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:

- Con AWS Entity Resolution figuración

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.

  - R coincidencia eady-to-use 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 Registro de 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 Creación de recursos de AWS Entity Resolution 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).

Con AWS Entity Resolution figuración

Antes de usarlo AWS Entity Resolution por primera vez, complete las siguientes tareas.

Temas

Inscríbase en AWS

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

Para suscribirte a una Cuenta de AWS

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

   Parte del procedimiento de registro consiste en recibir una llamada telefónica 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.

Creación de 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, consulte 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.	Siga las instrucciones en Creación del primer grupo de usuarios y usuario de administrador de IAM en la Guía del usuario de IAM.	Configurar el acceso programático mediante Administración de las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM.

Suscríbase a un servicio de proveedor en AWS Data Exchange

Complete el siguiente procedimiento si utiliza un flujo de trabajo de búsqueda de coincidencias basado en servicios de proveedores o un flujo de trabajo de mapeo de ID. Si no utiliza un flujo de trabajo de correspondencia basado en servicios de proveedores o un flujo de trabajo de mapeo de ID, puede omitir este paso.

En AWS Entity Resolution, puedes elegir ejecutar un flujo de trabajo coincidente con uno de los siguientes servicios de proveedores si tienes una suscripción con ese proveedor. AWS Data Exchange Sus datos se compararán con un conjunto de entradas definido por su proveedor preferido.

- LiveRamp
  - LiveRamp Resolución de identidad
  - LiveRamp Transcodificación
- TransUnion
  - TransUnion TruAudience Resolución y enriquecimiento de la identidad sin transferencia
  - TransUnion TruAudience Resolución de identidad sin transferencia
- ID unificada 2.0
  - Resolución de identidad de Unified ID 2.0

Además, puede ejecutar un flujo de trabajo de mapeo de LiveRamp identidades si tiene una suscripción con ese proveedor.

- LiveRamp
  - LiveRamp Transcodificación

Hay dos formas de suscribirse a un servicio de proveedor:

- Oferta privada: si ya tiene una relación con un proveedor, siga el procedimiento de productos y ofertas 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

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 contiene API, consulte Acceder a un producto de API en la Guía del AWS Data Exchange usuario.

Prepare tablas de datos

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 a Amazon S3. Una vez cargados 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.

La preparación de las tablas de datos consta de los siguientes pasos:

Temas

Paso 1: Prepare los datos de entrada

Complete el siguiente procedimiento si utiliza un flujo de trabajo coincidente con un servicio de un proveedor. Si no utiliza un flujo de trabajo coincidente con un servicio de proveedor, puede omitir este paso.

Para obtener más información, consulte Suscríbase a un servicio de proveedor en AWS Data Exchange.

Si desea ejecutar un flujo de trabajo coincidente con un flujo de trabajo coincidente basado en los servicios del proveedor o un flujo de trabajo de mapeo de identidades, consulte la siguiente tabla para preparar los datos de entrada:

Servicio de proveedor	¿Se necesita una identificación 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 correspondiente, 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 de proveedor	¿Se necesita una identificación única?	Acciones

TransUnion	Sí	Asegúrese de lo siguiente:
		• Existe un identificador único para el enriquecimiento TransUnion de datos.
		Note
		Se permite que los atributos de transferencia persistan en la entrada y la salida a TransUnion. Las claves E domésticas y el HHID son específicos del espacio de nombres del cliente.
		• **`Phone number`** debe tener 10 dígitos, sin caracteres especiales como espacios o guiones.
		• **`Addresses`** debe dividirse en
		  • una sola línea de dirección (combine las líneas de dirección 1 y 2, si las hay)
		  • ciudad
		  • zip (o zip plus4), sin caracteres especiales como espacios o guiones

Servicio de proveedor	¿Se necesita una identificación única?	Acciones
		• estado, especificado como código de 2 letras 3 • **`Email addresses`** debe estar en texto plano. • **`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.

Servicio de proveedor	¿Se necesita una identificación única?	Acciones
ID unificado 2.0	Sí	Asegúrese de lo siguiente: • El identificador único no puede ser un hash. • El UID2 admite tanto el correo electrónico como el número de teléfono para la generación del UID2. 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 generación del UID2 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 estos registros se dupliquen en la salida, lo mejor es crear un flujo de trabajo independiente para cada uno de ellos, 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.

Servicio de proveedor	¿Se necesita una identificación única?	Acciones
		Note Un correo electrónico o número de teléfono específico, en cualquier momento específico, da como resultado el mismo valor de UID2 sin procesar, independientemente de quién haya realizado la solicitud. Los UID2 sin procesar se crean añadiendo sales de cubos de sal que se giran aproximadamente una vez al año, lo que hace que el UID2 sin procesar también se rote con ellos. Los distintos cubos de sal rotan en diferentes momentos del año. AWS Entity Resolution actualmente no registra los cubos de sal giratorios ni los UID2 sin procesar, por lo que se recomienda regenerar los UID2 sin procesar a diario. Para obtener más información, consulte ¿Con qué frecuencia se

Servicio de proveedor	¿Se necesita una identific ación única?	Acciones
		deben actualizar los UID2 para realizar actualiza ciones incrementales? en la documentación del UID 2.0.

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

Si ya guardó los datos de entrada en un formato de datos compatible, puede omitir 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 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

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 la AWS Glue consola AWS Management Console y ábrala 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 base de datos de AWS Glue y 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.
13. Anote el nombre de la AWS Glue base de datos y el nombre de AWS Glue la tabla.

Cree un rol de IAM para un usuario de la 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.

   Puedes usar los 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: AWSEntityResolutionConsoleFullAccess
      - AWS política gestionada: AWSEntityResolutionConsoleReadOnlyAccess

   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. Elija Crear rol.

Cree 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 en 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.

```
{
    "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.

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

Sustituya cada *{{marcador de posición introducido por el usuario}}* 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.
cubos de entrada	Buckets de Amazon S3 que contienen los objetos de datos subyacentes desde los AWS Glue que `AWS Entity Resolution` se leerá.
cubos de salida	Los buckets de Amazon S3 son los `AWS Entity Resolution` que generarán los datos de salida.
bases de datos de entrada	AWS Glue bases de datos desde las que `AWS Entity Resolution` 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}}"
    ]
}
```

Sustituya cada *{{marcador de posición introducido por el usuario}}* 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.
Teclas de entrada	Llaves administradas en. 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}}"
            ]
        }
```

Sustituya cada *{{marcador de posición introducido por el usuario}}* 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.
Llaves de salida	Llaves administradas en. 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}}"
            ]
        }
```

Sustituya cada *{{marcador de posición introducido por el usuario}}* 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.
ID de revisioniD	La revisión del conjunto de datos, que se encuentra en la consola. AWS Data Exchange
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 del rol debe coincidir con el patrón de los `passRole` permisos concedidos al miembro que puede transferirlo `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. Elija Crear rol.

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

Creación de un mapeo de esquemas

Para definir los datos de entrada que desea resolver, cree un mapeo de esquemas. El proceso de mapeo de esquemas lo guía a través de una serie de pasos para definir los datos que desea resolver. Para ello, defina los campos de entrada y los tipos de atributos y, a continuación, defina y agrupe las claves de coincidencia.

Hay tres formas de crear un mapeo de esquemas en AWS Entity Resolution:

- Uso de un flujo guiado para importar la información del esquema existente.
- Uso de un flujo guiado para definir manualmente los datos de entrada.
- Uso del editor JSON para crear, pegar o importar un esquema de mapeo.

El siguiente proceso le guiará por los tres métodos diferentes para crear un mapeo de esquemas.

Temas

Cree un mapeo de esquemas (columnas rellenadas previamente)

Este procedimiento describe el proceso de creación de un mapeo de esquemas mediante la AWS Glue opción Importar desde de la AWS Entity Resolution consola. Puede utilizar este método de creación para definir los campos de entrada empezando por las columnas rellenadas previamente de una AWS Glue tabla.

Para crear un mapeo de esquemas mediante columnas rellenadas previamente:

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola con la suya Cuenta de AWS, si aún no lo ha hecho.
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, vaya 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.

   e. En el caso de los campos de entrada, selecciona de 1 a 25 columnas para usarlas como coincidencias y como paso opcional.

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

      ii. En Transferir: opcional, selecciona las columnas que deseas incluir como columnas de acceso directo.

   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. Para el paso 2: mapear los campos de entrada, haga lo siguiente:

   a. Para que los campos de entrada coincidan, especifique el tipo de entrada y la tecla de coincidencia para cada campo de entrada.

      El tipo de entrada le ayuda a clasificar los datos. La tecla Match permite comparar los campos de entrada con el flujo de trabajo correspondiente.

      > **Note**
      >
      > Si está creando un mapeo de esquemas para usarlo con la técnica de coincidencia basada en los servicios del LiveRamp proveedor, puede:
      >
      > - Especifique el tipo de entrada como LiveRampID.
      > - Especifique el campo de nombre como varios campos (por ejemplo**`first_name`**,**`last_name`**) o en un campo.
      > - Especifique el campo de dirección postal como varios campos (por ejemplo**`address1`**,**`address2`**) o en un solo campo.
      >
      >   Si coincide con una dirección, se requiere un código postal.
      > - Incluya el correo electrónico o el teléfono con su nombre, y esos campos pueden coincidir con la dirección postal.

   b. Elija Siguiente.

6. Para el paso 3: agrupar datos, haga lo siguiente:

   a. Elija los campos de nombre relacionados y, a continuación, introduzca el nombre del grupo y la clave de coincidencia.

      Example

      Por ejemplo, elija los campos de entrada y **`First nameMiddle name`**, y**`Last name`**, a continuación, introduzca un nombre de grupo denominado «**`Full name`**» y una clave de coincidencia denominada «**`Full name`**» para activar la comparación.

   b. Elija los campos de dirección relacionados y, a continuación, introduzca el nombre del grupo y la clave de coincidencia.

Example

Por ejemplo, elija los campos de entrada y **`Home street address 1Home street address 2`**, y**`Home city`**, a continuación, introduzca un nombre de grupo denominado «**`Shipping address`**» y una clave de coincidencia denominada «**`Shipping address`**» para activar la comparación.

c. Seleccione los campos de número de teléfono relacionados y, a continuación, introduzca el nombre del grupo y la clave de coincidencia.

Example

Por ejemplo, elija los campos de entrada y **`Home phone 1Home phone 2`**, y**`Cell phone`**, a continuación, introduzca un nombre de grupo denominado «**`Shipping phone number`**» y una clave de coincidencia denominada «**`Shipping phone number`**» para activar la comparación.

Si tiene más de un tipo de datos, puede añadir más grupos.

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.

Crea un mapeo de esquemas (columnas definidas manualmente)

Este procedimiento describe el proceso de creación de un mapeo de esquemas mediante la opción Crear un esquema personalizado de la AWS Entity Resolution consola. Utilice este método de creación para definir manualmente los campos de entrada mediante un flujo guiado.

Para crear un mapeo de esquemas mediante columnas definidas manualmente

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola con la suya Cuenta de AWS, si aún no lo ha hecho.
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.

    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. Para el paso 2: mapear los campos de entrada, haga lo siguiente:

   a. Para que los campos de entrada coincidan, añada el campo de entrada, el tipo de entrada y la tecla de coincidencia.

      Puede añadir hasta 25 campos de entrada.

      El tipo de entrada le ayuda a clasificar los datos. La tecla Match permite comparar los campos de entrada con el flujo de trabajo correspondiente.

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

   b. (Opcional) En el caso de los campos de entrada para transferirlos, añada los campos de entrada que no coincidan.

   c. Elija Siguiente.

6. Para el paso 3: agrupar datos:

   a. Elija los campos de nombre relacionados y, a continuación, introduzca el nombre del grupo y la clave de coincidencia.

      Example

      Por ejemplo, elija los campos de entrada y **`First nameMiddle name`**, y**`Last name`**, a continuación, introduzca un nombre de grupo denominado «**`Full name`**» y una clave de coincidencia denominada «**`Full name`**» para activar la comparación.

   b. Elija los campos de dirección relacionados y, a continuación, introduzca el nombre del grupo y la clave de coincidencia.

      Example

      Por ejemplo, elija los campos de entrada y **`Home street address 1Home street address 2`**, y**`Home city`**, a continuación, introduzca un nombre de grupo denominado «**`Shipping address`**» y una clave de coincidencia denominada «**`Shipping address`**» para activar la comparación.

c. Seleccione los campos de número de teléfono relacionados y, a continuación, introduzca el nombre del grupo y la clave de coincidencia.

   Example

   Por ejemplo, elija los campos de entrada y **`Home phone 1`**`Home phone 2`, y**`Cell phone`**, a continuación, introduzca un nombre de grupo denominado «**`Shipping phone number`**» y una clave de coincidencia denominada «**`Shipping phone number`**» para activar la comparación.

   Si tiene más de un tipo de datos, puede añadir más grupos.

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.

Crea un mapeo de esquemas (editor JSON)

Este procedimiento describe el proceso de creación de un mapeo de esquemas mediante la opción Usar el editor JSON de la AWS Entity Resolution consola. Utilice este método de creación para utilizar un editor de JSON para crear, pegar o importar una asignación de esquemas. Los campos de ID único y de entrada no están disponibles con esta opción.

Para crear un mapeo de esquemas mediante el editor JSON

1. Inicie sesión en AWS Management Console y abra la AWS Entity Resolution consola con el suyo Cuenta de AWS, si aún no lo ha hecho.

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:

Si desea...	Entonces elija...
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

   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.

Crear un flujo de trabajo coincidente

Después de crear un mapeo de esquemas, puede crear uno o más flujos de trabajo coincidentes para especificar las entradas de datos y los pasos de normalización y elegir las técnicas de coincidencia que desee. Existen tres técnicas de coincidencia:

- 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.
- La coincidencia basada en el aprendizaje automático es un proceso preestablecido que intentará hacer coincidir los registros de todos los datos que introduzca.
- Los servicios de proveedores le permiten hacer coincidir sus identificadores conocidos con los de su proveedor de servicios de datos preferido.

  AWS Entity Resolution actualmente se integra con los siguientes proveedores de servicios de datos: LiveRamp TransUnion, y UID 2.0. 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, consulte Suscríbase a un servicio de proveedor en AWS Data Exchange.

AWS Entity Resolution lee los datos de las ubicaciones especificadas por usted y escribe los resultados 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.

También puede utilizar el resultado de las coincidencias basadas en reglas o de aprendizaje automático como entrada para las coincidencias basadas en los servicios del proveedor o al revés para satisfacer las necesidades de su empresa. Por ejemplo, puede ejecutar primero una búsqueda de coincidencias basada en reglas para buscar coincidencias en sus datos y, a continuación, enviar un subconjunto de registros no coincidentes a una búsqueda basada en servicios de proveedores para ahorrar costos de suscripción a los proveedores.

Temas

- Siguientes pasos

Cree un flujo de trabajo de coincidencias basado en reglas

El flujo de trabajo de coincidencia basado en reglas le permite comparar datos en texto sin cifrar o codificados para encontrar coincidencias exactas en función de los criterios que personalice.

Cuando AWS Entity Resolution encuentra una coincidencia entre dos o más registros de sus datos, asigna un identificador de coincidencia a los registros del conjunto de datos coincidentes.

Para la coincidencia basada en reglas, aplica el número de regla que generó la coincidencia.

Para crear un flujo de trabajo de coincidencia basado en reglas:

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS (si aún no lo has hecho).
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.

    d. Especifique los permisos de Acceso a servicios seleccionando Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

Si eliges...	Entonces
Crear y usar un nuevo rol de servicio	• AWS Entity Resolution crea un rol de servicio con la política requerida para esta tabla.

Si eliges...	Entonces
	• 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, puede elegir la opción Estos datos se cifran con una clave de KMS y, a continuación, introducir una AWS KMS clave que se utilizará para descifrar los datos introducidos.

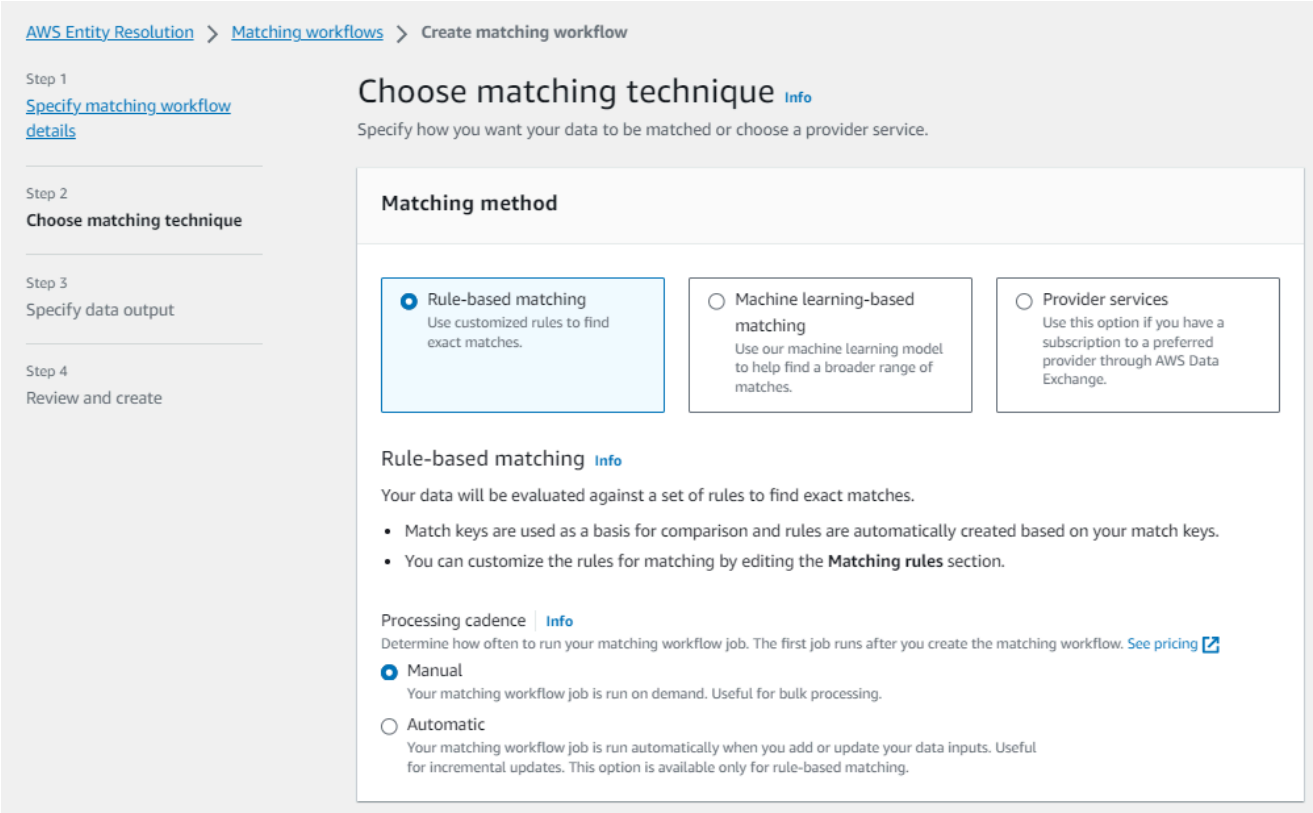
Si eliges...	Entonces
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Para ver la función de servicio, seleccione el enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de roles 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, elija una de las siguientes opciones.

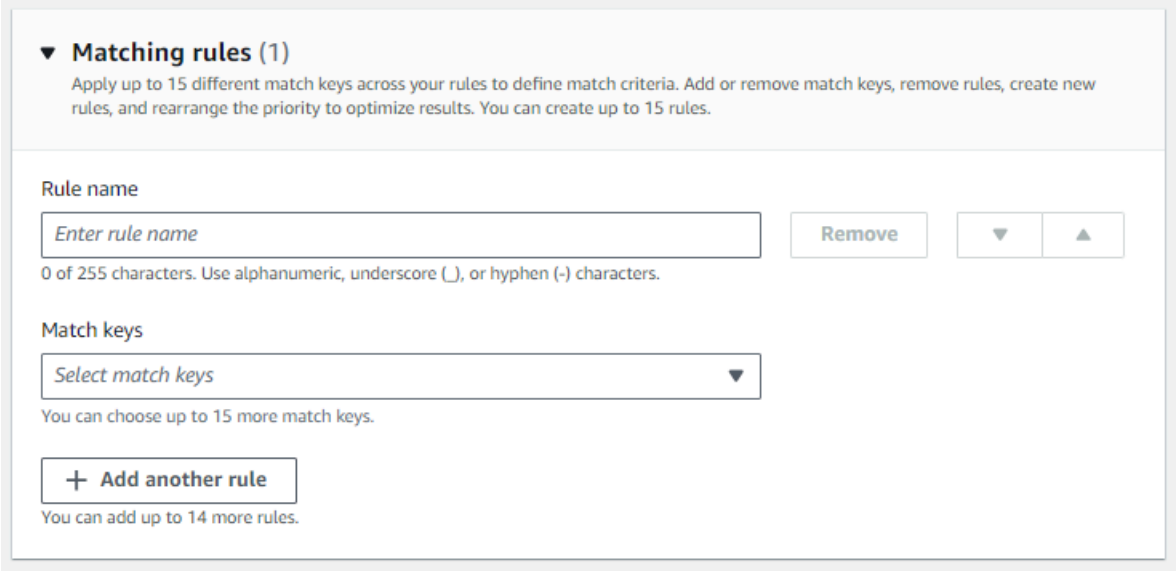
Si desea...	Entonces elija...
Ejecute un flujo de trabajo a pedido para realizar una actualización masiva	Manual
Ejecute un flujo de trabajo en cuanto haya nuevos datos en su bucket de S3	Automático

> **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. En el caso de las reglas de coincidencia, introduzca el nombre de una regla y, a continuación, elija las claves de coincidencia para esa regla.

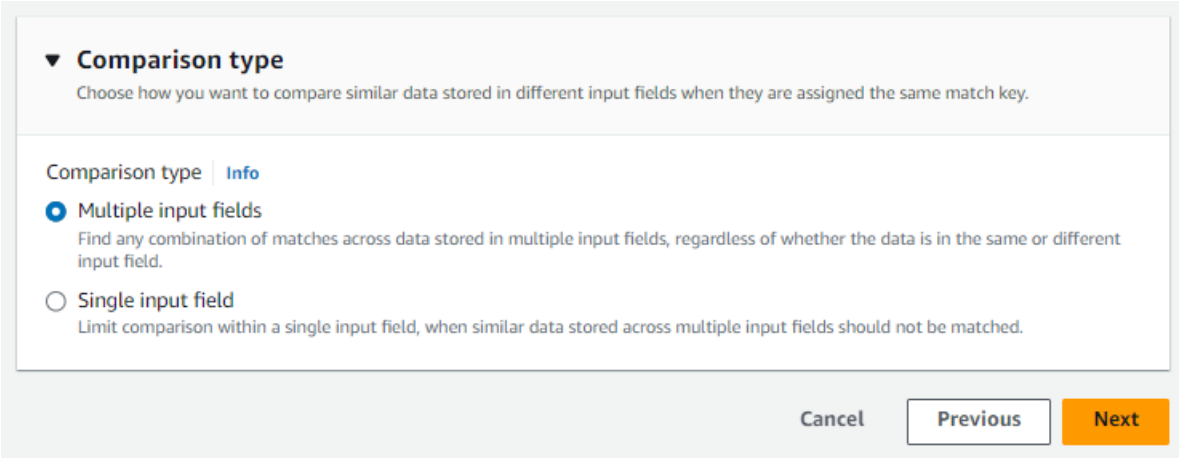
Puede aplicar hasta 15 claves de coincidencia diferentes a las reglas para definir los criterios de coincidencia.

Puedes crear hasta 15 reglas.



d. En Tipo de comparación, elija una de las siguientes opciones.

Si desea...	Entonces elija...
Busque cualquier combinación de coincidencias entre los datos almacenados en varios campos de entrada	Comparación de varios campos de entrada
Limite la comparación a un solo campo de entrada	Comparación de campos de entrada única



e. 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 la salida de datos, consulte todos los campos incluidos.

   e. Determine si desea incluir, ocultar o enmascarar los campos.

Si desea...	Entonces elija...
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.

   f. 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.
   - Los ID de coincidencia únicos generados.
   - 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.

Ya puede hacer lo siguiente:

- Edita un flujo de trabajo coincidente
- Elimine un flujo de trabajo coincidente
- Ejecute un flujo de trabajo coincidente

Cree un flujo de trabajo coincidente basado en el aprendizaje automático

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 sus datos, asigna un identificador de coincidencia a los registros del conjunto de datos coincidente.

En el caso de las coincidencias basadas en el aprendizaje automático, aplica el porcentaje del nivel de confianza de las coincidencias.

Para crear un flujo de trabajo de coincidencia basado en ML:

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS (si aún no lo has hecho).
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.
    d. Especifique los permisos de Acceso a servicios seleccionando Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

Si eliges...	Entonces
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, puede elegir la opción Estos datos se cifran con una clave de KMS y, a continuación, introducir una AWS KMS clave que se utilizará para descifrar los datos introducidos.

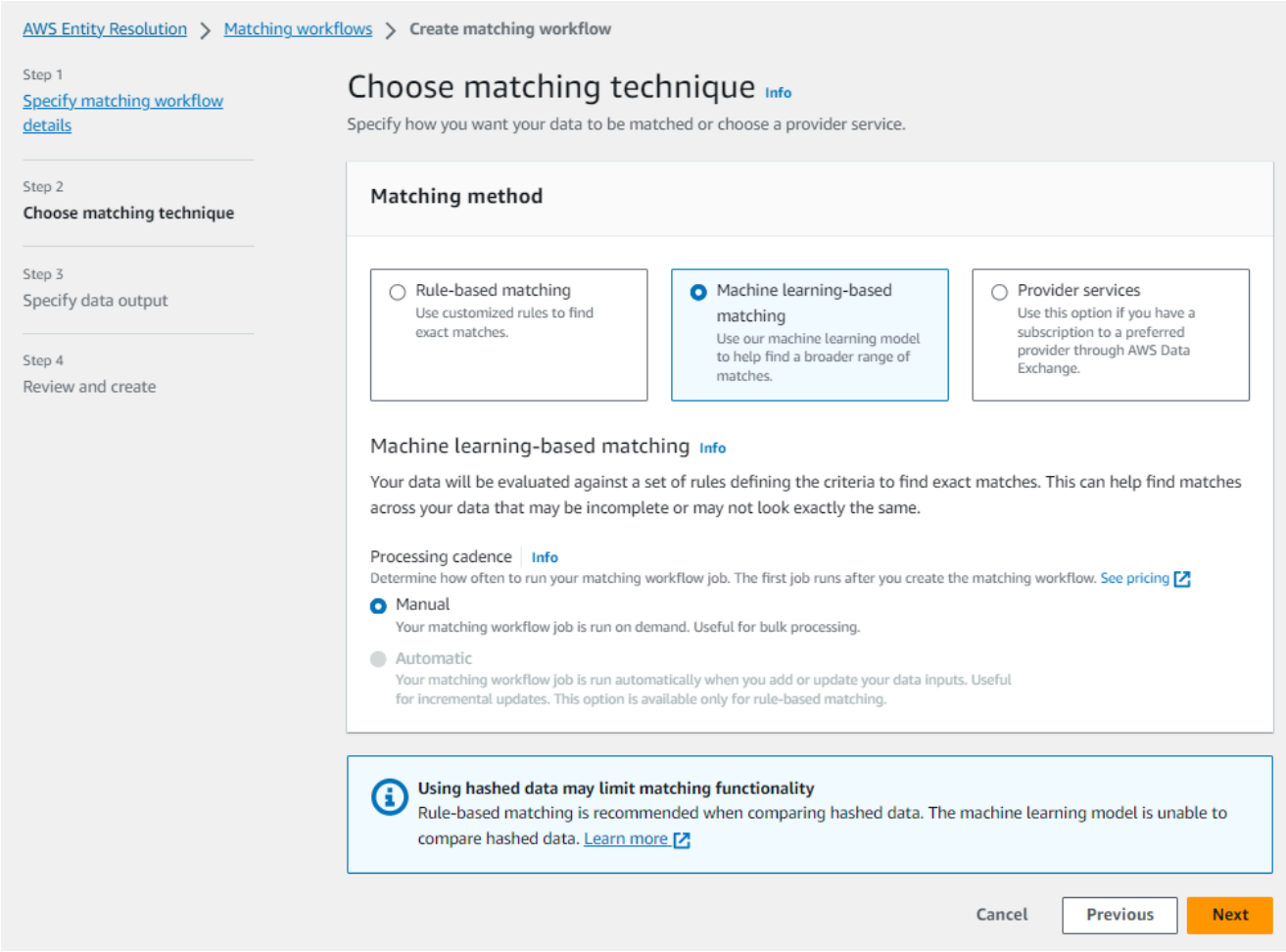
Si eliges...	Entonces
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. 2. Para ver la función de servicio, seleccione el enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de roles 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.

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 la salida de datos, consulte todos los campos incluidos.

   e. Determine si desea incluir, ocultar o enmascarar los campos.

Si desea...	Entonces elija...
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.

f. 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.
   - Los ID de coincidencia únicos generados.
   - 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.

Ya puede hacer lo siguiente:

- Edita un flujo de trabajo coincidente
- Elimine un flujo de trabajo coincidente
- Ejecute un flujo de trabajo coincidente

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

Si tienes una suscripción a través de un proveedor de servicios AWS Data Exchange, puedes hacer coincidir tus identificadores conocidos con los de tu proveedor preferido. AWS Entity Resolution actualmente admite los siguientes servicios de proveedores de datos:

- LiveRamp
- TransUnion
- ID unificada 2.0

Para obtener más información sobre cómo crear una nueva suscripción o reutilizar una suscripción existente a un servicio de un proveedor, consulteSuscríbase 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 identificadores más utilizados en las plataformas orientadas a la demanda para crear una audiencia para una campaña publicitaria. Si utilizas un flujo de trabajo coincidente con LiveRamp RampIDs, puedes convertir las direcciones de correo electrónico codificadas con hash.

> **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.

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

Sustituya cada uno <user input placeholder>por su propia información.

cubeta de almacenamiento	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. Inicia sesión en la AWS Entity Resolution consola AWS Management Console y ábrela con tu Cuenta de AWS (si aún no lo has hecho).
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 utiliza el proceso de resolución solo por correo electrónico, deseleccione la opción Normalizar datos, ya que solo se utilizan correos electrónicos cifrados como datos de entrada.

d. Especifique los permisos de Acceso a servicios seleccionando Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

Si eliges...	Entonces
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, puede elegir la opción Estos datos se cifran con una clave de KMS y, a continuación, introducir una AWS KMS clave que se utilizará para descifrar los datos introducidos.

Si eliges...	Entonces
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. Para ver la función de servicio, seleccione el enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de roles 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.

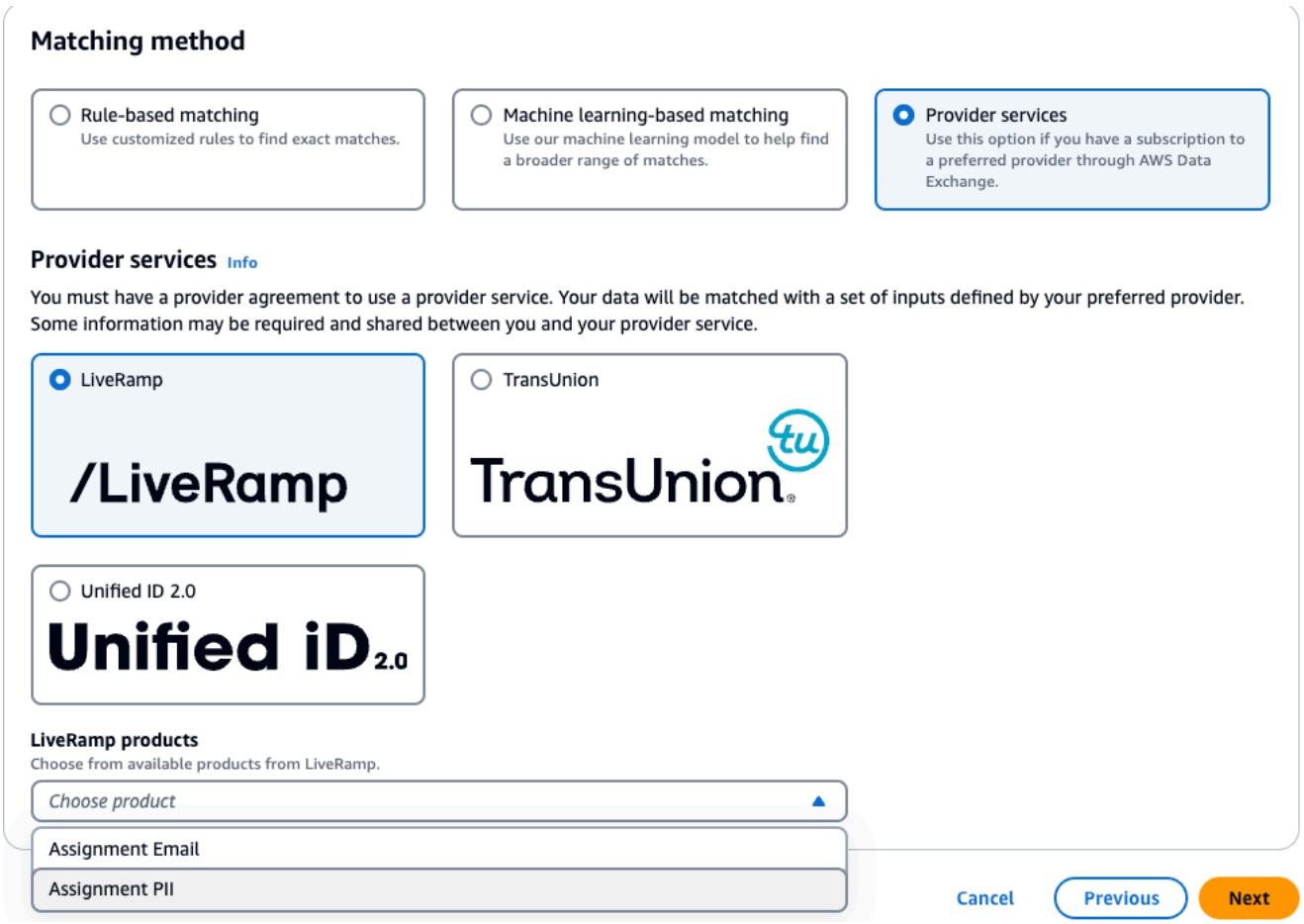
5. Para el paso 2: elija una técnica de coincidencia:

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

b. Para los servicios de proveedores, elija LiveRamp.

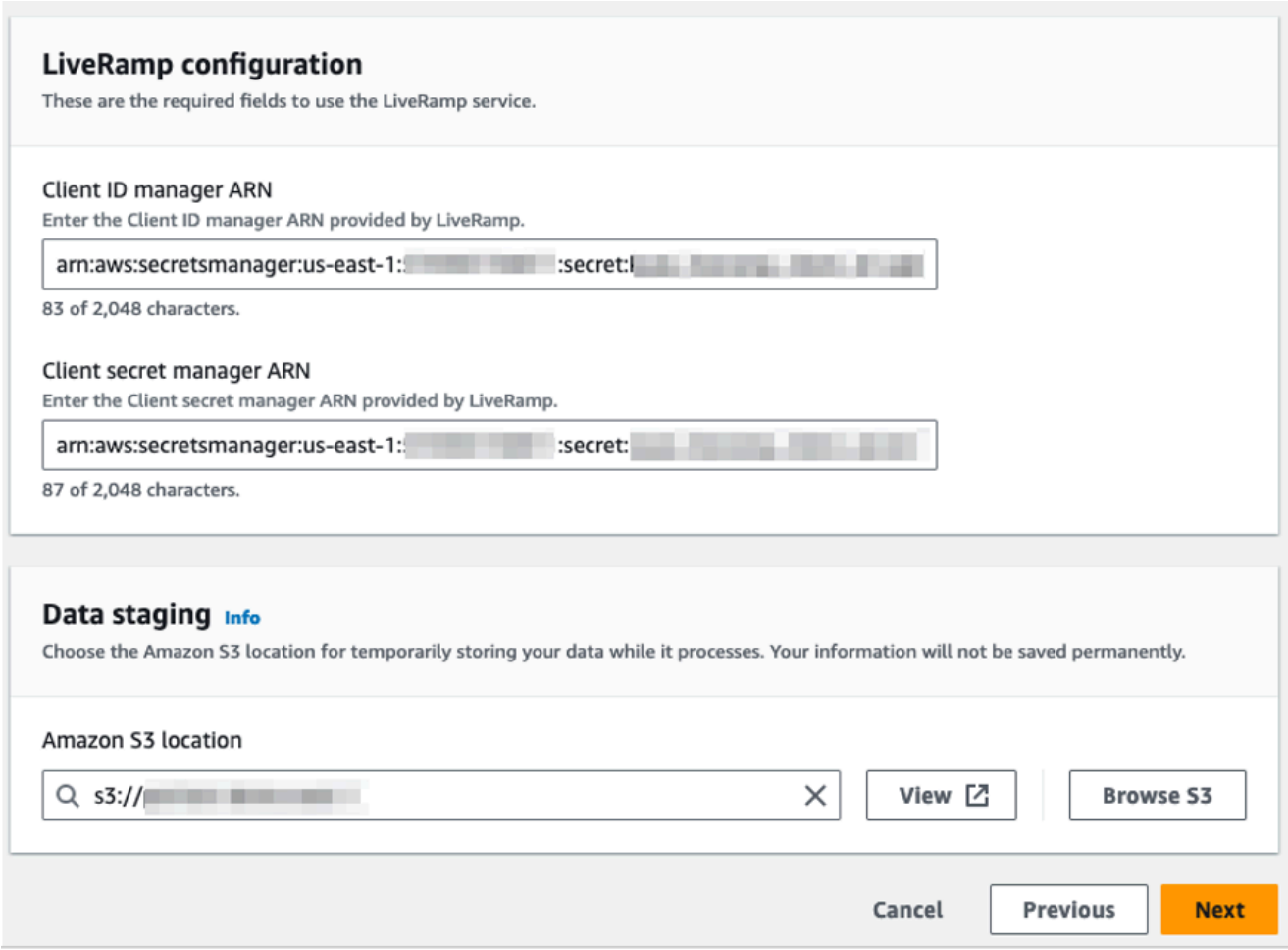
> **Note**
>
> Asegúrese de que el formato y la normalización del archivo de entrada de datos estén alineados con las directrices del servicio del proveedor.
> Para obtener más información sobre las pautas de formato de los archivos de entrada para el flujo de trabajo correspondiente, consulte Realizar 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 the section called “Cree un rol de trabajo de flujo de trabajo para AWS Entity Resolution”.

f. Seleccione 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.

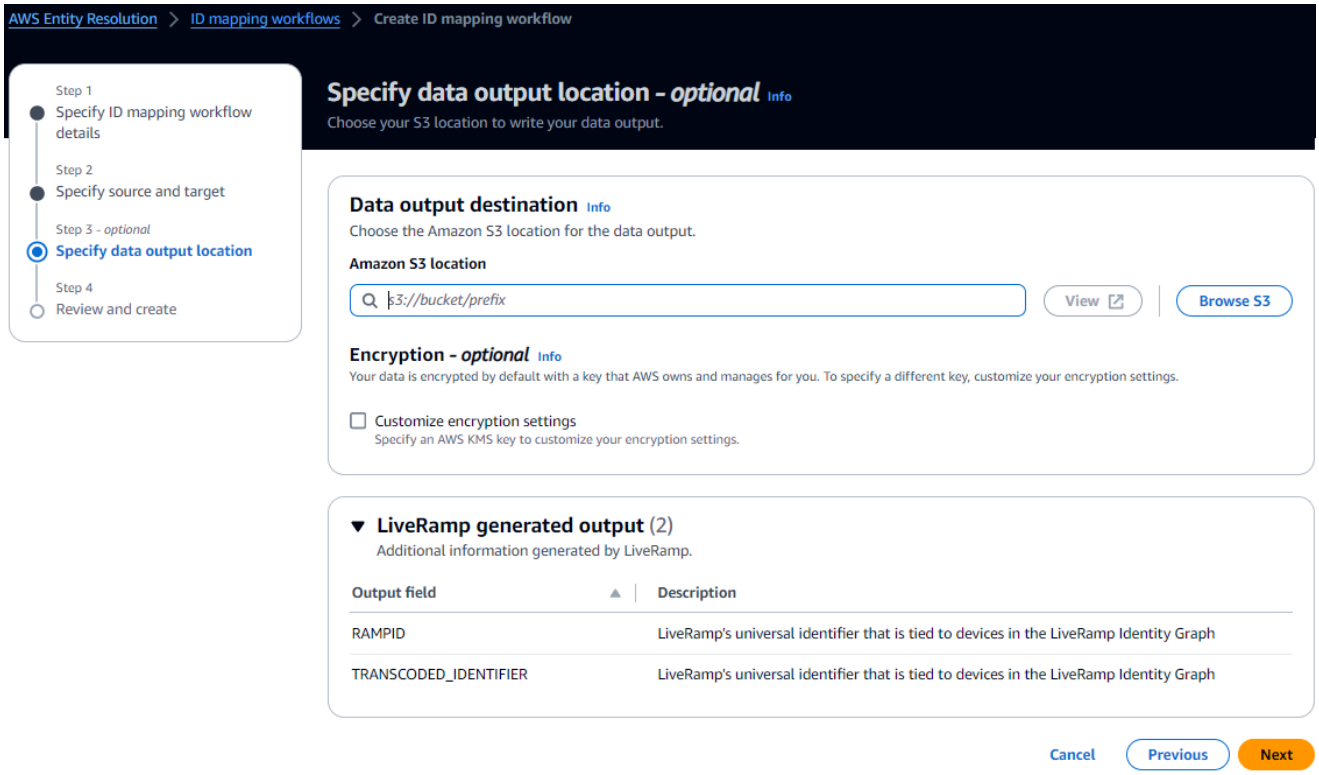
c. Vea la salida LiveRamp generada.

   Esta es la información adicional generada por LiveRamp.

d. Para la salida de datos, consulte todos los campos incluidos y determine si desea incluir, ocultar o enmascarar los campos.

> **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.

Si desea...	Entonces elija...
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.
   - Los ID de coincidencia únicos generados.
   - 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.

Ya puede hacer lo siguiente:

- Edita un flujo de trabajo coincidente
- Elimine un flujo de trabajo coincidente

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 identificadores TransUnion individuales y familiares. TransUnionproporciona 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.

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

            },
```

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

Sustituya cada uno <user input placeholder>por su propia información.

cubeta de almacenamiento	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. Inicia sesión en la AWS Entity Resolution consola AWS Management Console y ábrela con tu Cuenta de AWS (si aún no lo has hecho).
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.

   d. Especifique los permisos de Acceso a servicios seleccionando Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

Si eliges...	Entonces
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, puede elegir la opción Estos datos se cifran con una clave de KMS y, a continuación,

Si eliges...	Entonces
	introducir una AWS KMS clave que se utilizará para descifrar los datos introducidos.
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. Para ver la función de servicio, seleccione el enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de roles 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.

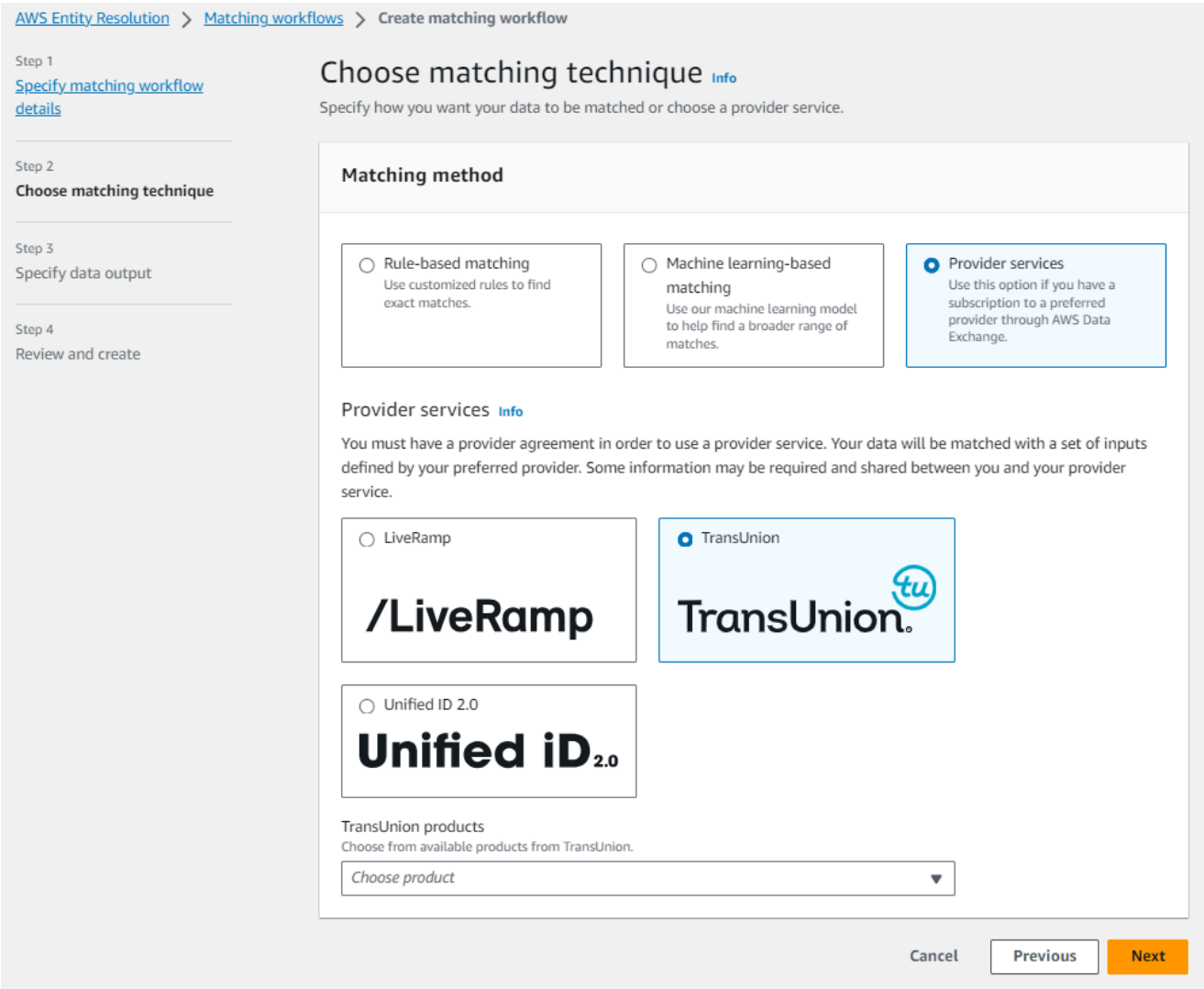
5. Para el paso 2: elija una técnica de coincidencia:

   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 TransUnion los productos, elige un producto de la lista desplegable.



d. 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 “Cree un rol de trabajo de flujo de trabajo para AWS Entity Resolution”.

6. Seleccione 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. Para la salida de datos, consulte todos los campos incluidos y determine si desea incluir, ocultar o enmascarar los campos.

Si desea...	Entonces elija...
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.
   - Los ID de coincidencia únicos generados.
   - 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.

Ya puede hacer lo siguiente:

- Edita un flujo de trabajo coincidente
- Elimine un flujo de trabajo coincidente

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 del ecosistema publicitario que utilizan el UID2. 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 utilizar uno **`Email Address`** o varios tipos de generación **`Phone number`** de UID2 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 no **`Email Address`** lo esté. A continuación, cree un segundo flujo de trabajo con este nuevo mapeo de esquemas.

> **Note**
>
> Los UID2 sin procesar se crean añadiendo sales de cubos de sal que se giran aproximadamente una vez al año, lo que hace que el UID2 sin procesar también gire con ellas, por lo que se recomienda actualizar los UID2 sin procesar a diario. Para obtener más how-often-should-uid información, consulte https://unifiedid.com/docs/getting-started/gs-faqs # 2 -incremental-updates s-be-refreshed-for

Para crear un flujo de trabajo coincidente con UID 2.0:

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS (si aún no lo has hecho).
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. Especifique los permisos de Acceso a servicios seleccionando Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

Si eliges...	Entonces
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, puede elegir la opción Estos datos se cifran con una clave de KMS y, a continuación, introducir una AWS KMS clave que se utilizará para descifrar los datos introducidos.

Si eliges...	Entonces
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. Para ver la función de servicio, seleccione el enlace externo Ver en IAM. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de roles existente para añadir los permisos necesarios.

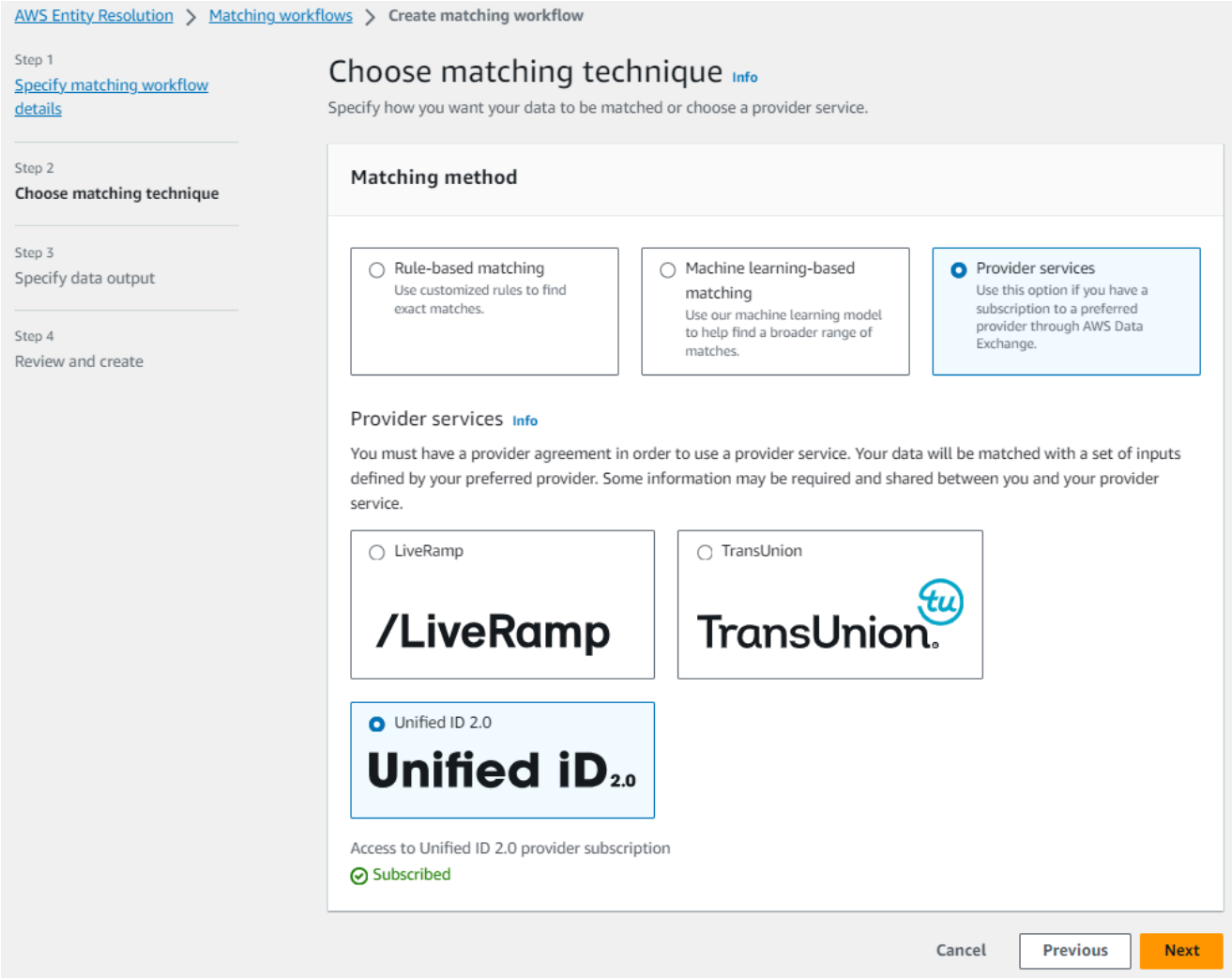
e. (Opcional) Para habilitar las etiquetas para el recurso, selecciona Añadir nueva etiqueta y, a continuación, introduce el par clave y valor.

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, vea todos los campos que se incluyen y determine si desea incluir, ocultar o enmascarar los campos.

Si desea...	Entonces elija...
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.
   - Los ID de coincidencia únicos generados.
   - 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.

Ya puede hacer lo siguiente:

- Edita un flujo de trabajo coincidente
- Elimine un flujo de trabajo coincidente

Ejecute un flujo de trabajo coincidente

Después de crear un flujo de trabajo de coincidencia basado en reglas o en aprendizaje automático con el tipo de procesamiento manual, puede ejecutar un trabajo de flujo de trabajo coincidente.

> **Note**
>
> Si crea un flujo de trabajo coincidente con el tipo de procesamiento automático, los trabajos de flujo de trabajo coincidentes se ejecutarán cada vez que se actualice una entrada de datos.

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 coincidentes.

- Si especificó la técnica de coincidencia basada en reglas, también AWS Entity Resolution asignará el número de regla aplicado que generó la coincidencia.
- Si especificó la técnica de coincidencia basada en el aprendizaje automático, también AWS Entity Resolution asignará el porcentaje del nivel de confianza de la coincidencia.

AWS Entity Resolution a continuación, escribe los archivos de salida de datos en la ubicación que elija.

Un flujo de trabajo 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 y la carpeta contendrá varios archivos, cada uno de los cuales contendrá 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 trabajo.

Para ejecutar un flujo de trabajo coincidente:

1. Inicia sesión AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS (si aún no lo has hecho).
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 Ejecutar flujo de trabajo.

   Aparece un mensaje que indica que el trabajo ha comenzado.
5. En la pestaña Métricas, en Historial de trabajos, consulta lo siguiente:

   - El estado del trabajo de flujo de trabajo coincidente: en curso, completado o fallido
   - El número de registros procesados.
   - El número de coincidencias encontradas.
   - El número de registros únicos.
   - La duración del trabajo.
   - El identificador del trabajo.
6. 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.

Siguientes pasos

Ya puede hacer lo siguiente:

- Edita un flujo de trabajo coincidente
- Elimine un flujo de trabajo coincidente

Crear un espacio de nombres de ID

Un espacio de nombres de ID es un envoltorio alrededor de la tabla de datos que se utiliza para proporcionar metadatos que explican los datos 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: de origen y de 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.

Los siguientes temas lo guían a través de una serie de pasos para crear los espacios de nombres de los ID de origen y destino y, a continuación, especificar la salida de datos en Amazon Simple Storage Service (Amazon S3).

> **Note**
>
> AWS Entity Resolution actualmente ofrece la LiveRamp transcodificación del método de espacio de nombres de ID al crear un espacio de nombres de ID.

Temas

Crea una fuente de espacio de nombres de ID

En este tema se describe el proceso de creación de una fuente de espacio de nombres de ID en la consola.AWS Entity Resolution Esta es la fuente de los datos 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

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS, si aún no lo has hecho.
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. Consulta el método del espacio de nombres de ID.

   > **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, consulteSuscríbase 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 Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

Si eliges...	Entonces
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, 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.

Si eliges...	Entonces
Usar un rol de servicio existente	Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos para enumerar funciones, aparecerá la lista de funciones. Si no tiene permisos para enumerar funciones, puede introducir el nombre de recurso de Amazon (ARN) de la función que quiere usar. Si no hay ningún rol de servicio existente, la opción de usar un rol de servicio existente no estará disponible. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de roles 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. Selecciona Crear espacio de nombres de ID.

Crea un objetivo de espacio de nombres de ID

En este tema se describe el proceso de creación de un destino de espacio de nombres de ID en la consola.AWS Entity Resolution Este es el destino de los datos en un flujo de trabajo de mapeo de ID. Todas las fuentes apuntan al objetivo.

Para crear un objetivo de espacio de nombres de ID

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS, si aún no lo has hecho.
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. Vea el método del espacio de nombres de ID.

   > **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, consulteSuscríbase 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. Selecciona Crear espacio de nombres de ID.

Después de crear los espacios de nombres de ID necesarios para un flujo de trabajo de mapeo de ID en dos Cuentas de AWS, estará listo para crear el flujo de trabajo de mapeo de ID.

Creación de un flujo de trabajo de mapeo de ID

El flujo de trabajo de mapeo de ID 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 LiveRamp para realizar la transcodificación. Con la LiveRamp transcodificación, puede traducir un conjunto de RampID de origen 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.

Puede realizar un mapeo de ID entre dos conjuntos de datos por su cuenta Cuenta de AWS o entre dos conjuntos de datos diferentes. Cuentas de AWS La fuente y el destino de entrada de datos dependen del tipo de mapeo de ID que desee realizar.

Para obtener más información, consulte Realizar traducciones mediante ADX en el sitio web de LiveRamp documentación.

Temas

Requisito previo

Este flujo de trabajo de mapeo de ID requiere 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. Antes de crear un flujo de trabajo de mapeo de ID LiveRamp, añada la siguiente política de permisos, que le permitirá acceder al depósito de almacenamiento provisional de datos.

```
{
    "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.

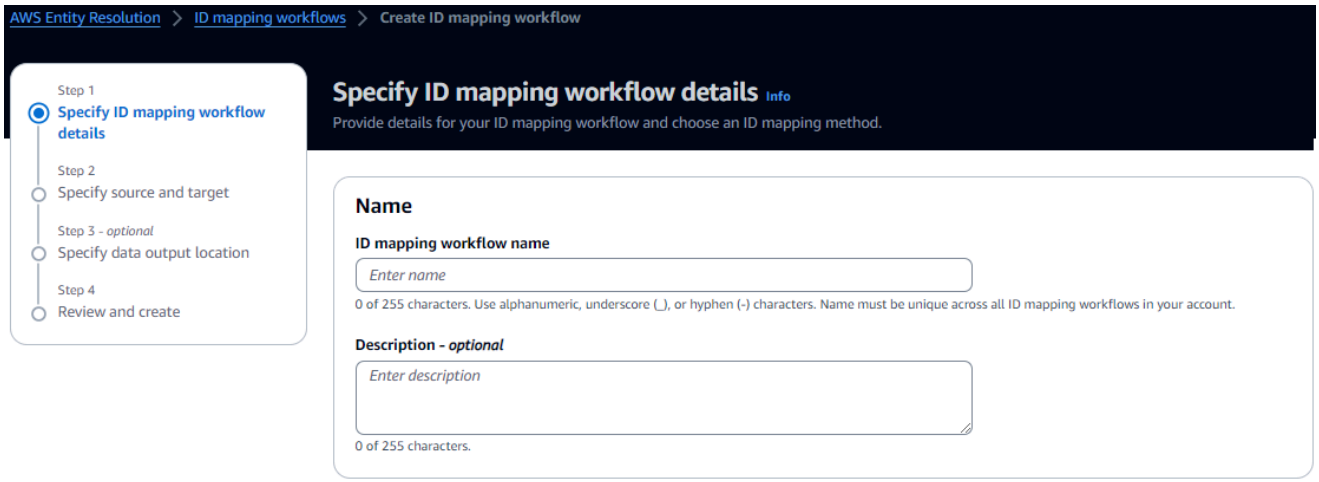
Crear un flujo de trabajo de mapeo de ID para uno Cuenta de AWS

Tras completar los pasos de configuración y crear un esquema de mapeo, puede crear uno o más flujos de trabajo de mapeo de ID para convertir un conjunto de RAMPID de origen en otro utilizando RAMPID mantenidos o derivados.

Para crear un flujo de trabajo de mapeo de ID para un Cuenta de AWS

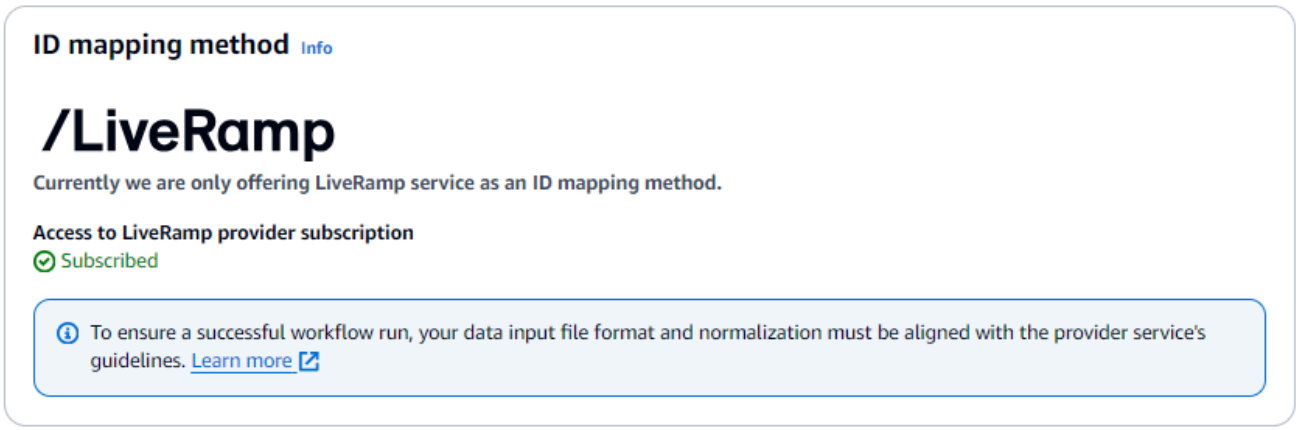
1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS, si aún no lo has hecho.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona el mapeo de ID.
3. En la página de flujos de trabajo de mapeo de ID, en la esquina superior derecha, 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. Vea el método de mapeo de ID.

      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, consulteSuscríbase 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)

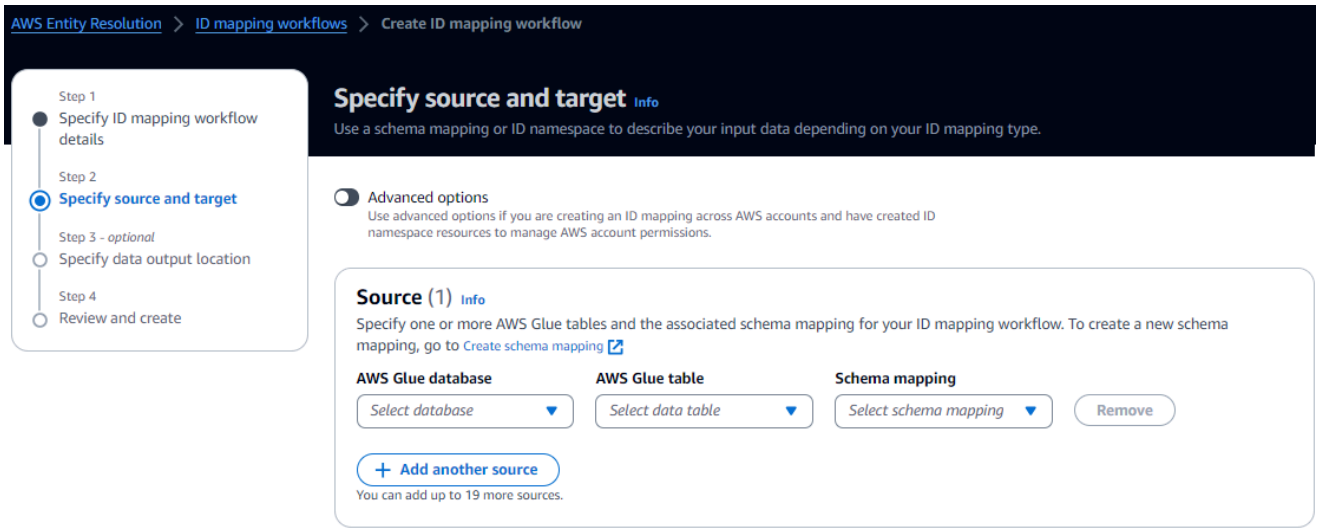
d. (Opcional) Para habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.

e. Elija Siguiente.

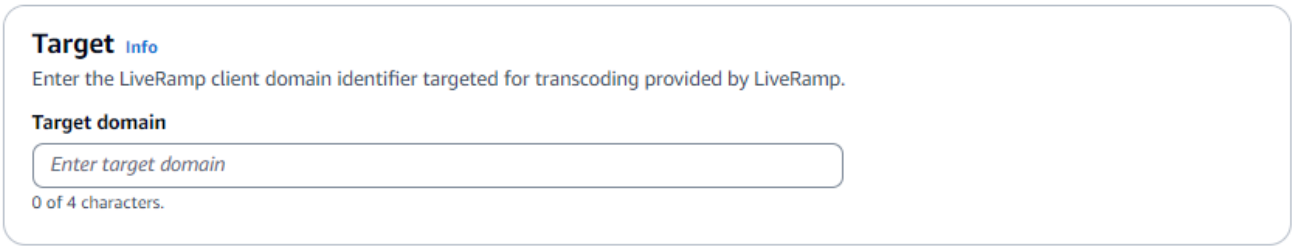
5. Para el paso 2: especificar el origen y el destino, haga lo siguiente:

a. En Origen, seleccione una AWS Gluebase de datos en el menú desplegable, seleccione la AWS Glue tabla y, a continuación, seleccione el mapeo de esquema correspondiente.

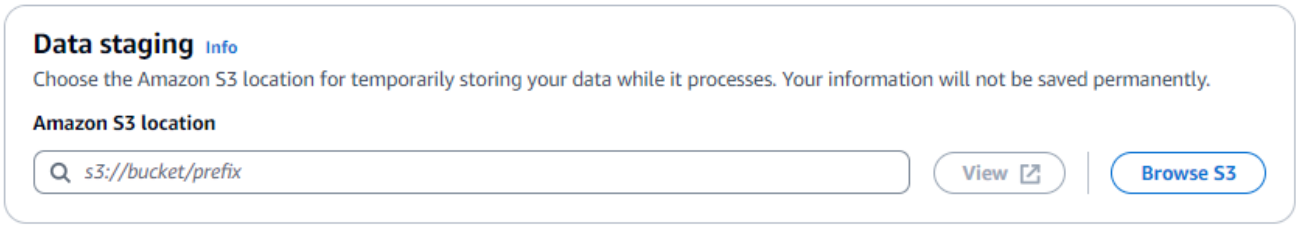
   Puede añadir hasta 19 entradas de datos.



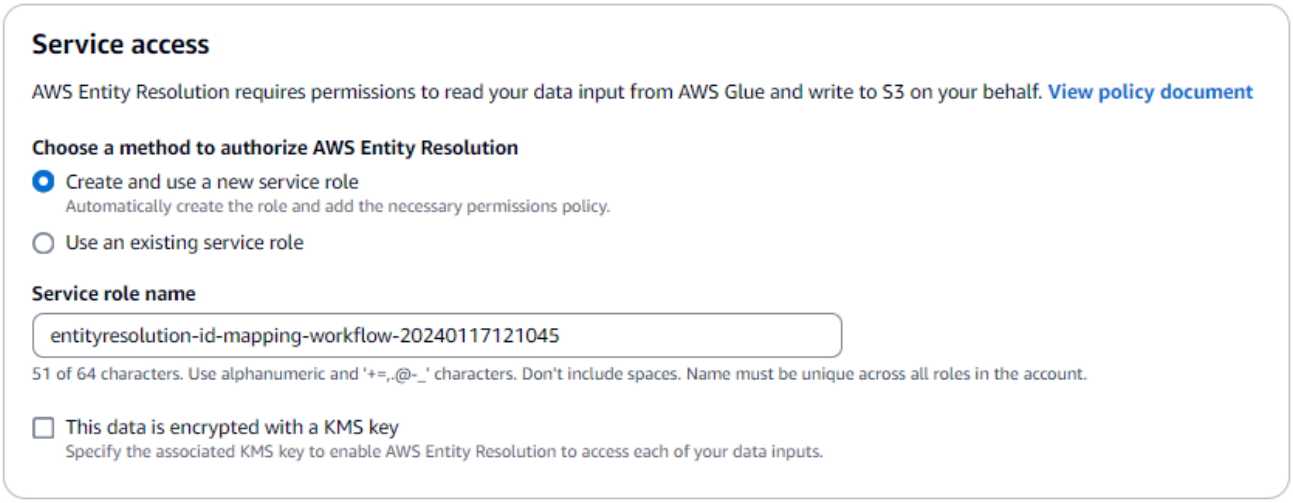
b. En Target, introduzca el identificador de dominio del LiveRamp cliente destinado a la transcodificación que LiveRamp proporciona.



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.



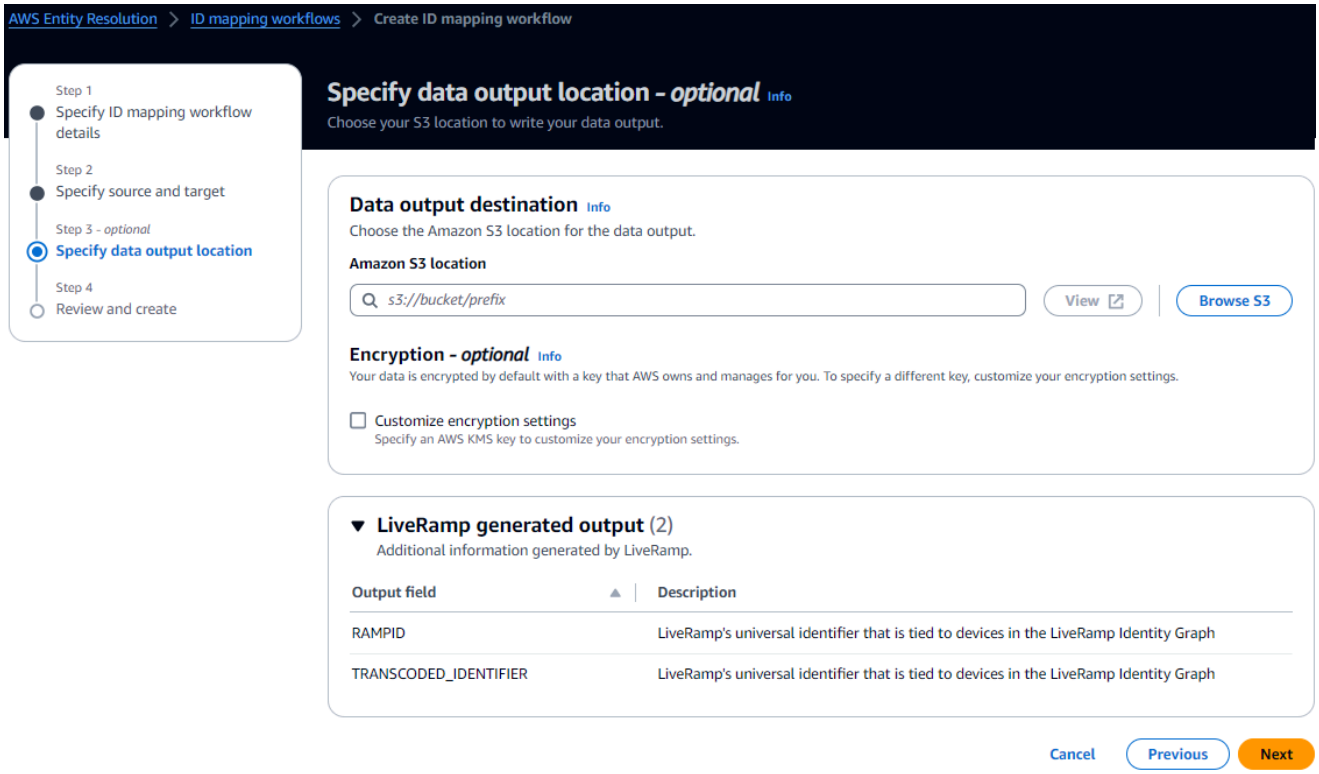
d. Para especificar los permisos de acceso al servicio, elija Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.



Si eliges...	Entonces
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, 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.

Si eliges...	Entonces
Usar un rol de servicio existente	Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos para enumerar funciones, aparecerá la lista de funciones. Si no tiene permisos para enumerar roles, puede introducir el nombre de recurso de Amazon (ARN) del rol que quiere usar. Si no hay ningún rol de servicio existente, la opción de usar un rol de servicio existente no estará disponible. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de roles existente para añadir los permisos necesarios.

6. Elija Siguiente.
7. En 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

Crear un flujo de trabajo de mapeo de ID a través de dos Cuentas de AWS

Requisito previo

Para crear un flujo de trabajo de mapeo de identidades entre dos personas se Cuentas de AWS necesita permiso LiveRamp para acceder al bucket de S3 y a la clave AWS Key Management Service (AWS KMS) gestionada 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.

```
{
    "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.

Cree un flujo de trabajo de mapeo de ID

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

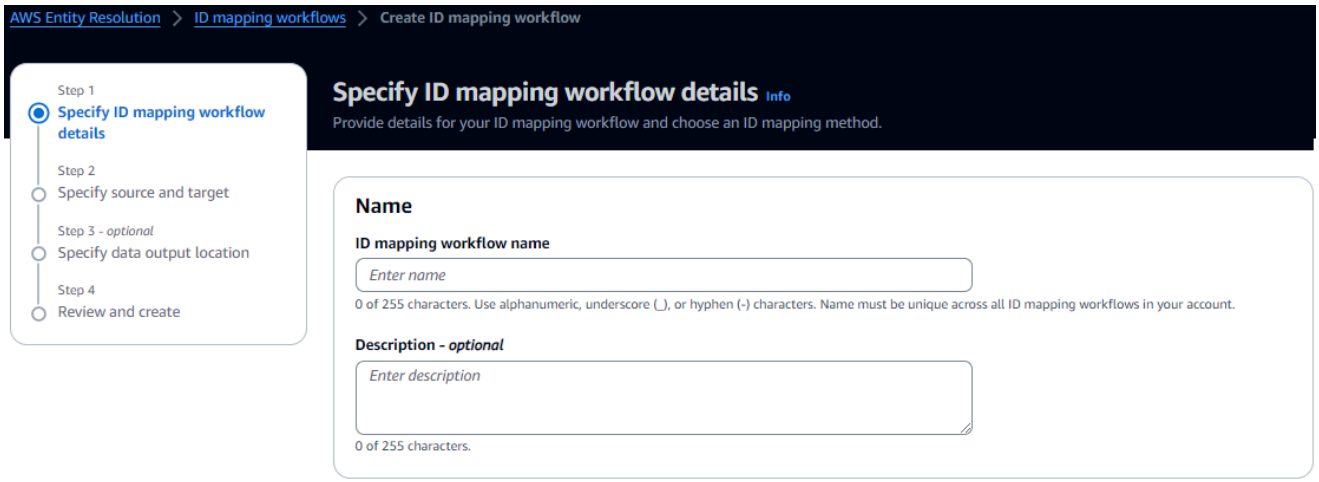
- Complete el requisito previo para añadir los permisos a la clave gestionada por el cliente.
- Completar las tareas de Con AWS Entity Resolution figuración.
- Cree una fuente de espacio de nombres de ID.
- Crea un objetivo de espacio de nombres de ID.

Tras completar las tareas enumeradas anteriormente, puede crear uno o más flujos de trabajo de mapeo de ID para convertir un conjunto de RAMPID de origen en otro utilizando RAMPID mantenidos o derivados.

Para crear un flujo de trabajo de mapeo de ID en dos Cuentas de AWS

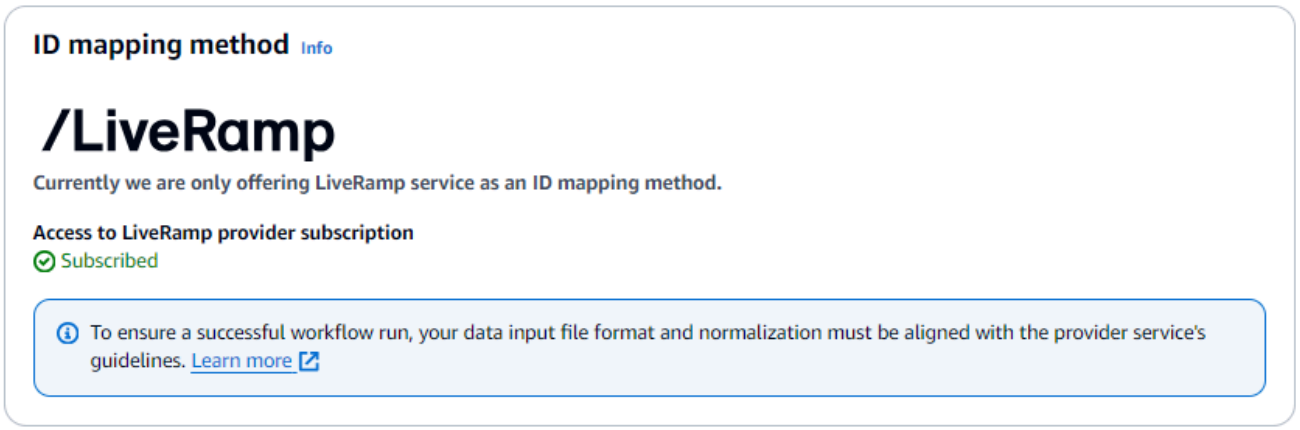
1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS, si aún no lo has hecho.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona el mapeo de ID.
3. En la página de flujos de trabajo de mapeo de ID, en la esquina superior derecha, 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. Vea el método de mapeo de ID.

    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, consulteSuscríbase 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)

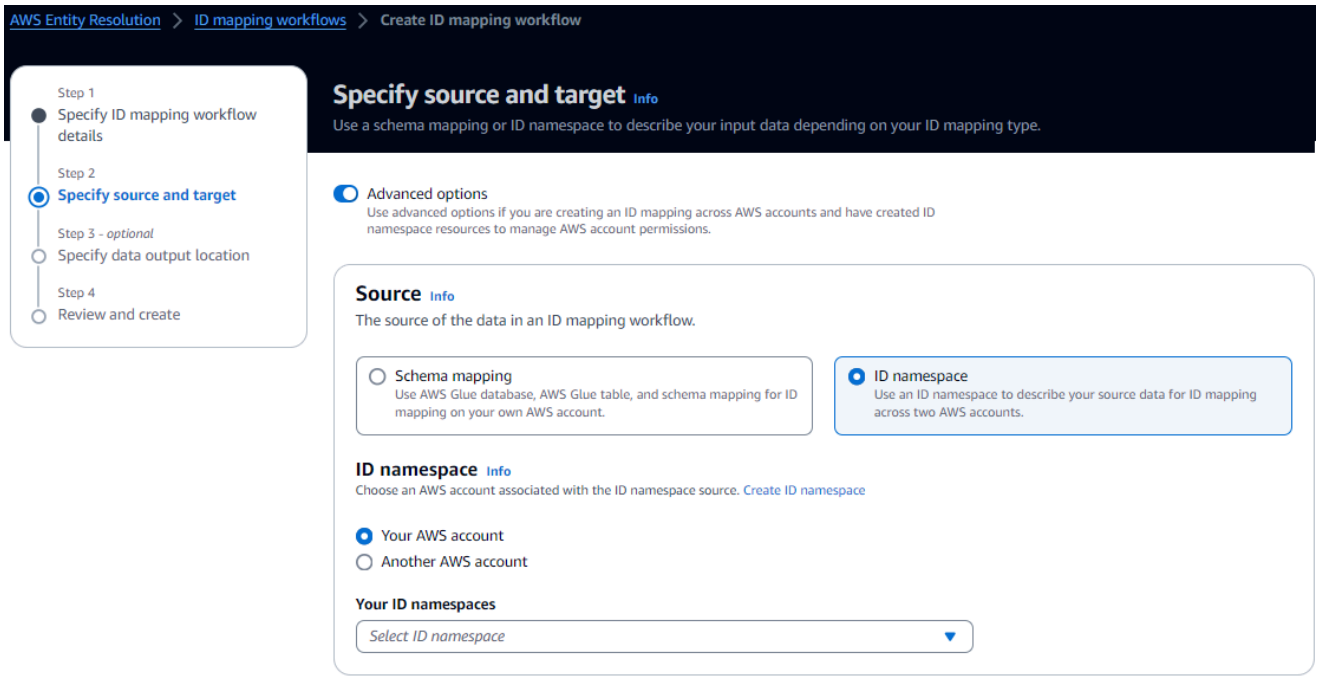
d. (Opcional) Para habilitar las etiquetas para el recurso, elija Agregar nueva etiqueta y, a continuación, introduzca el par clave y valor.

e. Elija Siguiente.

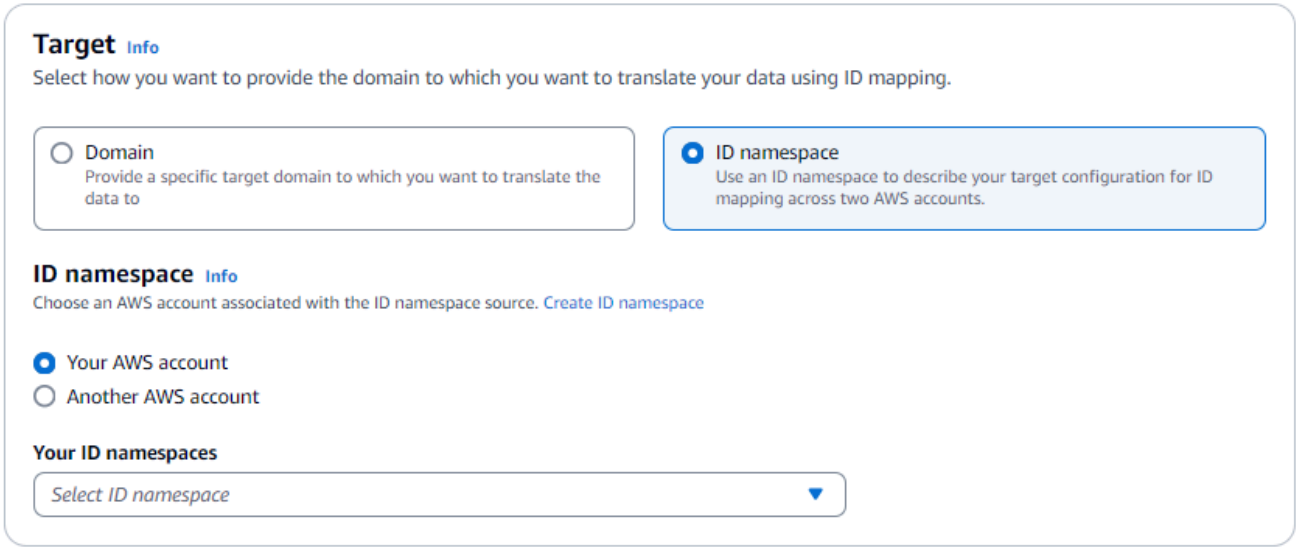
5. Para el paso 2: especificar el origen y el destino, haga lo siguiente:

a. Activa las opciones avanzadas.

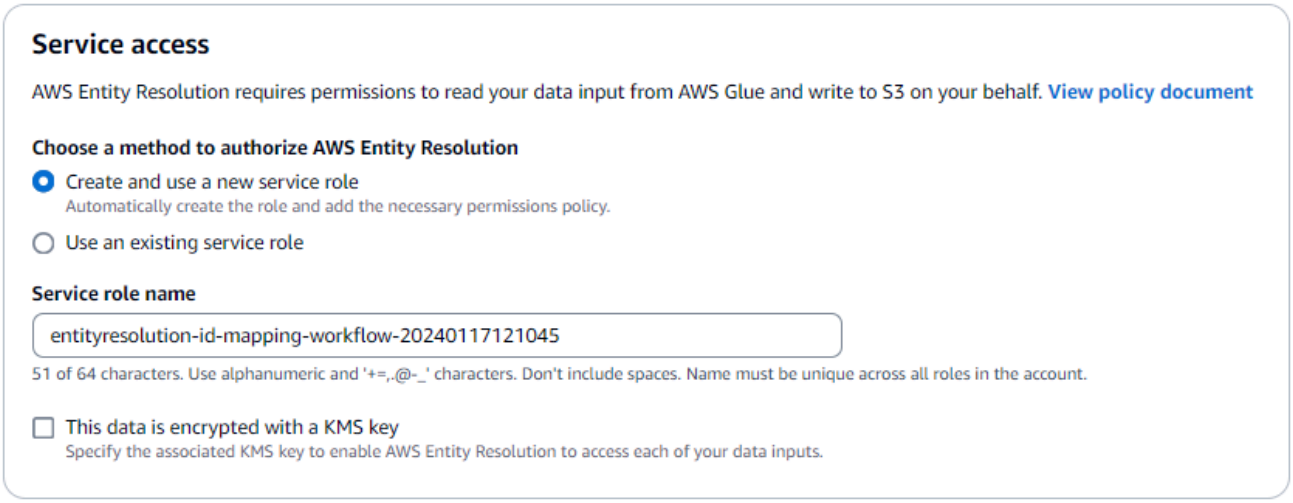
b. En Fuente, selecciona el espacio de nombres de ID.



c. En Target, elige el espacio de nombres de ID.



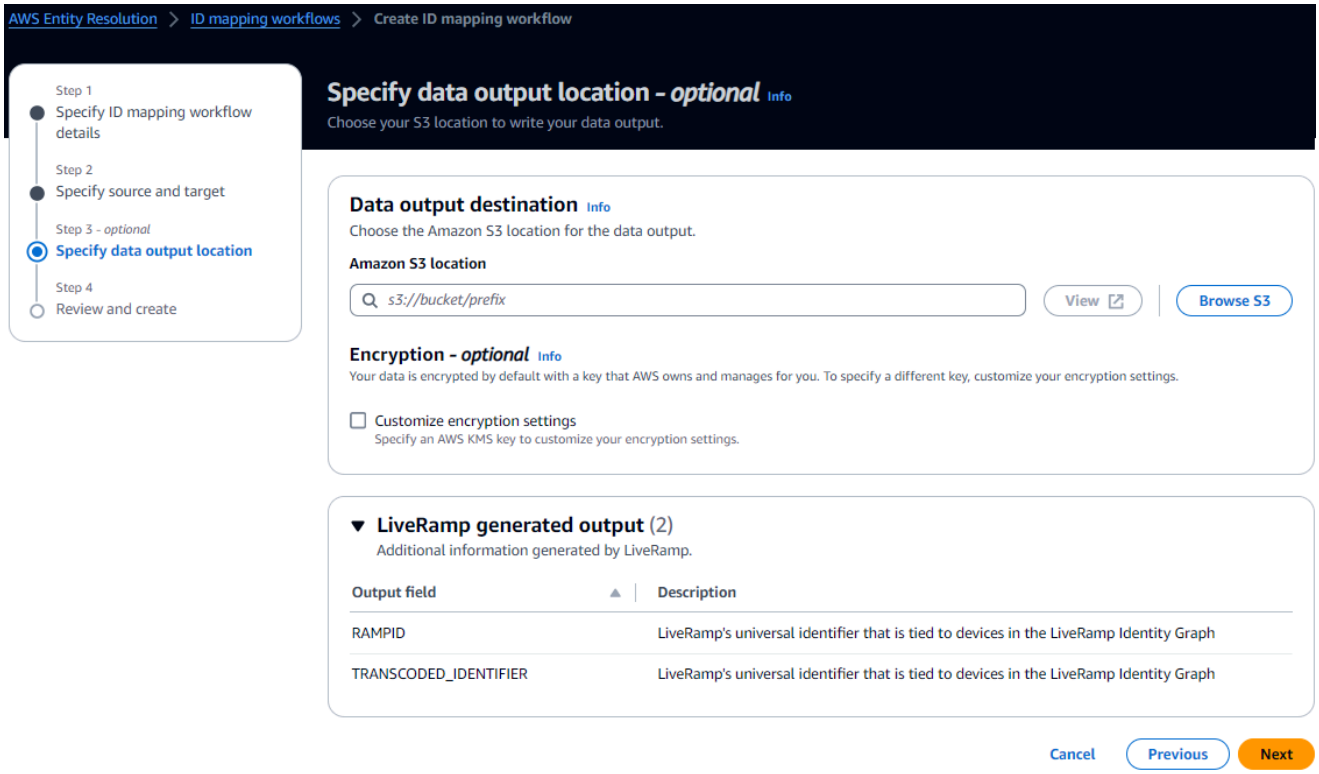
d. Para especificar los permisos de acceso al servicio, elija Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.



Si eliges...	Entonces
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, 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.

Si eliges...	Entonces
Usar un rol de servicio existente	Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos para enumerar funciones, aparecerá la lista de funciones. Si no tiene permisos para enumerar roles, puede introducir el nombre de recurso de Amazon (ARN) del rol que quiere usar. Si no hay ningún rol de servicio existente, la opción de usar un rol de servicio existente no estará disponible. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de roles existente para añadir los permisos necesarios.

6. Elija Siguiente.
7. En 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.

Para ejecutar un flujo de trabajo de mapeo de ID

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con la tuya Cuenta de AWS, si aún no lo has hecho.

2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona el mapeo 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. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS, si aún no lo has hecho.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona el mapeo 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 Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

Si eliges...	Entonces
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, 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	Seleccione un Nombre de rol de servicio existente en la lista desplegable.

Si eliges...	Entonces
	Si tiene permisos para enumerar funciones, aparecerá la lista de funciones. Si no tiene permisos para enumerar roles, puede introducir el nombre de recurso de Amazon (ARN) del rol que quiere usar. Si no hay ningún rol de servicio existente, la opción de usar un rol de servicio existente no estará disponible. De forma predeterminada, AWS Entity Resolution no intenta actualizar la política de roles existente para añadir los permisos necesarios.

7. Elija 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`.

Administrar AWS Entity Resolution

En los temas siguientes se explica cómo gestionar los flujos de trabajo mediante la AWS Entity Resolution consola.

Para obtener información sobre cómo gestionar el AWS Entity Resolution uso de los AWS SDK, consulta la referencia de la AWS Entity Resolution API.

Temas

Administrar las asignaciones de esquemas

En los temas siguientes se explica cómo gestionar las asignaciones de esquemas mediante la consola. AWS Entity Resolution

Temas

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 AWS Management Console y abra la AWS Entity Resolution consola con la suya Cuenta de AWS, si aún no lo ha hecho.

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.

Edite un esquema de mapeo

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 con la suya Cuenta de AWS, si aún no lo ha hecho.
2. En el panel de navegación izquierdo, en Preparación de datos, selecciona Asignaciones de esquemas.
3. Elija el mapeo de esquemas.
4. Elija 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.
9. En la página Revisar y guardar, realice los cambios necesarios y, a continuación, seleccione Editar mapeo de esquemas.

Elimine un mapeo de esquemas

No se 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 con la suya Cuenta de AWS, si aún no lo ha hecho.
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.

Administrar flujos de trabajo coincidentes

Después de crear un flujo de trabajo de emparejamiento basado en reglas, basado en aprendizaje automático o basado en servicios de proveedores, puede administrar los flujos de trabajo coincidentes de las siguientes maneras.

Temas

Edita un flujo de trabajo coincidente

Para editar un flujo de trabajo coincidente:

1. Inicia sesión AWS Management Console y abre la AWS Entity Resolution consola con la tuya Cuenta de AWS, si aún no lo has hecho.
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.
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.
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.

Elimine un flujo de trabajo coincidente

Para eliminar un flujo de trabajo coincidente:

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS, si aún no lo has hecho.
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.

Busca un identificador de coincidencia para un flujo de trabajo coincidente basado en reglas

Después de ejecutar un flujo de trabajo de coincidencia basado en reglas, puede encontrar el ID de coincidencia correspondiente y la regla asociada a los registros procesados.

Para encontrar un identificador de coincidencia para un flujo de trabajo de coincidencia basado en reglas:

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS, si aún no lo has hecho.
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 Buscar ID coincidente.
5. Realice una de las siguientes acciones siguientes:

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.

6. Amplíe las reglas de coincidencia.
7. Introduzca un valor para cada clave de coincidencia.

   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.

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

8. Elija Look up (Buscar).
9. Consulta el identificador de coincidencia correspondiente y la regla asociada que se utilizó para la coincidencia.

Elimine los 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 ML.

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

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS, si aún no lo has hecho.
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, selecciona Eliminar identificadores únicos en la lista desplegable Acciones.
5. Introduce el identificador único que deseas eliminar en la sección de identificadores únicos.

   Puedes introducir hasta 10 identificadores únicos.
6. Especifique la fuente de entrada desde la que se eliminarán los ID únicos.

   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, los ID únicos de las demás fuentes de entrada no se verán afectados.
7. Selecciona Eliminar identificadores únicos.

Administrar los espacios de nombres de ID

Puede administrar los espacios de nombres de ID de las siguientes maneras.

Temas

- Edita un espacio de nombres de ID

- Elimina un espacio de nombres de ID
- Agregue o actualice una política de recursos

Edita un espacio de nombres de ID

Solo puede 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. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS (si aún no lo has hecho).
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 Editar.
5. En la página Editar el espacio de nombres de ID, realiza los cambios necesarios y, a continuación, selecciona Guardar.

Elimina 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 esquema de mapeo de todo el flujo de trabajo de mapeo de ID asociado para poder eliminarlo.

Para eliminar un espacio de nombres de ID:

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS (si aún no lo has hecho).
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.

Agregue o actualice una política de recursos

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

Para añadir o actualizar una política de recursos

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con la tuya Cuenta de AWS, si aún no lo has hecho.
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. Elija Guardar cambios.

Administrar los flujos de trabajo de mapeo

Puede gestionar los flujos de trabajo de mapeo de ID de las siguientes maneras.

Temas

Edite un flujo de trabajo de mapeo de ID

Para editar un flujo de trabajo de mapeo de ID:

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con tu Cuenta de AWS, si aún no lo has hecho.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona el mapeo 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.

Elimine un flujo de trabajo de mapeo de ID

Para eliminar un flujo de trabajo de mapeo de ID:

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con la tuya Cuenta de AWS, si aún no lo has hecho.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona el mapeo 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.

Agregue o actualice una política de recursos

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

Para añadir o actualizar una política de recursos

1. Inicia sesión en AWS Management Console y abre la AWS Entity Resolution consola con la tuya Cuenta de AWS, si aún no lo has hecho.
2. En el panel de navegación izquierdo, en Flujos de trabajo, selecciona el mapeo 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. Elija Guardar cambios.

Solución de problemas de trabajo

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

He recibido un archivo de errores.

Los registros del archivo de errores se pueden 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
- Uno de los campos del mapeo del esquema incluye un nombre reservado:
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - MatchID
  - HashingProtocol
  - ConfidenceLevel
  - Origen

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.

Seguridad en AWS Entity Resolution

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS 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 ejecuta Servicios de AWS en Nube de AWS. Además, AWS proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWSProgramas de conformidad de . Para obtener información sobre los programas de conformidad que se aplican a AWS Entity Resolution, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el Servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Entity Resolution. En los siguientes temas, se le mostrará cómo configurar AWS Entity Resolution para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayudarán a supervisar y a proteger los recursos de AWS Entity Resolution.

Temas

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. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es 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, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte 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:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS 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
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice 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 140-2 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, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

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 AWS Entity Resolution o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos 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.

El 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 administrada 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 concesión 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 las AWS Management Console API o las AWS KMS API.

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 de MAC) y los algoritmos que admite la clave KMS. AWS Entity Resolution valida que `KeySpec` es y es`SYMMETRIC_DEFAULT`. `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 `CreateIdMappingWorkflowStartIdMappingJob`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:

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

Sustituya cada uno <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 un KMSarn, que se AWS Entity Resolution utiliza para cifrar los datos personales identificables almacenados en el recurso.

KMSarn: introduzca un ARN clave, que es un identificador clave para una clave gestionada por el cliente. AWS KMS

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 un KMSarn, que se AWS Entity Resolution utiliza para cifrar los datos personales identificables almacenados en el recurso.

KMSarn: introduzca un ARN clave, que es un identificador clave para una clave gestionada por el cliente. AWS KMS

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 administrada 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.

Acceso 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.

No 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 el tema Acceso a recursos entre cuentas en 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 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 ayudarlo 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 administrador 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. 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 administrador 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 cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS 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 Uso de la autenticación multifactor (MFA) en AWSen 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 utilice 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, consulte 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 utilice 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, consulte ¿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, consulte 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 puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo 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 permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) 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 determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM 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, puede 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 para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza 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 pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede 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 conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte el tema sobre el acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realiza una llamada en un servicio, es común 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 ellas AWS, se te considera director. 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, consulte 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 puede 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 puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un AWS rol a una instancia EC2 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 a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) 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, consulte 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 puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice 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 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.

Las políticas basadas en identidades pueden 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 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. 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 pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede 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 (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL 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 que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de 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 pueden 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 puede conceder a una entidad de IAM (usuario o rol de IAM). Puede 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, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP 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 gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus 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 acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- 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 pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte 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 AWS determinar 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
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
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 adjunto. Para 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 dentro de 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. 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 pueden utilizarlos para controlar el acceso a un recurso específico.

Para el recurso al que se asocia la política, la política define qué acciones puede 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 en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para AWS Entity Resolution

Admite acciones de política	Sí

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.

El elemento `Action` de una política JSON describe las acciones que puede 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

Admite 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 puede 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). Puede 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, utilice 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 ARN, consulte los recursos definidos por AWS Entity Resolution en la Referencia de autorización de servicios. 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

Admite 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 puede 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. Puede crear expresiones condicionales que utilicen 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 única 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 puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede 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, consulte 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

ACL en AWS Entity Resolution

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AWS Entity Resolution

Admite 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 ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AWS Entity Resolution

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que 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 más información sobre el cambio de roles, consulte Cambio a un rol (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 más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS Entity Resolution

Admite Forward access sessions (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 detallada sobre las políticas a la hora de realizar solicitudes de FAS, consulte Forward access sessions.

Roles de servicio para AWS Entity Resolution

Compatible 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**
>
> Si se cambian los permisos de un rol de servicio, es posible que se interrumpa 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

Compatible 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 puede 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 puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte 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 puede crear

políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden 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 en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por cada uno de los tipos de recursos AWS Entity Resolution, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de la Referencia de autorización de servicios. AWS Entity Resolution

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, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo 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 pueden 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, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede 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, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice 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 Política de validación de Analizador de acceso de IAM en la Guía de 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 solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las 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 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 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 administradas 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: AWSEntityResolutionConsoleFullAccess

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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EntityResolutionAccess",
            "Effect": "Allow",
            "Action": [
                "entityresolution:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GlueSourcesConsoleDisplay",
            "Effect": "Allow",
            "Action": [
```

```
                "glue:GetSchema",
                "glue:SearchTables",
                "glue:GetSchemaByDefinition",
                "glue:GetSchemaVersion",
                "glue:GetSchemaVersionsDiff",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetTableVersion",
                "glue:GetTableVersions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3BucketsConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3SourcesConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:ListBucketVersions",
                "s3:GetBucketVersioning"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TaggingConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSConsoleDisplay",
```

```
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListRolesToPickRoleForPassing",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PassRoleToEntityResolutionService",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*entityresolution*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "entityresolution.amazonaws.com"
                    ]
                }
            }
        },
        {
           "Sid": "ManageEventBridgeRules",
           "Effect": "Allow",
           "Action": [
              "events:PutRule",
              "events:DeleteRule",
              "events:PutTargets",
           ],
           "Resource": [
                "arn:aws:events:*:*:rule/entity-resolution-automatic*"
           ]
        },
        {
            "Sid": "ADXReadAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "dataexchange:GetDataSet"
            ],
            "Resource": "*"
        },
    ]
}
```

AWS política gestionada: AWSEntityResolutionConsoleReadOnlyAccess

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EntityResolutionRead",
            "Effect": "Allow",
            "Action": [
                "entityresolution:Get*",
                "entityresolution:List*"
            ],
            "Resource": "*"
        },
    ]
}
```

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 servicios del proveedor en el flujo de trabajo correspondiente.	16 de octubre de 2023
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 habituales 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 administrador 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

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que

asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para 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, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer la diferencia entre usar roles y políticas basadas en recursos para el acceso entre cuentas, consulte el tema 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:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.

- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con 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, consulte 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.

Resiliencia en AWS Entity Resolution

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes

y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. 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 centros de datos únicos o múltiples.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, AWS Entity Resolution ofrece varias características que le ayudan con sus necesidades de resiliencia y copia de seguridad de los datos.

Monitorización 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 dirección 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.

Temas

Registro de 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 a AWS Entity Resolution qué dirección IP 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 lo 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 CloudTrail UserIdentity.

Descripción AWS Entity Resolution de las entradas de los archivos de 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.

Creación de recursos de AWS Entity Resolution 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 de . 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	Ajustable	Descripción
Trabajos de mapeo de ID simultáneos	1	No	El número máximo de trabajos de mapeo de ID que se pueden procesar simultáneamente en el actual. Región de AWS
Trabajos coincidentes simultáneos	1	No	El número máximo de trabajos coincidentes que se pueden procesar simultáneamente en el actual. Región de AWS
El proveedor presta servicios simultáneos que coinciden con los trabajos	1	No	El número máximo de trabajos coincidentes del servicio del proveedor que se pueden procesar simultáneamente en el actual. Región de AWS
Entrada de datos	20	No	Esta es la lista de tablas de entrada que desea utilizar en un flujo de trabajo de coincidencias. Cada entrada

Nombre	Valor predeterminado	Ajustable	Descripción
			corresponde a una columna de la tabla de datos AWS Glue de entrada, que contiene el nombre de la columna e información adicional que se AWS Entity Resolution utiliza con fines de comparación. Las entradas deben contener un identificador único más al menos un campo de entrada adicional.
Salida de datos	750	No	Esta es una lista de `OutputAttribute` objetos, 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.
Esquema de datos	25	No	El número máximo de campos de entrada del esquema de datos.
Flujos de trabajo de mapeo	10	Sí	El número máximo de flujos de trabajo de mapeo de ID que puede crear Cuenta de AWS en este momento Región de AWS.
Espacios de nombres de ID	10	Sí	El número máximo de espacios de nombres de ID que se pueden crear en este Cuenta de AWS espacio en el actual. Región de AWS
Identificadores de coincidencias	500	No	El número máximo de registros que se pueden consolidar en un MatchID por carga de trabajo.

Nombre	Valor predeterminado	Ajustable	Descripción
Regla de coincidencia	15	No	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.
Coincidir con flujos	10	Sí	El número máximo de flujos de trabajo de coincidencias.
Número de reglas por flujo de trabajo	15	No	El número máximo de reglas por flujo de trabajo de coincidencias.
Tasa de solicitudes de API `GetMatchId`	50	Sí	El número máximo de solicitudes de `GetCustomerID` API por segundo.
Asignaciones de esquemas	50	Sí	El número máximo de mapeos de esquemas que puede crear en esta cuenta en la región actual. AWS
Claves de coincidencia únicas por conjunto de reglas	15	No	El número máximo de claves de coincidencia únicas por conjunto de reglas. Una clave de coincidencia indica AWS Entity Resolution qué campos de entrada deben considerarse datos similares y cuáles deben considerarse 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.

Cuotas de limitación controlada de la API

Recurso	Predeterminado	Descripción
Tasa de solicitudes de `GetMatchId`	50 TPS	Número máximo de llamadas a la `GetMatchId` 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
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
CloudFormation Recursos de AWS: recursos nuevos y actualizados	AWS Entity Resolution agregó los siguientes recursos: `AWS::EntityResolut ion::IdNamespace` `AWS::EntityResolut ion::PolicyStateme nt` y actualizó el siguiente recurso:`AWS::Enti tyResolution::IdMa ppingWorkflow` .	2 de abril de 2024

Encuentra el ID de coincidencia	Los clientes ahora pueden encontrar el ID de coincidencia 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 PrivateLink 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::SchemamappingAWS` .	19 de octubre de 2023

Actualización de una política existente	Se han agregado los siguientes permisos nuevos a la política `AWSEntityResolutionConsoleFullAccess` administrada: `ADXReadAccess` `yManageEventBridgeRules` .	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 Los ARN son necesarios cuando se necesita especificar un recurso de forma inequívoca en todos los ámbitos, 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.

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 de 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.

Flujo de trabajo de mapeo

El proceso que configuró para especificar los datos de entrada para traducir sus ID y cómo desea que se realice el mapeo de ID.

AWS Entity Resolution actualmente es compatible LiveRamp como método de mapeo de ID. Debe tener una suscripción para LiveRamp poder utilizar el flujo AWS Data Exchange de trabajo de mapeo de ID.

Para obtener más información, consulte Suscríbase a un servicio de proveedor en AWS Data Exchange.

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 usarlos 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.

Tipo de entrada

El tipo de datos de entrada. Se selecciona de una lista preconfigurada de valores, como el nombre, la dirección, el número de teléfono o la dirección de correo electrónico. El tipo de entrada indica AWS

Entity Resolution qué tipo de datos se están presentando, lo que permite clasificarlos y normalizarlos adecuadamente.

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.

Emparejamiento de muchos a muchos

La any-to-many coincidencia M 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 tus 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 te gustaría comparar entre sí, puedes asignarles 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 coincidencia uno a uno y coincidencia de varios a varios en la sección Flujo de trabajo coincidente).

Si desea que la coincidencia basada en reglas considere diferentes tipos de información de números de teléfono por separado, puede 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 un tipo de entrada de y los valores de `PHONE_NUMBER` la tabla de entrada tienen el formato correspondiente`(123) 456-7890`, se AWS Entity Resolution normalizarán los valores a. `1234567890`

En las siguientes secciones se describen las reglas de normalización.

Temas

Nombre

- 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

- 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_EMAIL_CHARS = Elimina todos los caracteres [a-zA-Z0-9] y [.@-] non-alpha-numeric

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

Dirección

- 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

Source_ID

- TRIM = Recorta los espacios en blanco iniciales y finales

Emparejamiento uno a uno

La ne-to-one coincidencia O 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`

Salida

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 el nombre completo, la dirección y el 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.

Mapeo 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.

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.

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.