARNs son necesarios cuando se necesita especificar un recurso de forma inequívoca en todos los aspectos, por ejemplo AWS Entity Resolution, en AWS Entity Resolution las políticas, las etiquetas de Amazon Relational Database Service (Amazon RDS) y las llamadas a la API.

Tipo de atributo

El tipo de atributo del campo de entrada. Al crear un esquema de mapeo, se selecciona el tipo de atributo de una lista preconfigurada de valores, como el nombre, la dirección, el número de teléfono o la dirección de correo electrónico. El tipo de atributo indica AWS Entity Resolution qué tipo de datos se están presentando, lo que permite clasificarlos y normalizarlos adecuadamente.

Procesamiento automático

Una opción de cadencia de procesamiento para un trabajo de flujo de trabajo coincidente que permite ejecutarlo automáticamente cuando se modifican los datos introducidos.

Esta opción solo está disponible para la coincidencia basada en reglas.

De forma predeterminada, la cadencia de procesamiento de un trabajo de flujo de trabajo coincidente se establece en Manual, lo que permite ejecutarlo bajo demanda. Puede configurar el procesamiento automático para que ejecute automáticamente el trabajo de flujo de trabajo correspondiente cuando cambie la entrada de datos. Esto mantiene la salida del flujo de trabajo coincidente up-to-date.

AWS KMS key ARN

Este es su nombre de recurso de AWS KMS Amazon (ARN) para el cifrado en reposo. Si no se proporciona, el sistema utilizará una clave KMS AWS Entity Resolution administrada.

Texto claro

Datos que no están protegidos criptográficamente.

Nivel de confianza () ConfidenceLevel

En el caso de la coincidencia de ML, este es el nivel de confianza que se aplica AWS Entity Resolution cuando ML identifica un conjunto de registros coincidente. Esto forma parte de los metadatos del flujo de trabajo coincidentes que se incluirán en la salida.

Descifrado

El proceso de transformar los datos cifrados para devolverles su forma original. El descifrado solo se puede realizar si se tiene el acceso a la clave secreta.

Cifrado

Proceso de codificación de datos en un formato aparentemente aleatorio utilizando un valor secreto denominado clave. Es imposible determinar el texto sin formato original sin tener acceso a la clave.

Nombre del grupo

El nombre del grupo hace referencia a todo el grupo de campos de entrada y puede ayudarle a agrupar los datos analizados para hacer coincidir los datos.

Por ejemplo, si hay tres campos de entrada: **`first_namemiddle_name`**, y**`last_name`**, puede agruparlos introduciendo el nombre del grupo **`full_name`** para que coincidan y salgan.

Hash

El uso de hash consiste en aplicar un algoritmo criptográfico que produce una cadena única e irreversible de caracteres de un tamaño fijo, denominada hash. AWS Entity Resolution utiliza el protocolo hash Secure Hash Algorithm de 256 bits (SHA256) y generará una cadena de caracteres de 32 bytes. En AWS Entity Resolution, puede elegir si desea codificar los valores de los datos en la salida.

Protocolo hash (HashingProtocol)

AWS Entity Resolution utiliza el protocolo hash Secure Hash Algorithm de 256 bits (SHA256) y generará una cadena de caracteres de 32 bytes. Esto forma parte de los metadatos del flujo de trabajo coincidentes que se incluirán en la salida.

Método de mapeo de ID

Cómo desea que se realice la asignación de ID.

Hay dos métodos de mapeo de ID:

- Basado en reglas: método mediante el cual se utilizan reglas de coincidencia para traducir datos propios de una fuente a un destino en un flujo de trabajo de mapeo de ID.
- Servicios de proveedores: método mediante el cual se utiliza un servicio de proveedor para traducir datos codificados de terceros de una fuente a un destino en un flujo de trabajo de mapeo de ID.

  AWS Entity Resolution actualmente es compatible con el LiveRamp método de mapeo de ID basado en los servicios del proveedor. Debe tener una suscripción AWS Data Exchange para LiveRamp utilizar este método. Para obtener más información, consulte Paso 1: Suscríbase a un servicio de proveedor en AWS Data Exchange.

Flujo de trabajo de asignación de ID

Un trabajo de procesamiento de datos que mapea los datos de una fuente de datos de entrada a un destino de datos de entrada en función del método de mapeo de ID especificado. Produce una tabla de asignación de ID. Este flujo de trabajo requiere que especifique el método de mapeo de ID y los datos de entrada que desea traducir de una fuente a un destino.

Puedes configurar un flujo de trabajo de mapeo de ID para que se ejecute por tu cuenta Cuenta de AWS o en dos Cuentas de AWS.

Espacio de nombres de ID

Un recurso AWS Entity Resolution que contiene metadatos que explican los conjuntos de datos de varios conjuntos de datos Cuentas de AWS y cómo utilizarlos en un flujo de trabajo de mapeo de ID.

Hay dos tipos de espacios de nombres de ID: y. `SOURCE` `TARGET` `SOURCE`Contiene configuraciones para los datos de origen que se procesarán en un flujo de trabajo de mapeo de ID. `TARGET`Contiene una configuración de los datos de destino a la que se adaptarán todas las fuentes. Para definir los datos de entrada que desea dividir en dos Cuentas de AWS, cree una fuente de espacio de nombres de ID y un destino de espacio de nombres de ID para traducir los datos de un conjunto () a otro ()`SOURCE`. `TARGET`

Después de crear espacios de nombres de ID con otro miembro y ejecutar un flujo de trabajo de mapeo de ID, pueden unirse a una colaboración AWS Clean Rooms para realizar una unión de varias tablas en la tabla de mapeo de ID y analizar los datos.

Para obtener más información, consulte la Guía del usuario de AWS Clean Rooms.

Campo de entrada

Un campo de entrada corresponde al nombre de una columna de la tabla AWS Glue de datos de entrada.

Fuente de entrada ARN (ARNInputSource)

El nombre de recurso de Amazon (ARN) que se generó para una entrada de AWS Glue tabla. Esto forma parte de los metadatos del flujo de trabajo coincidentes que se incluirán en la salida.

Emparejamiento basado en el aprendizaje automático

La coincidencia basada en el aprendizaje automático (coincidencia de aprendizaje automático) busca coincidencias en sus datos que pueden estar incompletas o que no tengan exactamente el mismo aspecto. La coincidencia de aprendizaje automático es un proceso preestablecido que intentará hacer coincidir los registros de todos los datos que introduzcas. La coincidencia de ML devuelve un identificador de coincidencia y un nivel de confianza para cada conjunto de datos coincidente.

Procesamiento manual

Una opción de cadencia de procesamiento para un trabajo de flujo de trabajo coincidente que permite ejecutarlo bajo demanda.

Esta opción está configurada de forma predeterminada y está disponible tanto para la coincidencia basada en reglas como para la coincidencia basada en el aprendizaje automático.

Many-to-Many coincidente

Many-to-many la coincidencia compara varias instancias de datos similares. Los valores de los campos de entrada a los que se haya asignado la misma clave de coincidencia se compararán entre sí, independientemente de si están en el mismo campo de entrada o en campos de entrada diferentes.

Por ejemplo, es posible que tengas varios campos de introducción de números de teléfono, como «Teléfono» `mobile_phone` y `home_phone` que tengan la misma clave coincidente. Usa la many-to-many coincidencia para comparar los datos del campo `mobile_phone` de entrada con los datos del campo `mobile_phone` de entrada y los datos del campo `home_phone` de entrada.

Las reglas de coincidencia evalúan los datos de varios campos de entrada con la misma clave de coincidencia con una operación (o), y la one-to-many coincidencia compara los valores de varios campos de entrada. Esto significa que si hay alguna combinación `mobile_phone` o `home_phone` coincidencia entre dos registros, la clave de coincidencia «Teléfono» devolverá una coincidencia. Para encontrar una coincidencia, pulse «Teléfono», `Record One mobile_phone = Record Two mobile_phone` `Record One mobile_phone = Record Two home_phone` OR `Record One home_phone = Record Two home_phone` OR`Record One home_phone = Record Two mobile_phone`.

ID de coincidencia (matchID)

Para la coincidencia basada en reglas y la coincidencia de aprendizaje automático, este es el ID generado AWS Entity Resolution y aplicado a cada conjunto de registros coincidente. Esto forma parte de los metadatos del flujo de trabajo coincidentes que se incluirán en la salida.

Haga coincidir la clave (MatchKey)

La tecla Match indica AWS Entity Resolution qué campos de entrada se deben considerar como datos similares y cuáles se deben considerar como datos diferentes. Esto ayuda a configurar AWS Entity Resolution automáticamente las reglas de coincidencia basadas en reglas y a comparar datos similares almacenados en diferentes campos de entrada.

Si en sus datos hay varios tipos de información sobre números de teléfono, como un `mobile_phone` campo de `home_phone` entrada y un campo de entrada, que le gustaría comparar entre sí, puede asignar a ambos la tecla correspondiente «Teléfono». Luego, la coincidencia basada en reglas se puede configurar para comparar datos utilizando las instrucciones «o» en todos los campos de entrada con la tecla de coincidencia «Teléfono» (consulte las definiciones de One-to-One coincidencia y Many-to-Many coincidencia en la sección Flujo de trabajo coincidente).

Si quieres que las coincidencias basadas en reglas consideren distintos tipos de información de números de teléfono por separado, puedes crear claves de coincidencia más específicas, como «Mobile_Phone» y «Home_Phone». A continuación, al configurar un flujo de trabajo de coincidencia,

puede especificar cómo se utilizará cada clave de coincidencia de teléfonos en la búsqueda de coincidencias basada en reglas.

Si MatchKey se especifica un número para un campo de entrada concreto, no se puede usar para la coincidencia, pero se puede llevar a cabo durante el proceso de flujo de trabajo de coincidencia y, si se desea, se puede generar como salida.

Haga coincidir el nombre de la clave

El nombre asignado a una clave de coincidencia.

Regla de coincidencia (MatchRule)

En el caso de las coincidencias basadas en reglas, este es el número de regla aplicado que generó un conjunto de registros coincidentes. Esto forma parte de los metadatos del flujo de trabajo coincidentes que se incluirán en la salida.

Coincidencia

Proceso de combinar y comparar datos de distintos campos de entrada, tablas o bases de datos y determinar cuáles son iguales (o «coinciden») en función del cumplimiento de ciertos criterios de coincidencia (por ejemplo, mediante reglas o modelos coincidentes).

Flujo de trabajo correspondiente

El proceso que se configura para especificar los datos de entrada que deben coincidir y cómo se debe realizar la coincidencia.

Descripción del flujo de trabajo coincidente

Una descripción opcional del flujo de trabajo coincidente que puede decidir introducir. Las descripciones le ayudan a diferenciar entre los flujos de trabajo coincidentes si crea más de uno.

Nombre del flujo de trabajo coincidente

El nombre del flujo de trabajo coincidente que especifique.

> **Note**
>
> Los nombres de los flujos de trabajo coincidentes deben ser únicos. No pueden tener el mismo nombre o se devolverá un error.

Los metadatos del flujo de trabajo coinciden

Información generada y generada AWS Entity Resolution durante un trabajo de flujo de trabajo coincidente. Esta información es obligatoria en la salida.

Normalización (ApplyNormalization)

Elija si desea normalizar los datos de entrada tal como se define en el esquema. La normalización estandariza los datos al eliminar los espacios adicionales y los caracteres especiales y estandarizarlos al formato en minúsculas.

Por ejemplo, si un campo de entrada tiene el tipo de atributo Teléfono completo y los valores de la tabla de entrada tienen el formato correspondiente`(123) 456-7890`, los valores se AWS Entity Resolution normalizarán a. `1234567890`

> **Note**
>
> La normalización solo es compatible con el tipo de grupo correspondiente al nombre, la dirección, el teléfono y el correo electrónico.

En las siguientes secciones se describen nuestras reglas de normalización estándar.

Para obtener información específica sobre la coincidencia basada en ML, consulteNormalización ()ApplyNormalization: solo basada en ML.

Temas

- Nombre
- Correo electrónico
- Teléfono

- Dirección
- Con un hash
- ID de origen

Nombre

> **Note**
>
> La normalización solo se admite para el tipo de grupo de nombres.
> El tipo de grupo de nombres aparece como nombre completo en la consola y **`NAME`** en la API.
> Si quieres normalizar los subtipos del grupo de nombres, escribe:
>
> - En la consola, asigne los siguientes subtipos al grupo de nombres completos: nombre, segundo nombre y apellido.
> - En la CreateSchemaMappingAPI, asigne los siguientes tipos a `NAME` GroupName: `NAME_FIRSTNAME_MIDDLE`, y. `NAME_LAST`

- TRIM = Recorta los espacios en blanco iniciales y finales
- MINÚSCULAS = Pone en minúscula todos los caracteres alfabéticos
- CONVERT_ACCENT = Convierte una letra acentuada a una letra normal
- REMOVE_ALL_NON_ALPHA = Elimina todos los caracteres no alfabéticos [A-zA-z]

Correo electrónico

> **Note**
>
> Se admite la normalización para el tipo de grupo de correo electrónico.
> El tipo de grupo de correo electrónico aparece como dirección de correo electrónico en la consola y **`EMAIL_ADDRESS`** en la API.

- TRIM = Recorta los espacios en blanco iniciales y finales
- MINÚSCULAS = Pone en minúscula todos los caracteres alfabéticos
- CONVERT_ACCENT = Convierte una letra acentuada a una letra normal

- EMAIL_ADDRESS_UTIL_NORM = Elimina cualquier punto (.) del nombre de usuario, elimina todo lo que esté después de un signo más (+) en el nombre de usuario y estandariza las variaciones de dominio más comunes
- REMOVE_ALL_NON_EMAIL_CHARS = Elimina todos los caracteres [a-zA-Z0-9] y [.@ -] non-alpha-numeric

Teléfono

> **Note**
>
> La normalización solo es compatible con el tipo de grupo de teléfonos.
> El tipo de grupo de teléfonos aparece como Teléfono completo en la consola y `PHONE` en la API.
> Si quieres normalizar los subtipos del tipo de grupo de teléfonos:
>
> - En la consola, asigne los siguientes subtipos al grupo de teléfonos completo: número de teléfono y código de país del teléfono.
> - En la CreateSchemaMappingAPI, asigne los siguientes tipos a `PHONE` GroupName: `PHONE_NUMBER` y. `PHONE_COUNTRYCODE`

- TRIM = Recorta los espacios en blanco iniciales y finales
- REMOVE_ALL_NON_NUMERIC = Elimina todos los caracteres no numéricos [0-9]
- REMOVE_ALL_LEADING_ZEROES = Elimina todos los ceros iniciales
- ENSURE_PREFIX_WITH_MAP, "" = Examina cada número de teléfono e intenta compararlo con los patrones del. phonePrefixMap phonePrefixMap Si se encuentra una coincidencia, la regla añadirá o modificará el prefijo del número de teléfono para garantizar que se ajusta al formato estandarizado especificado en el mapa.

Dirección

> **Note**
>
> La normalización solo se admite para el tipo de grupo de direcciones.
> El tipo de grupo de direcciones aparece como dirección completa en la consola y `ADDRESS` en la API.

Si quieres normalizar los subtipos del tipo de grupo de direcciones:

- En la consola, asigne los siguientes subtipos al grupo de direcciones completo: dirección 1, dirección 2: nombre de la dirección 3, nombre de la ciudad, estado, país y código postal t
- En la CreateSchemaMappingAPI, asigne los siguientes tipos a `ADDRESS` GroupName:`ADDRESS_STREET1`,`ADDRESS_STREET2`,`ADDRESS_STREET3`, `ADDRESS_CITY` `ADDRESS_STATE`ADDRESS_COUNTRY, y. `ADDRESS_POSTALCODE`

- TRIM = Recorta los espacios en blanco iniciales y finales
- MINÚSCULAS = Pone en minúscula todos los caracteres alfabéticos
- CONVERT_ACCENT = Convierte una letra acentuada a una letra normal
- REMOVE_ALL_NON_ALPHA = Elimina todos los caracteres no alfabéticos [A-zA-z]
- RENAME_WORDS utilizando ADDRESS_RENAME_WORD_MAP = sustituye las palabras de la cadena de direcciones por palabras de ADDRESS_RENAME_WORD_MAP
- RENAME_DELIMITERS mediante ADDRESS_RENAME_DELIMITER_MAP = reemplazar los delimitadores de la cadena de direcciones por la cadena de direcciones de ADDRESS_RENAME_DELIMITER_MAP
- RENAME_DIRECTIONS utilizando ADDRESS_RENAME_DIRECTION_MAP = reemplazar los delimitadores de la cadena de direcciones por una cadena de ADDRESS_RENAME_DIRECTION_MAP
- RENAME_NUMBERS con ADDRESS_RENAME_NUMBER_MAP = reemplaza los números de la cadena de direcciones por la cadena de direcciones de ADDRESS_RENAME_NUMBER_MAP
- RENAME_SPECIAL_CHARS utilizando ADDRESS_RENAME_SPECIAL_CHAR_MAP = sustituir los caracteres especiales de la cadena de direcciones por una cadena de ADDRESS_RENAME_SPECIAL_CHAR_MAP

ADDRESS_RENAME_WORD_MAP

Estas son las palabras a las que se les cambiará el nombre al normalizar la cadena de direcciones.

```
"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

Estos son los delimitadores a los que se les cambiará el nombre al normalizar la cadena de direcciones.

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

ADDRESS_RENAME_DIRECTION_MAP

Estos son los identificadores de dirección a los que se les cambiará el nombre al normalizar la cadena de direcciones.

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

ADDRESS_RENAME_NUMBER_MAP

Estas son las cadenas numéricas a las que se les cambiará el nombre al normalizar la cadena de direcciones.

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

ADDRESS_RENAME_SPECIAL_CHAR_MAP

Estas son las cadenas de caracteres especiales a las que se les cambiará el nombre al normalizar la cadena de direcciones.

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

Con un hash

- TRIM = Recorta los espacios en blanco iniciales y finales

ID de origen

- TRIM = Recorta los espacios en blanco iniciales y finales

Normalización ()ApplyNormalization: solo basada en ML

Elija si desea normalizar los datos de entrada tal como se define en el esquema. La normalización estandariza los datos al eliminar los espacios adicionales y los caracteres especiales y estandarizarlos al formato en minúsculas.

Por ejemplo, si un campo de entrada tiene un tipo de atributo de y los valores de `NAME` la tabla de entrada tienen el formato correspondiente`Johns Smith`, los valores se AWS Entity Resolution normalizarán a. `john smith`

En las siguientes secciones se describen las reglas de normalización para los flujos de trabajo de coincidencia basados en el aprendizaje automático.

Temas

- Nombre
- Correo electrónico
- Teléfono

Nombre

- TRIM = Recorta los espacios en blanco iniciales y finales
- MINÚSCULAS = Pone en minúscula todos los caracteres alfabéticos

Correo electrónico

- MINÚSCULAS = Pone en minúscula todos los caracteres alfabéticos
- Sustituye únicamente (at) (distingue entre mayúsculas y minúsculas) por el símbolo @
- Elimina todos los espacios en blanco de cualquier parte del valor
- Elimina todo lo que esté fuera del primero, "< >" si existe

Teléfono

- TRIM = Recorta los espacios en blanco iniciales y finales
- REMOVE_ALL_NON_NUMERIC = Elimina todos los caracteres no numéricos [0-9]
- REMOVE_ALL_LEADING_ZEROES = Elimina todos los ceros iniciales

- ENSURE_PREFIX_WITH_MAP, "" = Examina cada número de teléfono e intenta compararlo con los patrones del. phonePrefixMap phonePrefixMap Si se encuentra una coincidencia, la regla añadirá o modificará el prefijo del número de teléfono para garantizar que se ajusta al formato estandarizado especificado en el mapa.

One-to-One coincidente

One-to-one la coincidencia compara instancias individuales de datos similares. Los campos de entrada con la misma clave de coincidencia y los valores del mismo campo de entrada se compararán entre sí.

Por ejemplo, es posible que tengas varios campos de entrada de números de teléfono, como `mobile_phone` y `home_phone` que tengan la misma clave de coincidencia: «Teléfono». Utilice la one-to-one coincidencia para comparar los datos del campo de `mobile_phone` entrada con los datos del campo de `mobile_phone` entrada y para comparar los datos del campo `home_phone` de entrada con los datos del campo `home_phone` de entrada. Los datos del campo `mobile_phone` de entrada no se compararán con los datos del campo `home_phone` de entrada.

Las reglas de coincidencia evalúan los datos de varios campos de entrada con la misma clave de coincidencia con una operación (o), y la one-to-many coincidencia compara los valores de un solo campo de entrada. Esto significa que si dos registros `home_phone` coinciden `mobile_phone` o coinciden entre ellos, la clave de coincidencia «Teléfono» devolverá una coincidencia. Para encontrar una coincidencia, escriba «Teléfono» `Record One mobile_phone = Record Two mobile_phone` o`Record One home_phone = Record Two home_phone`.

Las reglas de coincidencia evalúan los datos de los campos de entrada con diferentes claves de coincidencia mediante una operación (y). Si quieres que las coincidencias basadas en reglas consideren distintos tipos de información de números de teléfono por separado, puedes crear claves de coincidencia más específicas, como «mobile_phone» y «home_phone». Si quieres usar ambas claves de coincidencia en una regla para buscar coincidencias, AND. `Record One mobile_phone = Record Two mobile_phone` `Record One home_phone = Record Two home_phone`

Output

Una lista de OutputAttributeobjetos, cada uno de los cuales tiene los campos Nombre y Hashed. Cada uno de estos objetos representa una columna que se incluirá en la tabla de AWS Glue resultados y si desea que los valores de la columna estén codificados con un hash.

Ruta 3 de salida

El destino S3 en el que se AWS Entity Resolution escribirá la tabla de resultados.

OutputSourceConfig

Una lista de OutputSource objetos, cada uno de los cuales tiene los campos Outputs3Path y Output. ApplyNormalization

Coincidencia basada en los servicios del proveedor

La correspondencia basada en los servicios de los proveedores es un proceso diseñado para hacer coincidir, vincular y mejorar sus registros con los proveedores de servicios de datos preferidos y los conjuntos de datos con licencia. Debe estar suscrito al servicio del proveedor para utilizar esta técnica de comparación. AWS Data Exchange

AWS Entity Resolution actualmente se integra con los siguientes proveedores de servicios de datos:

- LiveRamp
- TransUnion
- UID 2.0

Emparejamiento basado en reglas

La coincidencia basada en reglas es un proceso diseñado para encontrar coincidencias exactas. La coincidencia basada en reglas es un conjunto jerárquico de reglas de coincidencia en cascada, sugeridas por AWS Entity Resolution, basadas en los datos que usted introduce y que usted puede configurar completamente. Todas las claves de coincidencia incluidas en los criterios de la regla deben coincidir exactamente para que los datos comparados se declaren coincidentes y para que se generen los metadatos asociados. La coincidencia basada en reglas devuelve un identificador de coincidencia y un número de regla para cada conjunto de datos coincidente.

Recomendamos definir reglas que puedan identificar de forma única a una entidad. Ordene primero sus reglas para encontrar coincidencias más precisas.

Por ejemplo, supongamos que tienes dos reglas, la regla 1 y la regla 2.

Estas reglas tienen las siguientes claves de coincidencia:

- La regla 1 incluye el nombre completo y la dirección
- La regla 2 incluye nombre completo, dirección y teléfono

Como la regla 1 se ejecuta primero, la regla 2 no encontrará coincidencias porque la regla 1 las habría encontrado todas.

Para buscar coincidencias diferenciadas por teléfono, reordena las reglas de la siguiente manera:

- La regla 2 incluye nombre completo, dirección y teléfono
- La regla 1 incluye el nombre completo y la dirección

Esquema

Término utilizado para una estructura o diseño que define cómo se organiza y conecta un conjunto de datos.

Descripción del esquema

Una descripción opcional del esquema que puede elegir introducir. Las descripciones le ayudan a diferenciar entre las asignaciones de esquemas si crea más de una.

Nombre del esquema

El nombre del esquema.

> **Note**
>
> Los nombres de los esquemas deben ser únicos. No pueden tener el mismo nombre o se devolverá un error.

Asignación de esquemas

El mapeo de esquemas AWS Entity Resolution es el proceso mediante el cual se indica AWS Entity Resolution cómo interpretar los datos para que coincidan. Usted define el esquema de la tabla de datos de entrada que AWS Entity Resolution desea leer en un flujo de trabajo coincidente.

ARN de mapeo de esquemas

El nombre de recurso de Amazon (ARN) generado para el mapeo del esquema.

ID único

Un identificador único que usted designe y que debe asignarse a cada fila de datos de entrada que se AWS Entity Resolution lea.

Example

Por ejemplo: **`Primary_key`**, **`Row_ID`** o **`Record_ID`**.

La columna de ID único es obligatoria.

El identificador único debe ser un identificador único dentro de una sola tabla.

El identificador único debe cumplir este patrón: `[a-zA-Z0-9_-]`

En diferentes tablas, el identificador único puede tener valores duplicados.

Cuando se ejecute el flujo de trabajo coincidente, el registro se rechazará si el identificador único:

- no está especificado
- no es único en la misma tabla
- se superpone en términos de nombre de atributo en todas las fuentes.
- supera los 38 caracteres (solo flujos de trabajo de coincidencia basados en reglas)

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.