Manual do usuário

AWS Entity Resolution

AWS Entity Resolution: Manual do usuário

Table of Contents

O que é AWS Entity Resolution?

AWS Entity Resolution é um serviço que ajuda você a combinar, vincular e aprimorar registros relacionados armazenados em vários aplicativos, canais e armazenamentos de dados. Você pode começar a usar fluxos de trabalho de resolução de entidades que são flexíveis, escaláveis e podem se conectar aos seus aplicativos e provedores de serviços de dados existentes.

AWS Entity Resolution oferece técnicas avançadas de correspondência, como correspondência baseada em regras, correspondência baseada em aprendizado de máquina (correspondência de ML) e correspondência liderada por provedores de serviços de dados. Essas técnicas podem ajudá-lo a vincular e aprimorar com mais precisão os registros relacionados de informações de clientes, códigos de produtos ou códigos de dados comerciais.

Você pode usar AWS Entity Resolution para criar uma visão unificada das interações com os clientes vinculando eventos recentes (como cliques em anúncios, abandono de carrinho e compras) a sinais pseudonimizados de seus provedores de serviços de dados em um ID de entidade exclusivo. Você também pode acompanhar melhor os produtos que usam códigos diferentes (por exemplo, SKU, UPC) em suas lojas. Você pode usar AWS Entity Resolution para controlar a precisão da correspondência e proteger melhor a segurança dos dados, minimizando a movimentação dos dados.

Tópicos

Você é um AWS Entity Resolution usuário iniciante?

Se você é usuário iniciante do AWS Entity Resolution, recomendamos que comece lendo as seguintes seções:

- Conf AWS Entity Resolution iguração

Características do AWS Entity Resolution

AWS Entity Resolution inclui os seguintes recursos:

- Preparação de dados flexível e personalizável

  AWS Entity Resolution lê seus dados AWS Glue para usar como entradas para processamento de partidas. Você pode especificar no máximo 20 entradas de dados. AWS Entity Resolution processa cada linha da tabela de entrada de dados como um registro, com uma entidade exclusiva servindo como chave primária. AWS Entity Resolution pode operar em conjuntos de dados criptografados. Primeiro, defina o mapeamento do esquema AWS Entity Resolution para entender quais campos de entrada você deseja usar no fluxo de trabalho correspondente. Você pode trazer seu próprio esquema de dados, ou blueprint, a partir de uma entrada de AWS Glue dados existente. Ou você pode criar seu esquema personalizado usando uma interface de usuário interativa ou um editor JSON. Por padrão, AWS Entity Resolution também normaliza as entradas de dados antes da correspondência para melhorar o processamento da correspondência, como remover caracteres especiais e espaços extras e formatar texto em minúsculas. Se a entrada de dados já estiver normalizada, você poderá desativar a normalização. Também fornecemos uma GitHub biblioteca, que você pode usar para personalizar ainda mais o processo de normalização de dados de acordo com suas necessidades.

- Fluxos de trabalho de correspondência de entidades configuráveis

  Um fluxo de trabalho de correspondência de entidades é uma sequência de etapas que você configura para saber AWS Entity Resolution como combinar sua entrada de dados e onde gravar a saída de dados consolidada. Você pode configurar um ou mais fluxos de trabalho correspondentes para comparar diferentes entradas de dados e usar diferentes técnicas de correspondência, como correspondência baseada em regras, correspondência de aprendizado de máquina ou correspondência liderada por provedor de serviços de dados sem resolução de entidades ou experiência em ML. Você também pode visualizar o status do trabalho dos fluxos de trabalho e métricas correspondentes existentes, como número do recurso, número de registros processados e número de correspondências encontradas.

  - eady-to-use Correspondência baseada em regras R

    Essa técnica de correspondência inclui um conjunto de ready-to-use regras no AWS Management Console ou AWS Command Line Interface (AWS CLI). Você pode usar essas

regras para encontrar registros relacionados com base em seus campos de entrada. Você também pode personalizar as regras adicionando ou removendo campos de entrada para cada regra, excluindo regras, reorganizando a prioridade da regra e criando novas regras. Você também pode redefinir as regras para retorná-las às configurações originais. A saída de dados em seu bucket do Amazon Simple Storage Service (Amazon S3) tem grupos de correspondência AWS Entity Resolution que são gerados usando a técnica de correspondência baseada em regras. Cada grupo de correspondência tem o número da regra usado para gerar a correspondência associada a ele para ajudar você a entender a correspondência. Por exemplo, o número da regra pode demonstrar a precisão de cada grupo de correspondência, de forma que a regra um seja mais precisa do que a regra dois.

- Correspondência pré-configurada baseada em aprendizado de máquina (correspondência de ML)

  Essa técnica de correspondência inclui um modelo de ML pré-configurado para encontrar correspondências em todas as suas entradas de dados, especialmente nos registros baseados no consumidor. O modelo usa todos os campos de entrada associados aos tipos de dados de nome, endereço de e-mail, número de telefone, endereço e data de nascimento. O modelo gera grupos de correspondência de registros relacionados com uma pontuação de confiança em cada grupo, explicando a qualidade da correspondência em relação a outros grupos de correspondência. O modelo considera os campos de entrada ausentes e analisa todo o registro em conjunto para representar uma entidade. A saída de dados em seu bucket do Amazon S3 tem grupos de correspondência que são AWS Entity Resolution gerados usando a correspondência de ML. É aqui que cada grupo de correspondência tem uma pontuação de confiança associada de 0,0—1,0, o que indica a precisão da partida.

- Combinando registros com provedores de serviços de dados

  Com isso, AWS Entity Resolution você pode combinar, vincular e aprimorar seus registros com os principais fornecedores de serviços de dados e conjuntos de dados licenciados para expandir sua capacidade de entender, alcançar e atender seus clientes. Por exemplo, você pode acrescentar atributos aos seus dados para aprimorar seus registros ou pode melhorar a interoperabilidade dos sistemas e plataformas com os quais trabalha para atingir suas metas de negócios. Você pode usar esse fluxo de trabalho correspondente com alguns cliques, eliminando a necessidade de criar e manter integrações proprietárias complexas. Você deve ter um contrato de licença com esses provedores de serviços de dados para aproveitar essa técnica de correspondência.

- Processamento manual em massa e processamento incremental automático

Você pode usar o processamento de dados para ajudar a converter suas entradas ou entradas de dados em uma tabela de saída de dados consolidada com registros semelhantes que tenham uma ID de correspondência comum gerada usando configurações de fluxo de trabalho de correspondência de entidades. Usando a API AWS Management Console e/ou o AWS CLI, você pode executar o processamento manual em massa sob demanda, com base em seu pipeline de dados de extração, transformação e carregamento (ETL) existente, que reprocessa todos os dados para quaisquer novas correspondências e atualizações para correspondências existentes. Além disso, para cenários de correspondência baseados em regras, você pode iniciar o processamento incremental automático para que, assim que novos dados estejam disponíveis em seu bucket do Amazon S3, o serviço leia esses novos registros e os compare com os registros existentes. Isso mantém suas correspondências atualizadas com quaisquer alterações nos dados do Amazon S3.

- Pesquisa quase em tempo real

  Pesquisar qualquer campo de entidade por meio da operação da AWS Entity Resolution GetMatchId API ajuda você a recuperar de forma síncrona um ID de correspondência existente. Você pode ligar AWS Entity Resolution com atributos de informações de identificação pessoal (PII) adquiridos por meio de diferentes fontes e canais. AWS Entity Resolution faz o hash desses atributos para proteção de dados e recupera a ID de correspondência correspondente para vincular e combinar o cliente. Por exemplo, você pode obter uma inscrição na web com um nome, e-mail e endereço para correspondência associados. Use a operação de AWS Entity Resolution GetMatchId API para descobrir se esse cliente ou entidade já existe nos resultados correspondentes armazenados em seu bucket do S3, junto com o ID de correspondência da entidade correspondente associado a ele. Depois de obter a ID de correspondência da entidade, você pode encontrar as informações transacionais associadas a ela em seus aplicativos de origem, como seus sistemas de gerenciamento de relacionamento com o cliente (CRM) ou plataforma de dados do cliente (CDP).

- Proteção de dados e regionalização por design

  AWS Entity Resolution oferece um recurso de criptografia padrão que pode ajudá-lo a proteger seus dados e fornece uma chave de criptografia para cada entrada de dados no serviço. Por exemplo, AWS Entity Resolution oferece a flexibilidade de trazer dados criptografados e com hash do lado do servidor para executar fluxos de trabalho de correspondência baseados em regras. AWS Entity Resolution oferece suporte à regionalização, o que significa que seus fluxos de trabalho correspondentes são executados para processar seus dados da mesma forma Região da AWS de onde você está usando o serviço. Você também pode criptografar e fazer o hash da saída de dados no Amazon S3 antes de usar seus dados resolvidos em outros aplicativos.

- Transcodificação multipartidária

  AWS Entity Resolution ajuda você a definir suas fontes de dados e as configurações correspondentes entre várias partes que desejam usar uma colaboração de dados, como em AWS Clean Rooms.

Serviços relacionados

Os itens a seguir Serviços da AWS estão relacionados a AWS Entity Resolution:

- Amazon S3

  Armazene os dados que você traz para AWS Entity Resolution o Amazon S3.

  Para obter mais informações, consulte O que é o Amazon S3? no Guia do usuário do Amazon Simple Storage Service.

- AWS Glue

  Crie AWS Glue tabelas a partir de seus dados no Amazon S3 para uso em. AWS Entity Resolution

  Para obter mais informações, consulte O que é AWS Glue? no Guia do AWS Glue desenvolvedor.

- AWS CloudTrail

  Use AWS Entity Resolution com CloudTrail registros para aprimorar sua análise da AWS service (Serviço da AWS) atividade.

  Para ter mais informações, consulte Registrando chamadas de AWS Entity Resolution API usando AWS CloudTrail.

- AWS CloudFormation

  Crie os seguintes recursos em AWS CloudFormation: AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e AWS::EntityResolution::PolicyStatement

  Para ter mais informações, consulte Criação de recursos de resolução de entidades da AWS com AWS CloudFormation.

Acessando AWS Entity Resolution

Você pode acessar AWS Entity Resolution por meio das seguintes opções:

- Diretamente pelo AWS Entity Resolution console em https://console.aws.amazon.com/entityresolution/.
- Programaticamente por meio da API. AWS Entity Resolution Para obter mais informações, consulte a Referência da API do AWS Entity Resolution .
  - Se você planeja chamar a AWS Entity Resolution API no AWS Lambda Runtime, crie seu próprio pacote de implantação e inclua a versão desejada da biblioteca do AWS SDK. Para obter mais informações, consulte os exemplos a seguir no Guia do AWS Lambda desenvolvedor:
    - Implemente funções Java Lambda com arquivamentos de arquivos.zip ou JAR
    - Trabalhando com arquivos de arquivos.zip para funções Python Lambda

Preços para AWS Entity Resolution

Para obter informações sobre a definição de preço, consulte Definição de preço do AWS Entity Resolution.

Conf AWS Entity Resolution iguração

Antes de usar AWS Entity Resolution pela primeira vez, conclua as tarefas a seguir.

Tópicos

Inscreva-se para AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

Criação de um usuário administrador

Para criar um usuário administrador, selecione uma das opções a seguir.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
Centro de Identidade do IAM (Recomendado)	Use credenciais de curto prazo para acessar a AWS. Isso está de acordo com as práticas recomendadas de segurança. Para obter informações sobre as práticas recomendadas, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.	Seguindo as instruções em Conceitos básicos no Guia do usuário do AWS IAM Identity Center .	Configure o acesso programático configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário.
No IAM (Não recomendado)	Use credenciais de curto prazo para acessar a AWS.	Seguindo as instruções em Criar o seu primeiro usuário administrador e um grupo de usuários do IAM no Guia do usuário do IAM.	Para configurar o acesso programático, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM.

Assine um serviço de provedor em AWS Data Exchange

Conclua o procedimento a seguir se você estiver usando um fluxo de trabalho de correspondência baseado no serviço do provedor ou um fluxo de trabalho de mapeamento de ID. Se você não estiver

usando um fluxo de trabalho de correspondência baseado no serviço do provedor ou um fluxo de trabalho de mapeamento de ID, você pode pular esta etapa.

Em AWS Entity Resolution, você pode optar por executar um fluxo de trabalho correspondente com um dos seguintes serviços de provedor se tiver uma assinatura com esse provedor ativada AWS Data Exchange. Seus dados serão combinados com um conjunto de entradas definido pelo seu provedor preferido.

- LiveRamp
  - LiveRamp Resolução de identidade
  - LiveRamp Transcodificação
- TransUnion
  - TransUnion TruAudience Resolução e enriquecimento de identidade sem transferência
  - TransUnion TruAudience Resolução de identidade sem transferência
- ID unificada 2.0
  - Resolução de identidade unificada de ID 2.0

Além disso, você pode executar um fluxo de trabalho de mapeamento de ID LiveRamp se tiver uma assinatura com esse provedor.

- LiveRamp
  - LiveRamp Transcodificação

Há duas maneiras de assinar um serviço de provedor:

- Oferta privada — Se você já tem um relacionamento com um fornecedor, siga o procedimento de produtos e ofertas privadas no Guia AWS Data Exchange do usuário para aceitar uma oferta privada em AWS Data Exchange.
- Traga sua própria assinatura — Se você já tem uma assinatura de dados existente com um provedor, siga o procedimento de ofertas Traga sua própria assinatura (BYOS) no Guia do AWS Data Exchange usuário para aceitar uma oferta de BYOS em. AWS Data Exchange

Depois de assinar um serviço de provedor em AWS Data Exchange, você pode criar um fluxo de trabalho correspondente ou um fluxo de trabalho de mapeamento de ID com esse serviço de provedor.

Para obter mais informações sobre como acessar um produto do provedor que contém APIs, consulte Como acessar um produto de API no Guia do AWS Data Exchange usuário.

Prepare tabelas de dados

Em AWS Entity Resolution, cada uma de suas tabelas de dados de entrada contém registros de origem. Esses registros contêm identificadores de consumidores, como nome, sobrenome, endereço de e-mail ou número de telefone. Esses registros de origem podem ser combinados com outros registros de origem fornecidos na mesma tabela de dados ou em outras tabelas de dados de entrada. Cada registro deve ter uma ID de registro exclusiva (ID exclusivo) e você deve defini-la como uma chave primária ao criar um mapeamento de esquema dentro AWS Entity Resolution dela.

Cada tabela de dados de entrada está disponível como uma AWS Glue tabela apoiada pelo Amazon S3. Você pode usar seus dados primários que já estão no Amazon S3 ou importar tabelas de dados de outros provedores de SaaS para o Amazon S3. Depois que os dados forem carregados para o Amazon S3, você poderá usar um AWS Glue rastreador para criar uma tabela de dados no. AWS Glue Data Catalog Em seguida, você pode usar a tabela de dados como entrada para AWS Entity Resolution.

A preparação de suas tabelas de dados envolve as seguintes etapas:

Tópicos

Etapa 1: Prepare seus dados de entrada

Conclua o procedimento a seguir se você estiver usando um fluxo de trabalho correspondente com um serviço de provedor. Se você não estiver usando um fluxo de trabalho correspondente com um serviço de provedor, você pode pular esta etapa.

Para ter mais informações, consulte Assine um serviço de provedor em AWS Data Exchange.

Se você quiser executar um fluxo de trabalho correspondente com um fluxo de trabalho de correspondência baseado em serviços do provedor ou um fluxo de trabalho de mapeamento de ID, consulte a tabela a seguir para preparar seus dados de entrada:

Serviço do provedor	É necessário um ID exclusivo?	Ações
LiveRamp	Sim	Garanta o seguinte: • O ID exclusivo pode ser seu próprio identificador pseudônimo ou um ID de linha. • O formato e a normalização do arquivo de entrada de dados estão alinhados com as LiveRamp diretrizes. Para obter mais informações sobre as diretrizes de formatação do arquivo de entrada para o fluxo de trabalho correspondente, consulte Executar resolução de identidade por meio do ADX na LiveRamp documentação. Para obter mais informações sobre as diretrizes de formatação do arquivo de entrada para o fluxo de trabalho de mapeamento de ID, consulte Executar transcodificação por meio do ADX na documentação. LiveRamp
TransUnion	Sim	Garanta o seguinte: • Existe uma ID exclusiva para enriquecimento TransUnion de dados.

Serviço do provedor	É necessário um ID exclusivo?	Ações

		> **Note**
		> Os atributos de transmissão podem persistir na entrada e na saída para TransUnion. As chaves E domésticas e o HHID são específicos para o namespace do cliente.
		• **`Phone number`** deve ter 10 dígitos, sem caracteres especiais, como espaços ou hífens.
		• **`Addresses`** deve ser dividido em
		  • uma única linha de endereço (combine as linhas de endereço 1 e 2, se houver)
		  • city
		  • zip (ou zip plus4), sem caracteres especiais, como espaços ou hífens
		  • estado, especificado como código de 2 letras 3
		• **`Email addresses`** deve estar em texto simples.
		• **`First Name`** podem ser maiúsculas ou minúsculas, apelidos são suportados, mas

Serviço do provedor	É necessário um ID exclusivo?	Ações
		títulos e sufixos devem ser excluídos. • **`Last Name`**podem ser minúsculas ou maiúsculas, as iniciais médias devem ser excluídas.

Serviço do provedor	É necessário um ID exclusivo?	Ações
ID unificada 2.0	Sim	Garanta o seguinte: • O ID exclusivo não pode ser um hash. • O UID2 suporta e-mail e número de telefone para a geração UID2. No entanto, se os dois valores estiverem presentes no mapeamento do esquema, o fluxo de trabalho duplicará cada registro na saída. Um registro usa o e-mail para geração de UID2 e o segundo registro usa o número de telefone. Se seus dados incluírem uma combinação de e-mails e números de telefone e você não quiser essa duplicação de registros na saída, a melhor abordagem é criar um fluxo de trabalho separado para cada um, com mapeamentos de esquema separados. Nesse cenário, siga as etapas duas vezes: crie um fluxo de trabalho para e-mails e outro separado para números de telefone. **Note** Um e-mail ou número de telefone específico, em

Serviço do provedor	É necessário um ID exclusivo?	Ações
		qualquer momento específico, resulta no mesmo valor bruto de UID2, independentemente de quem fez a solicitação. Os UID2s brutos são criados pela adição de sais de baldes de sal que são girados aproximadamente uma vez por ano, fazendo com que o UID2 bruto também seja girado com ele. Diferentes baldes de sal giram em épocas diferentes ao longo do ano. AWS Entity Resolution atualmente não monitora baldes de sal rotativos e UID2s brutos, portanto, é recomendável que você regenere os UID2s brutos diariamente. Para obter mais informações, consulte Com que frequência os UID2s devem ser atualizados para atualizações incrementais? na documentação do UID 2.0.

Etapa 2: Salve sua tabela de dados de entrada em um formato de dados compatível

Se você já salvou seus dados de entrada em um formato de dados compatível, você pode pular esta etapa.

Para serem usados AWS Entity Resolution, os dados de entrada devem estar em um formato AWS Entity Resolution compatível. AWS Entity Resolution suporta os seguintes formatos de dados:

- valor separado por vírgula (CSV)

> **Note**
>
> LiveRamp só oferece suporte a arquivos CSV.

- Parquet

Etapa 3: Faça o upload da sua tabela de dados de entrada para o Amazon S3

Se você já tem sua tabela de dados primários no Amazon S3, você pode pular esta etapa.

> **Note**
>
> Os dados de entrada devem ser armazenados no Amazon Simple Storage Service (Amazon S3) no Conta da AWS mesmo local Região da AWS e no qual você deseja executar o fluxo de trabalho correspondente.

Para carregar sua tabela de dados de entrada para o Amazon S3

1. Faça login AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha Buckets e, em seguida, escolha um bucket para armazenar sua tabela de dados.
3. Escolha Upload e siga as instruções.
4. Escolha a guia Objetos para visualizar o prefixo do onde seus dados são armazenados. Anote o nome da pasta.

Você pode selecionar a pasta para visualizar a tabela de dados.

Etapa 4: criar uma AWS Glue tabela

Os dados de entrada no Amazon S3 devem ser catalogados AWS Glue e representados como uma tabela. AWS Glue Para obter mais informações sobre como criar uma AWS Glue tabela com o Amazon S3 como entrada, consulte Como trabalhar com rastreadores no AWS Glue console no Guia do desenvolvedor.AWS Glue

> **Note**
>
> AWS Entity Resolution não oferece suporte a tabelas particionadas.

Nesta etapa, você configura um rastreador AWS Glue que rastreia todos os arquivos em seu bucket do S3 e cria uma tabela. AWS Glue

> **Note**
>
> AWS Entity Resolution atualmente não oferece suporte a locais do Amazon S3 registrados com. AWS Lake Formation

Para criar uma AWS Glue tabela

1. Faça login no AWS Management Console e abra o AWS Glue console em https://console.aws.amazon.com/glue/.
2. Na barra de navegação, selecione Crawlers.
3. Selecione o bucket do S3 na lista e escolha Adicionar crawler.
4. Na página Adicionar crawler, insira um nome do crawler e escolha Avançar.
5. Continue na página Adicionar crawler, especificando os detalhes.
6. Na página Escolher uma função do IAM, escolha Escolher um perfil do IAM existente e, em seguida, escolha Avançar.

   Você também pode escolher Criar um perfil do IAM ou fazer com que seu administrador crie o perfil do IAM, se necessário.

7. Em Criar uma programação para esse crawler, mantenha a Frequência padrão (Executar sob demanda) e escolha Avançar.
8. Em Configurar a saída do crawler, insira o AWS Glue banco de dados e escolha Avançar.
9. Revise os detalhes e depois escolha Concluir.
10. Na página Crawlers, marque a caixa de seleção ao lado do bucket S3 e escolha Executar crawler.
11. Depois que o rastreador terminar de ser executado, na barra de AWS Glue navegação, escolha Bancos de dados e, em seguida, escolha o nome do banco de dados.
12. Na página Banco de dados, escolha Tabelas em {nome do seu banco de dados}.

    a. Visualize as tabelas no AWS Glue banco de dados.

    b. Para visualizar o esquema de uma tabela, selecione uma tabela específica.
13. Anote o nome do AWS Glue banco de dados e o nome AWS Glue da tabela.

Crie uma função do IAM para um usuário do console

Para criar um perfil do IAM

1. Faça login no console do IAM em (https://console.aws.amazon.com/iam/) com sua conta de administrador.
2. Em Gerenciamento de acesso, escolha Perfis.

   Você pode usar Funções para criar credenciais de curto prazo, o que é recomendado para aumentar a segurança. Você também pode escolher Usuários para criar credenciais de longo prazo.
3. Selecione Criar perfil.
4. No assistente de criação de função, em Tipo de entidade confiável, escolha Conta da AWS.
5. Mantenha a opção Esta conta selecionada e, em seguida, escolha Avançar.
6. Em Adicionar permissões, escolha Criar política.

   Uma nova guia será aberta.

   a. Selecione a guia JSON e adicione políticas de acordo com as habilidades concedidas ao usuário do console. AWS Entity Resolution oferece as seguintes políticas gerenciadas com base em casos de uso comuns:

- AWS política gerenciada: AWSEntityResolutionConsoleFullAccess
- AWS política gerenciada: AWSEntityResolutionConsoleReadOnlyAccess

b. Escolha Próximo: Etiquetas, adicionar tags (opcional) e escolha Próximo: Revisão.

c. Em Política de revisão, insira um Nome e uma Descrição e revise o Resumo.

d. Escolha Criar política.

Você criou uma política para um membro da colaboração.

e. Volte para a guia original e, em Adicionar permissões, insira o nome da política que você acabou de criar. (Você pode precisar recarregar a página.)

f. Marque a caixa de seleção ao lado do nome da política que você criou e escolha Avançar.

7. Na página Nome, revisar e criar, insira um nome de perfil e uma descrição.

a. Revise Selecionar entidades confiáveis, insira o Conta da AWS para o nome da pessoa ou pessoas que assumirão a função (se necessário).

b. Revise as permissões em Adicionar permissões e edite, se necessário.

c. Revise as tags e adicione tags, se necessário.

d. Selecione Criar perfil.

Crie uma função de trabalho de fluxo de trabalho para AWS Entity Resolution

AWS Entity Resolution usa uma função de trabalho de fluxo de trabalho para executar um fluxo de trabalho. Você pode criar esse perfil usando o console se você tiver as permissões necessárias do IAM. Se você não tiver `CreateRole` permissões, peça ao administrador que crie a função.

Para criar uma função de trabalho de fluxo de trabalho para AWS Entity Resolution

1. Faça login no console do IAM em https://console.aws.amazon.com/iam/ com sua conta de administrador.
2. Em Gerenciamento de acesso, escolha Perfis.

Você pode usar Funções para criar credenciais de curto prazo, o que é recomendado para aumentar a segurança. Você também pode escolher Usuários para criar credenciais de longo prazo.

3. Selecione Criar perfil.
4. No assistente Criar perfil, para Tipo de entidade confiável, escolha Política de confiança personalizada.
5. Copie e cole a seguinte política de confiança personalizada no editor JSON.

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

6. Escolha Próximo.
7. Em Adicionar permissões, escolha Criar política.

   Uma nova guia é exibida.

   a. Copie e cole a política a seguir no editor JSON.

> **Note**
>
> O exemplo de política a seguir oferece suporte às permissões necessárias para ler os recursos de dados correspondentes, como Amazon S3 e. AWS Glue No entanto, talvez seja necessário modificar essa política dependendo de como você configurou suas fontes de dados.
> Seus AWS Glue recursos e os recursos subjacentes do Amazon S3 devem estar no mesmo Região da AWS que. AWS Entity Resolution
> Você não precisa conceder AWS KMS permissões se suas fontes de dados não estiverem criptografadas ou descriptografadas.

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

Substitua cada *{{espaço reservado de entrada do usuário}}* por suas próprias informações.

aws-region	Região da AWS de seus recursos. Seus AWS Glue recursos, recursos e AWS KMS recursos subjacentes do Amazon S3 devem estar no mesmo Região da AWS que. `AWS Entity Resolution`
accountId	Sua Conta da AWS identidade.
baldes de entrada	Buckets do Amazon S3 que contêm os objetos de dados subjacentes de AWS Glue onde `AWS Entity Resolution` serão lidos.
baldes de saída	Buckets do Amazon S3 onde `AWS Entity Resolution` gerarão os dados de saída.

bancos de dados de entrada	AWS Glue bancos de dados de onde AWS Entity Resolution serão lidos.

b. (Opcional) Se o bucket de entrada do Amazon S3 for criptografado usando a chave KMS do cliente, adicione o seguinte:

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

Substitua cada *{{espaço reservado de entrada do usuário}}* por suas próprias informações.

aws-region	Região da AWS de seus recursos. Seus AWS Glue recursos, recursos e AWS KMS recursos subjacentes do Amazon S3 devem estar no mesmo Região da AWS que. AWS Entity Resolution
accountId	Sua Conta da AWS identidade.
Teclas de entrada	Entrada gerenciada de chaves AWS Key Management Service. Se suas fontes de entrada forem criptografadas, AWS Entity Resolution deverá descripto grafar seus dados usando sua chave.

c. (Opcional) Se os dados que estão sendo gravados no bucket de saída do Amazon S3 precisarem ser criptografados, adicione o seguinte:

```
{
    "Effect": "Allow",
    "Action": [
```

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

Substitua cada *{{espaço reservado de entrada do usuário}}* por suas próprias informações.

aws-region	Região da AWS de seus recursos. Seus AWS Glue recursos, recursos e AWS KMS recursos subjacentes do Amazon S3 devem estar no mesmo Região da AWS que. `AWS Entity Resolution`
accountId	Sua Conta da AWS identidade.
Teclas de saída	Entrada gerenciada de chaves AWS Key Management Service. Se você precisar que suas fontes de saída sejam criptografadas, `AWS Entity Resolution` deverá criptografar os dados de saída usando sua chave.

d. (Opcional) Se você tiver uma assinatura com um serviço de provedor por meio AWS Data Exchange de e quiser usar uma função existente para um fluxo de trabalho baseado em serviços de provedor, adicione o seguinte:

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

Substitua cada *{{espaço reservado de entrada do usuário}}* por suas próprias informações.

aws-region	O Região da AWS local onde o recurso do provedor é concedido. Você pode encontrar esse valor no ARN do ativo no AWS Data Exchange console. Por exemplo: `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
ID do conjunto de dados	O ID do conjunto de dados, encontrado no AWS Data Exchange console.
revisionID	A revisão do conjunto de dados, encontrada no AWS Data Exchange console.
AssetID	O ID do ativo, encontrado no AWS Data Exchange console.

8. Volte para a guia original e, em Adicionar permissões, insira o nome da política que você acabou de criar. (Você pode precisar recarregar a página.)
9. Marque a caixa de seleção ao lado do nome da política que você criou e escolha Avançar.
10. Para Nome, revisar e criar, insira um nome de perfil e uma descrição.

> **Note**
>
> O nome da função deve corresponder ao padrão nas `passRole` permissões concedidas ao membro que pode passar o `workflow job role` para criar um fluxo de trabalho correspondente.
> Por exemplo, se você estiver usando a política `AWSEntityResolutionConsoleFullAccess` gerenciada, lembre-se de incluir `entityresolution` no nome da sua função.

a. Revise Selecionar entidades confiáveis e edite, se necessário.
b. Revise as permissões em Adicionar permissões e edite, se necessário.
c. Revise as tags e adicione tags, se necessário.
d. Selecione Criar perfil.

A função de trabalho do fluxo de trabalho para AWS Entity Resolution foi criada.

Criação de um mapeamento de esquema

Para definir os dados de entrada que você deseja resolver, crie um mapeamento de esquema. O processo de mapeamento do esquema orienta você em um conjunto de etapas para definir os dados que você deseja resolver, definindo seus campos de entrada e tipos de atributos e, em seguida, definindo e agrupando suas chaves de correspondência.

Há três maneiras de criar um mapeamento de esquema em: AWS Entity Resolution

- Usando um fluxo guiado para importar as informações do esquema existente.
- Usando um fluxo guiado para definir manualmente os dados de entrada.
- Usando o editor JSON para criar, colar ou importar um mapeamento de esquema.

O processo a seguir orienta você pelos três métodos diferentes para criar um mapeamento de esquema.

Tópicos

Crie um mapeamento de esquema (colunas pré-preenchidas)

Esse procedimento descreve o processo de criação de um mapeamento de esquema usando a AWS Glue opção Importar de no AWS Entity Resolution console. Você pode usar esse método de criação para definir campos de entrada começando com colunas pré-preenchidas de uma AWS Glue tabela.

Para criar mapeamento de esquema usando colunas pré-preenchidas:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Preparação de dados, escolha Mapeamentos do esquema.
3. Na página Mapeamentos do esquema, no canto superior direito, escolha Criar mapeamento do esquema.

4. Para a Etapa 1: Especificar detalhes do esquema, faça o seguinte:

   a. Em Nome e método de criação, insira um nome de mapeamento do esquema e uma Descrição opcional.

   b. Em Método de criação, escolha Importar de AWS Glue.

   c. Escolha o AWS Glue banco de dados na lista suspensa e, em seguida, escolha a AWS Glue tabela na lista suspensa.

      Para criar uma nova tabela, acesse o AWS Glue console https://console.aws.amazon.com/glue/. Para obter mais informações, consulte AWS Glue as tabelas no Guia AWS Glue do usuário.

   d. Para ID exclusivo, especifique a coluna que faz referência distinta a cada linha de seus dados.

      Example

      Por exemplo: **`Primary_key`**, **`Row_ID`** ou **`Record_ID`**.

      > **Note**
      >
      > A coluna ID exclusiva é obrigatória. O ID exclusivo deve ser um identificador exclusivo em uma única tabela. No entanto, em tabelas diferentes, o ID exclusivo pode ter valores duplicados. Se a ID exclusiva não for especificada, não for exclusiva na mesma fonte ou se sobrepor em termos de nomes de atributos nas fontes, AWS Entity Resolution rejeitará o registro quando o fluxo de trabalho correspondente for executado.

   e. Em Campos de entrada, escolha de 1 a 25 colunas para usar para correspondência e para passagem opcional.

      i. Selecione Adicionar colunas para passar se quiser especificar as colunas que não são usadas para correspondência.

      ii. Em Passar — opcional, escolha as colunas a serem incluídas como colunas de passagem.

   f. (Opcional) Se você quiser ativar Tags para o recurso, escolha Adicionar nova tag e insira o par Chave e Valor.

   g. Escolha Próximo.

5. Para a Etapa 2: mapear campos de entrada, faça o seguinte:

   a. Em Campos de entrada para correspondência, especifique o tipo de entrada e a chave de correspondência para cada campo de entrada.

      O tipo de entrada ajuda você a classificar os dados. A tecla Match permite a comparação do campo de entrada com seu fluxo de trabalho correspondente.

      > **Note**
      >
      > Se você estiver criando um mapeamento de esquema para usar com a técnica de correspondência baseada em serviços do LiveRamp provedor, poderá:
      >
      > - Especifique o tipo de entrada como LiveRampID.
      > - Especifique o campo de nome como vários campos (como**`first_name`**,**`last_name`**) ou em um campo.
      > - Especifique o campo de endereço da rua como vários campos (como**`address1`**,**`address2`**) ou em um campo.
      >
      >   Se corresponder a um endereço, é necessário um CEP.
      > - Inclua e-mail ou telefone com nome, e esses campos podem corresponder ao endereço da rua.

   b. Escolha Próximo.

6. Para a Etapa 3: Agrupar dados, faça o seguinte:

   a. Escolha os campos de nome relacionados e, em seguida, insira o nome do grupo e a chave de correspondência.

      Example

      Por exemplo, escolha os campos de entrada**`First name`**,**`Middle name`**, e e**`Last name`**, em seguida, insira um nome de grupo chamado “**`Full name`**” e uma tecla de correspondência chamada “**`Full name`**” para permitir a comparação.

   b. Escolha os campos de endereço relacionados e, em seguida, insira o nome do grupo e a chave de correspondência.

Example

Por exemplo, escolha os campos de entrada**`Home street address 1`**,**`Home street address 2`**, e e**`Home city`**, em seguida, insira um nome de grupo chamado “**`Shipping address`**” e uma tecla de correspondência chamada “**`Shipping address`**” para permitir a comparação.

c. Escolha os campos de número de telefone relacionados e, em seguida, insira o nome do grupo e a chave de correspondência.

Example

Por exemplo, escolha os campos de entrada**`Home phone 1`**,**`Home phone 2`**, e e**`Cell phone`**, em seguida, insira um nome de grupo chamado “**`Shipping phone number`**” e uma tecla de correspondência chamada “**`Shipping phone number`**” para permitir a comparação.

Se você tiver mais de um tipo de dados, poderá adicionar mais grupos.

d. Escolha Próximo.

7. Para a Etapa 4: revisar e criar, faça o seguinte:

a. Revise as seleções feitas nas etapas anteriores e edite, se necessário.

b. Escolha Criar mapeamento de esquema.

> **Note**
>
> Você não pode modificar um mapeamento de esquema depois de associá-lo a um fluxo de trabalho. Você pode clonar um mapeamento de esquema se quiser usar uma configuração existente para criar um novo mapeamento de esquema.

Depois de criar o mapeamento do esquema, você estará pronto para criar um fluxo de trabalho correspondente ou criar um namespace de ID.

Crie um mapeamento de esquema (colunas definidas manualmente)

Esse procedimento descreve o processo de criação de um mapeamento de esquema usando a opção Criar esquema personalizado no AWS Entity Resolution console. Use esse método de criação para definir manualmente os campos de entrada usando um fluxo guiado.

Para criar mapeamento de esquema usando colunas definidas manualmente

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Preparação de dados, escolha Mapeamentos do esquema.
3. Na página Mapeamentos do esquema, no canto superior direito, escolha Criar mapeamento do esquema.
4. Para a Etapa 1: Especificar detalhes do esquema, faça o seguinte:

   a. Em nome e método de criação, insira um nome de mapeamento do esquema e uma Descrição opcional.

   b. Em Método de criação, escolha Criar esquema personalizado.

   c. Em ID exclusiva, insira uma ID exclusiva para identificar cada linha de seus dados.

      Example

      Por exemplo: **`Primary_key`**, **`Row_ID`** ou **`Record_ID`**.

      > **Note**
      >
      > A coluna ID exclusiva é obrigatória. O ID exclusivo deve ser um identificador exclusivo em uma única tabela. No entanto, em tabelas diferentes, o ID exclusivo pode ter valores duplicados. Se a ID exclusiva não for especificada, não for exclusiva na mesma fonte ou se sobrepor em termos de nomes de atributos nas fontes, AWS Entity Resolution rejeitará o registro quando o fluxo de trabalho correspondente for executado.

   d. (Opcional) Se você quiser ativar Tags para o recurso, escolha Adicionar nova tag e insira o par Chave e Valor.

e. Escolha Próximo.

5. Para a Etapa 2: mapear campos de entrada, faça o seguinte:

   a. Em Campos de entrada para correspondência, adicione o campo de entrada, o tipo de entrada e a chave de correspondência.

      Você pode adicionar até 25 campos de entrada.

      O tipo de entrada ajuda você a classificar os dados. A tecla Match permite a comparação do campo de entrada com seu fluxo de trabalho correspondente.

      > **Note**
      >
      > Se você estiver criando um mapeamento de esquema para usar com a técnica de correspondência baseada em serviços do LiveRamp provedor, poderá especificar o tipo de entrada como ID. LiveRamp Se você quiser incluir dados de PII na saída, deverá especificar o tipo de entrada como Cadeia de caracteres personalizada.

   b. (Opcional) Para campos de entrada a serem transmitidos, adicione os campos de entrada que não serão correspondidos.

   c. Escolha Próximo.

6. Para a Etapa 3: Dados do grupo:

   a. Escolha os campos de nome relacionados e, em seguida, insira o nome do grupo e a chave de correspondência.

      Example

      Por exemplo, escolha os campos de entrada**`First name`**,**`Middle name`**, e e**`Last name`**, em seguida, insira um nome de grupo chamado “**`Full name`**” e uma tecla de correspondência chamada “**`Full name`**” para permitir a comparação.

   b. Escolha os campos de endereço relacionados e, em seguida, insira o nome do grupo e a chave de correspondência.

      Example

      Por exemplo, escolha os campos de entrada**`Home street address 1`**,**`Home street address 2`**, e e**`Home city`**, em seguida, insira um nome de grupo chamado “**`Shipping`**

address" e uma tecla de correspondência chamada "**Shipping address**" para permitir a comparação.

c. Escolha os campos de número de telefone relacionados e, em seguida, insira o nome do grupo e a chave de correspondência.

Example

Por exemplo, escolha os campos de entrada**Home phone 1**,**Home phone 2**, e e**Cell phone**, em seguida, insira um nome de grupo chamado "**Shipping phone number**" e uma tecla de correspondência chamada "**Shipping phone number**" para permitir a comparação.

Se você tiver mais de um tipo de dados, poderá adicionar mais grupos.

d. Escolha Próximo.

7. Para a Etapa 4: revisar e criar, faça o seguinte:

a. Revise as seleções feitas nas etapas anteriores e edite, se necessário.

b. Escolha Criar mapeamento de esquema.

> **Note**
>
> Você não pode modificar um mapeamento de esquema depois de associá-lo a um fluxo de trabalho. Você pode clonar um mapeamento de esquema se quiser usar uma configuração existente para criar um novo mapeamento de esquema.

Depois de criar o mapeamento do esquema, você estará pronto para criar um fluxo de trabalho correspondente ou criar um namespace de ID.

Crie um mapeamento de esquema (editor JSON)

Esse procedimento descreve o processo de criação de um mapeamento de esquema usando a opção Usar editor JSON no AWS Entity Resolution console. Use esse método de criação para usar um editor JSON para criar, colar ou importar um mapeamento de esquema. Os campos ID exclusivo e Entrada não estão disponíveis com essa opção.

Para criar mapeamento de esquema usando o editor JSON

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Preparação de dados, escolha Mapeamentos do esquema.
3. Na página Mapeamentos do esquema, no canto superior direito, escolha Criar mapeamento do esquema.
4. Para a Etapa 1: Especificar detalhes do esquema, faça o seguinte:
   a. Em nome e método de criação, insira um nome de mapeamento do esquema e uma Descrição opcional.
   b. Em Método de criação, escolha Usar editor JSON.
   c. (Opcional) Se você quiser ativar Tags para o recurso, escolha Adicionar nova tag e insira o par Chave e Valor.
   d. Escolha Próximo.
5. Para a Etapa 2: Especifique o mapeamento:
   a. Comece a criar o esquema no editor JSON ou escolha uma das seguintes opções:

Se você deseja…	A seguir, escolha…
Comece a criar seu mapeamento de esquema	Insira uma amostra de JSON e edite as informações conforme necessário.
Use um arquivo JSON existente	Importar do arquivo

   b. Escolha Próximo.
6. Para a Etapa 3: Revise e crie:
   a. Revise as seleções feitas nas etapas anteriores e edite, se necessário.
   b. Escolha Criar mapeamento de esquema.

> **Note**
>
> Você não pode modificar um mapeamento de esquema depois de associá-lo a um fluxo de trabalho. Você pode clonar um mapeamento de esquema se quiser usar uma configuração existente para criar um novo mapeamento de esquema.

Depois de criar o mapeamento do esquema, você estará pronto para criar um fluxo de trabalho correspondente ou criar um namespace de ID.

Criação de um fluxo de trabalho correspondente

Depois de criar um mapeamento de esquema, você pode criar um ou mais fluxos de trabalho correspondentes para especificar entradas de dados, etapas de normalização e escolher as técnicas de correspondência desejadas. Existem três técnicas de correspondência:

- A correspondência baseada em regras é um conjunto hierárquico de regras de correspondência em cascata, sugerido por AWS Entity Resolution, com base nos dados que você insere e é totalmente configurável por você.
- A correspondência baseada em aprendizado de máquina é um processo predefinido que tentará combinar registros em todos os dados que você inserir.
- Os serviços do provedor permitem que você combine seus identificadores conhecidos com seu provedor de serviços de dados preferido.

  AWS Entity Resolution atualmente se integra aos seguintes provedores de serviços de dados: LiveRamp TransUnion, e UID 2.0. Você pode usar uma assinatura pública para esses provedores AWS Data Exchange ou negociar uma oferta privada diretamente com o provedor de dados. Para ter mais informações, consulte Assine um serviço de provedor em AWS Data Exchange.

AWS Entity Resolution lê seus dados do (s) local (s) especificado (s) por você e grava os resultados em um local que você escolher. Você pode usar AWS Entity Resolution para fazer o hash dos dados de saída, se desejar, ajudando você a manter o controle sobre seus dados.

Você também pode usar a saída da correspondência baseada em regras ou ML como uma entrada para a correspondência baseada em serviços do provedor ou vice-versa para atender às suas necessidades comerciais. Por exemplo, você pode primeiro executar a correspondência baseada em regras para encontrar correspondências em seus dados e, em seguida, enviar um subconjunto de registros incomparáveis para a correspondência baseada em serviços do provedor para economizar nos custos de assinatura do provedor.

Tópicos

Crie um fluxo de trabalho de correspondência baseado em regras

O fluxo de trabalho de correspondência baseado em regras permite comparar texto não criptografado ou dados com hash para encontrar correspondências exatas com base nos critérios que você personaliza.

Quando AWS Entity Resolution encontra uma correspondência entre dois ou mais registros em seus dados, ele atribui uma ID de correspondência aos registros no conjunto de dados correspondente.

Para correspondência baseada em regras, ele aplica o número da regra que gerou a correspondência.

Para criar um fluxo de trabalho de correspondência baseado em regras:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Na página Fluxos de trabalho correspondentes, no canto superior direito, escolha Criar fluxo de trabalho correspondente.
4. Para a Etapa 1: Especificar os detalhes correspondentes do fluxo de trabalho, faça o seguinte:

    a. Insira um nome de fluxo de trabalho correspondente e uma Descrição opcional.

    b. Em Entrada de dados, escolha um AWS Glue banco de dados na lista suspensa, selecione a AWS Glue tabela e, em seguida, o mapeamento do esquema correspondente.

    Você pode adicionar até 19 entradas de dados.

    c. A opção Normalizar dados é selecionada por padrão, para que as entradas de dados sejam normalizadas antes da correspondência. Se você não quiser normalizar dados, desmarque a opção Normalizar dados.

    d. Especifique as permissões de Acesso ao serviço selecionando Criar e usar um novo perfil de serviço ou Usar um perfil de serviço existente.

Se você escolher...	Então
Criar e usar um novo perfil de serviço	• AWS Entity Resolution cria uma função de serviço com a política necessária para essa tabela.

Se você escolher...	Então
	• O nome do perfil de serviço padrão é `entityresolution-matching-workflow-<timestamp>` . • Você deve ter permissões para criar perfis e anexar políticas. • Se seus dados de entrada estiverem criptografados, você poderá escolher a opção Esses dados são criptografados com uma chave KMS e, em seguida, inserir uma AWS KMS chave que será usada para descriptografar sua entrada de dados.

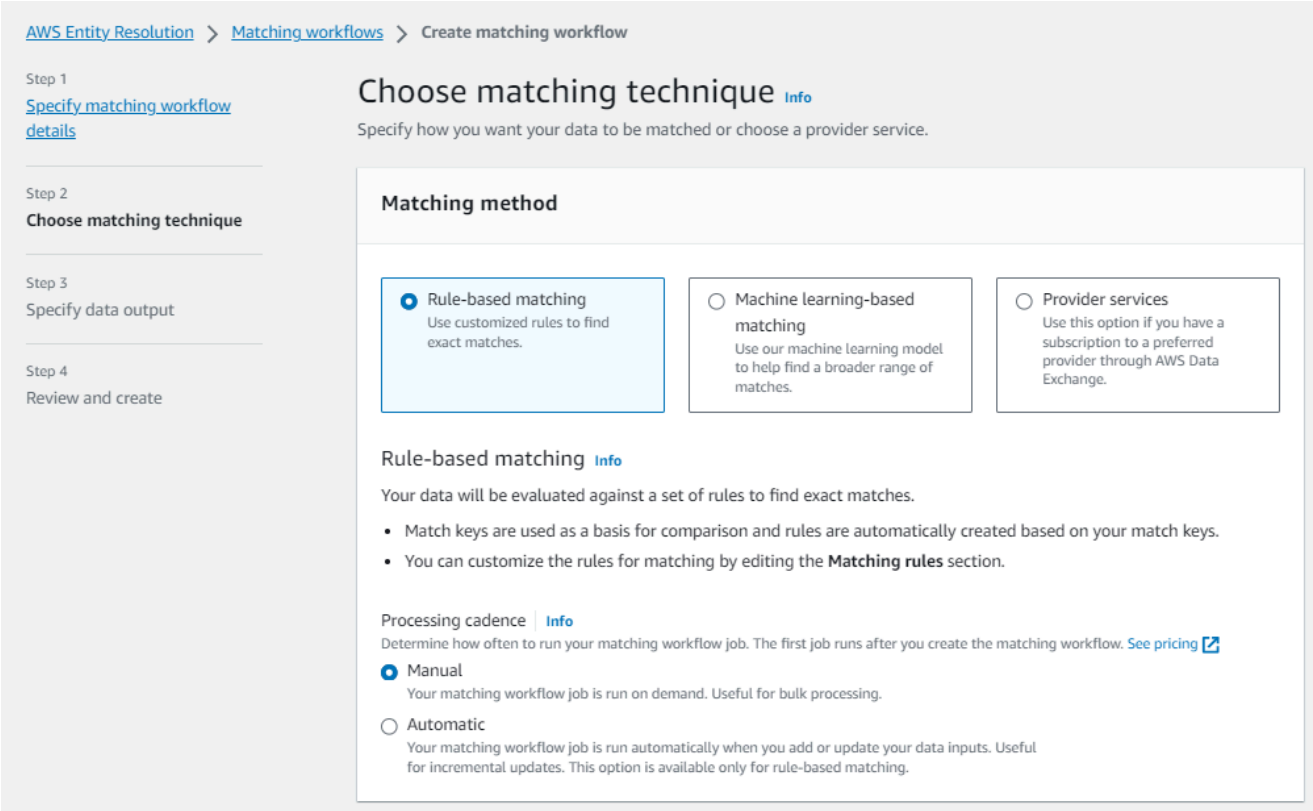
Se você escolher...	Então
Use um perfil de serviço existente	1. Escolha um nome do perfil de serviço existente na lista suspensa. A lista de perfis é exibida se você tiver permissões para listar funções. Se você não tiver permissões para listar perfis, insira o nome do recurso da Amazon (ARN) do perfil que você deseja usar. Se não houver perfis de serviço existentes, a opção de Usar um perfil de serviço existente não estará disponível. 2. Veja a função de serviço escolhendo o link externo Exibir no IAM. Por padrão, AWS Entity Resolution não tenta atualizar a política de função existente para adicionar as permissões necessárias.

e. (Opcional) Para ativar tags para o recurso, escolha Adicionar nova tag e insira o par de chave e valor.

f. Escolha Próximo.

5. Para a Etapa 2: Escolha a técnica de correspondência:

   a. Em Método de correspondência, escolha Correspondência baseada em regras.



b. Em Cadência de processamento, escolha uma das opções a seguir.

Se você deseja…	A seguir, escolha…
Execute um fluxo de trabalho sob demanda para uma atualização em massa	Manual
Execute um fluxo de trabalho assim que novos dados estiverem em seu bucket do S3	Automatic

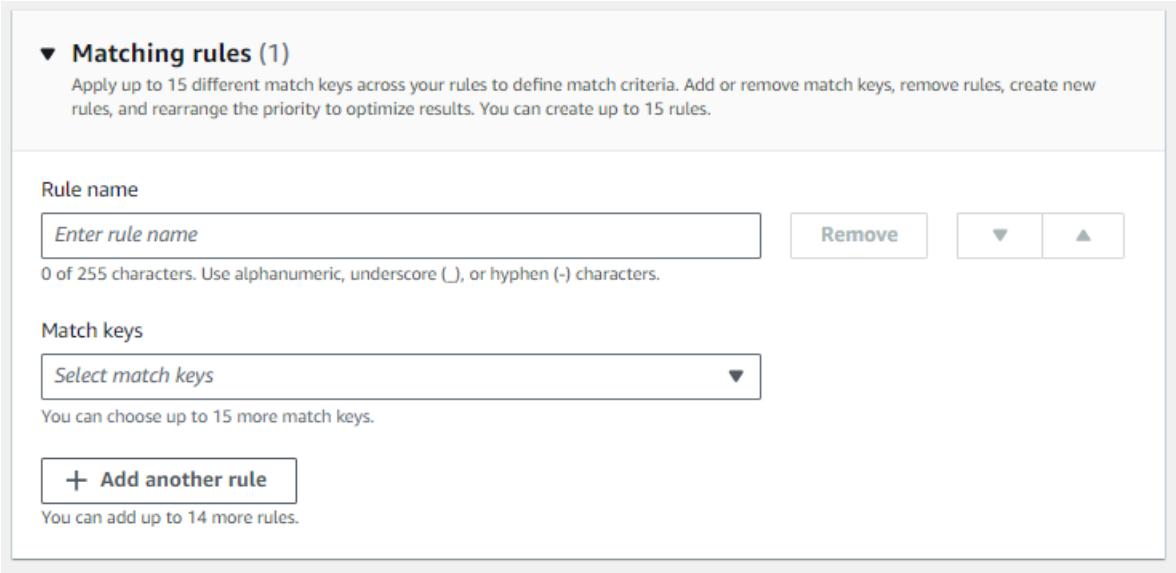
> **Note**
>
> Se você escolher Automático, certifique-se de ter EventBridge as notificações da Amazon ativadas para seu bucket do S3. Para obter instruções sobre como habilitar

a Amazon EventBridge usando o console do S3, consulte Habilitando a Amazon EventBridge no Guia do usuário do Amazon S3.

c. Em Regras de correspondência, insira um nome de regra e escolha as chaves de correspondência para essa regra.

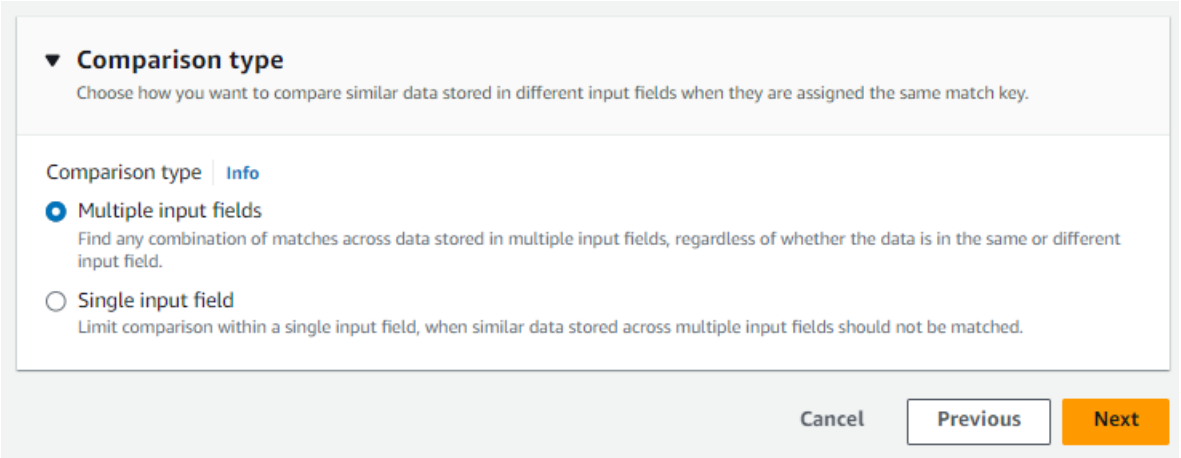
Você pode aplicar até 15 chaves de correspondência diferentes em suas regras para definir os critérios de correspondência.

Você pode criar até 15 regras.



d. Em Tipo de comparação, escolha uma das opções a seguir.

Se você deseja…	A seguir, escolha…
Encontre qualquer combinação de correspon dências nos dados armazenados em vários campos de entrada	Comparação de vários campos de entrada
Limitar a comparação a um único campo de entrada	Comparação de campo de entrada único



e. Escolha Próximo.

6. Para a Etapa 3: Especifique a saída e o formato dos dados:

   a. Em Destino e formato de saída de dados, escolha a localização do Amazon S3 para a saída de dados e se o formato dos dados será dados normalizados ou dados originais.

   b. Em Criptografia, se você optar por Personalizar as configurações de criptografia, insira o ARN da AWS KMS chave.

   c. Visualize a saída gerada pelo sistema.

   d. Para Saída de dados, visualize todos os campos incluídos.

   e. Determine se você deseja incluir, ocultar ou mascarar campos.

Se você deseja…	A seguir, escolha…
Incluir campos	Mantenha o estado de saída como Incluído.
Ocultar campos (excluir da saída)	Escolha o campo Saída e, em seguida, escolha Ocultar.
Campos de máscara	Escolha o campo Saída e, em seguida, escolha Saída de hash.
Redefinir as configurações anteriores	Escolha Redefinir.

   f. Escolha Próximo.

7. Para a Etapa 4: Revise e crie:

   a. Revise as seleções feitas nas etapas anteriores e edite, se necessário.

   b. Escolha Criar e executar.

      Uma mensagem aparece indicando que o fluxo de trabalho correspondente foi criado e que o trabalho foi iniciado.

8. Na página de detalhes do fluxo de trabalho correspondente, na guia Métricas, veja o seguinte em Métricas do último trabalho:

   - O Job ID.
   - O status da tarefa de fluxo de trabalho correspondente: Em fila, em andamento, concluída, com falha
   - O tempo concluído para o trabalho do fluxo de trabalho.
   - O número de registros processados.
   - O número de registros não processados.
   - Os IDs de correspondência exclusivos gerados.
   - O número de registros de entrada.

   Você também pode visualizar as métricas de trabalho para trabalhos de fluxo de trabalho correspondentes que foram executados anteriormente no Histórico de trabalhos.

9. Após a conclusão do trabalho de fluxo de trabalho correspondente (o status é concluído), você pode acessar a guia Saída de dados e selecionar sua localização no Amazon S3 para visualizar os resultados.

Agora está tudo pronto para:

- Editar um fluxo de trabalho correspondente
- Excluir um fluxo de trabalho correspondente
- Execute um fluxo de trabalho correspondente

Crie um fluxo de trabalho de correspondência baseado em aprendizado de máquina

O fluxo de trabalho de correspondência baseado em aprendizado de máquina permite comparar dados de texto não criptografado para encontrar uma ampla variedade de correspondências usando um modelo de aprendizado de máquina.

> **Note**
>
> O modelo de aprendizado de máquina não suporta a comparação de dados com hash.

Quando AWS Entity Resolution encontra uma correspondência entre dois ou mais registros em seus dados, ele atribui uma ID de correspondência aos registros no conjunto de dados correspondente.

Para correspondência baseada em aprendizado de máquina, ele aplica a porcentagem do nível de confiança da correspondência.

Para criar um fluxo de trabalho de correspondência baseado em ML:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Na página Fluxos de trabalho correspondentes, no canto superior direito, escolha Criar fluxo de trabalho correspondente.
4. Para a Etapa 1: Especificar os detalhes correspondentes do fluxo de trabalho, faça o seguinte:

    a. Insira um nome de fluxo de trabalho correspondente e uma Descrição opcional.

    b. Em Entrada de dados, escolha um AWS Glue banco de dados na lista suspensa, selecione a AWS Glue tabela e, em seguida, o mapeamento do esquema correspondente.

    Você pode adicionar até 20 entradas de dados.

    c. A opção Normalizar dados é selecionada por padrão, para que as entradas de dados sejam normalizadas antes da correspondência. Se você não quiser normalizar dados, desmarque a opção Normalizar dados.

    d. Especifique as permissões de Acesso ao serviço selecionando Criar e usar um novo perfil de serviço ou Usar um perfil de serviço existente.

Se você escolher...	Então
Criar e usar um novo perfil de serviço	• AWS Entity Resolution cria uma função de serviço com a política necessária para essa tabela. • O nome do perfil de serviço padrão é `entityresolution-matching-workflow-<timestamp>` . • Você deve ter permissões para criar perfis e anexar políticas. • Se seus dados de entrada estiverem criptografados, você poderá escolher a opção Esses dados são criptografados com uma chave KMS e, em seguida, inserir uma AWS KMS chave que será usada para descriptografar sua entrada de dados.

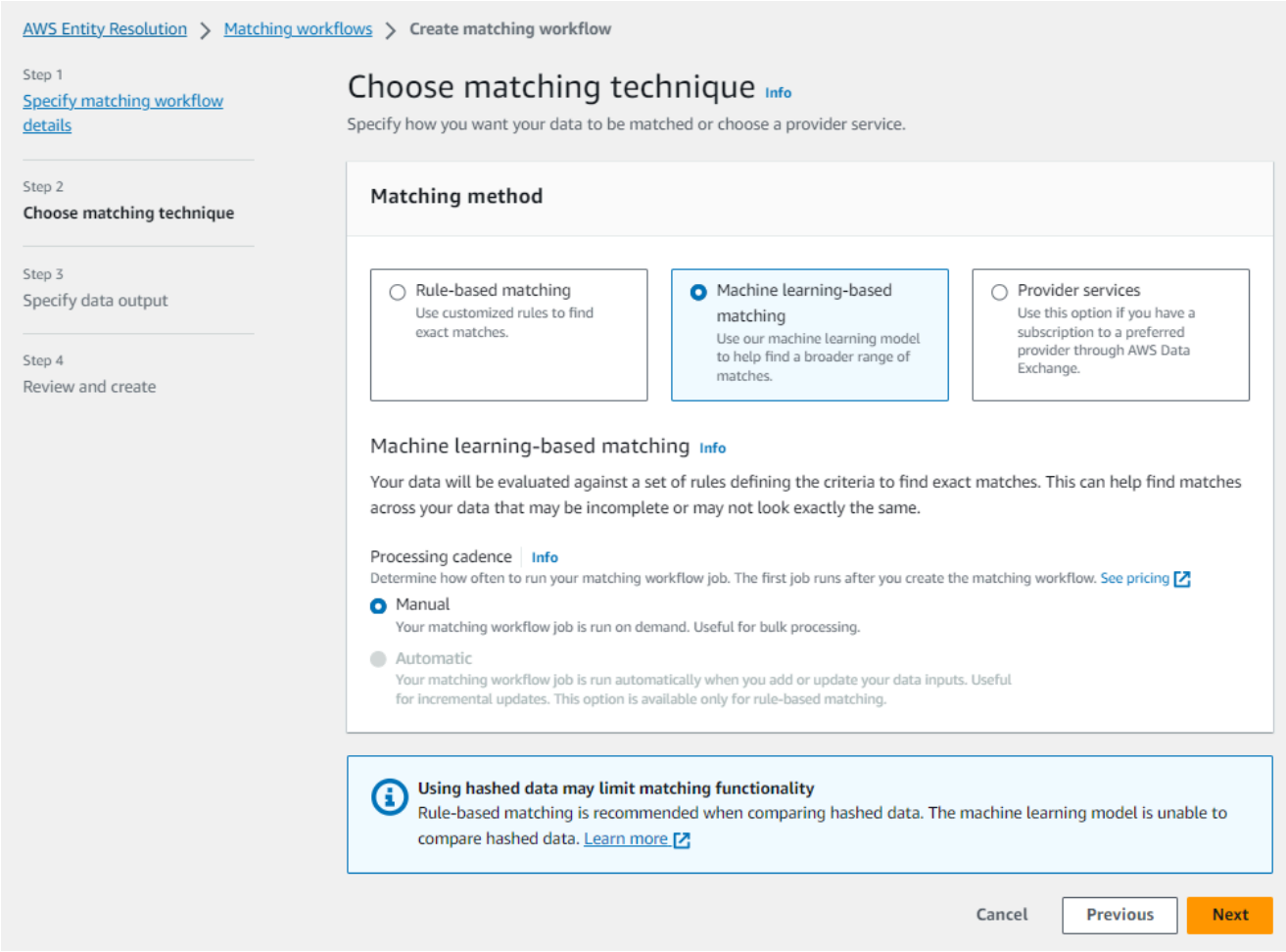
Se você escolher...	Então
Use um perfil de serviço existente	1. Escolha um nome do perfil de serviço existente na lista suspensa. A lista de perfis é exibida se você tiver permissões para listar funções. Se você não tiver permissões para listar perfis, insira o nome do recurso da Amazon (ARN) do perfil que você deseja usar. Se não houver perfis de serviço existentes, a opção de Usar um perfil de serviço existente não estará disponível. 2. Veja a função de serviço escolhendo o link externo Exibir no IAM. Por padrão, AWS Entity Resolution não tenta atualizar a política de função existente para adicionar as permissões necessárias.

e. (Opcional) Para ativar tags para o recurso, escolha Adicionar nova tag e insira o par de chave e valor.

f. Escolha Próximo.

5. Para a Etapa 2: Escolha a técnica de correspondência:

   a. Em Método de correspondência, escolha Correspondência baseada em aprendizado de máquina.



b. Em Cadência de processamento, a opção Manual é selecionada.

   Essa opção permite que você execute um fluxo de trabalho sob demanda para uma atualização em massa.

c. Escolha Próximo.

6. Para a Etapa 3: Especifique a saída e o formato dos dados:

   a. Em Destino e formato de saída de dados, escolha a localização do Amazon S3 para a saída de dados e se o formato dos dados será dados normalizados ou dados originais.

   b. Em Criptografia, se você optar por Personalizar as configurações de criptografia, insira o ARN da AWS KMS chave.

   c. Visualize a saída gerada pelo sistema.

   d. Para Saída de dados, visualize todos os campos incluídos.

   e. Determine se você deseja incluir, ocultar ou mascarar campos.

Se você deseja…	A seguir, escolha…
Incluir campos	Mantenha o estado de saída como Incluído.
Ocultar campos (excluir da saída)	Escolha o campo Saída e, em seguida, escolha Ocultar.
Campos de máscara	Escolha o campo Saída e, em seguida, escolha Saída de hash.
Redefinir as configurações anteriores	Escolha Redefinir.

f. Escolha Próximo.

7. Para a Etapa 4: Revise e crie:

   a. Revise as seleções feitas nas etapas anteriores e edite, se necessário.

   b. Escolha Criar e executar.

      Uma mensagem aparece indicando que o fluxo de trabalho correspondente foi criado e que o trabalho foi iniciado.

8. Na página de detalhes do fluxo de trabalho correspondente, na guia Métricas, veja o seguinte em Métricas do último trabalho:

   - O Job ID.
   - O status da tarefa de fluxo de trabalho correspondente: Em fila, em andamento, concluída, com falha
   - O tempo concluído para o trabalho do fluxo de trabalho.
   - O número de registros processados.
   - O número de registros não processados.
   - Os IDs de correspondência exclusivos gerados.
   - O número de registros de entrada.

   Você também pode visualizar as métricas de trabalho para trabalhos de fluxo de trabalho correspondentes que foram executados anteriormente no Histórico de trabalhos.

9. Após a conclusão do trabalho de fluxo de trabalho correspondente (o status é concluído), você pode acessar a guia Saída de dados e selecionar sua localização no Amazon S3 para visualizar os resultados.

Agora está tudo pronto para:

- Editar um fluxo de trabalho correspondente
- Excluir um fluxo de trabalho correspondente
- Execute um fluxo de trabalho correspondente

Crie um fluxo de trabalho de correspondência baseado em serviços do provedor

Se você tiver uma assinatura com um provedor de serviços por meio de AWS Data Exchange, poderá combinar seus identificadores conhecidos com seu provedor preferido. AWS Entity Resolution atualmente oferece suporte aos seguintes serviços de provedor de dados:

- LiveRamp
- TransUnion
- ID unificada 2.0

Para obter mais informações sobre como criar uma nova assinatura ou reutilizar uma assinatura existente de um serviço de provedor, consulteAssine um serviço de provedor em AWS Data Exchange.

As seções a seguir descrevem como criar um fluxo de trabalho de correspondência baseado no provedor.

Tópicos

- Criando um fluxo de trabalho correspondente com LiveRamp
- Criando um fluxo de trabalho correspondente com TransUnion
- Criando um fluxo de trabalho correspondente com o UID 2.0

Criando um fluxo de trabalho correspondente com LiveRamp

Se você tiver uma assinatura do LiveRamp serviço, poderá criar um fluxo de trabalho compatível com o LiveRamp serviço para realizar a resolução de identidade.

O LiveRamp serviço fornece um identificador chamado RampID. O RampID é um dos IDs mais usados em plataformas de demanda para criar um público para uma campanha publicitária. Usando um fluxo de trabalho correspondente com LiveRamp, você pode resolver endereços de e-mail com hash para RAMPIDs.

> **Note**
>
> AWS Entity Resolution suporta atribuição de RampID baseada em PII.

Esse fluxo de trabalho requer um bucket de preparação de dados do Amazon S3 no qual você deseja que a saída do fluxo de trabalho correspondente seja gravada temporariamente. Antes de criar um fluxo de trabalho de mapeamento de ID com LiveRamp, adicione as seguintes permissões ao intervalo de preparação de dados.

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

Substitua cada um <user input placeholder>por suas próprias informações.

balde de preparação	Bucket Amazon S3 que armazena temporari amente seus dados enquanto executa um fluxo de trabalho baseado em serviços do provedor.

Para criar um fluxo de trabalho correspondente com LiveRamp:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Na página Fluxos de trabalho correspondentes, no canto superior direito, escolha Criar fluxo de trabalho correspondente.
4. Para a Etapa 1: Especificar os detalhes correspondentes do fluxo de trabalho, faça o seguinte:

    a. Insira um nome de fluxo de trabalho correspondente e uma Descrição opcional.

    b. Em Entrada de dados, escolha um AWS Glue banco de dados na lista suspensa, selecione a AWS Glue tabela e, em seguida, selecione o mapeamento do esquema correspondente.

    Você pode adicionar até 20 entradas de dados.

c. A opção Normalizar dados é selecionada por padrão, para que as entradas de dados sejam normalizadas antes da correspondência.

   Se você estiver usando o processo de resolução somente por e-mail, desmarque a opção Normalizar dados, pois somente e-mails com hash são usados para dados de entrada.

d. Especifique as permissões de Acesso ao serviço selecionando Criar e usar um novo perfil de serviço ou Usar um perfil de serviço existente.

Se você escolher...	Então
Criar e usar um novo perfil de serviço	• AWS Entity Resolution cria uma função de serviço com a política necessária para essa tabela. • O nome do perfil de serviço padrão é `entityresolution-matching-workflow-<timestamp>` . • Você deve ter permissões para criar perfis e anexar políticas. • Se seus dados de entrada estiverem criptografados, você poderá escolher a opção Esses dados são criptografados com uma chave KMS e, em seguida, inserir uma AWS KMS chave que será usada para descriptografar sua entrada de dados.

Se você escolher...	Então
Use um perfil de serviço existente	1. Escolha um nome do perfil de serviço existente na lista suspensa. A lista de perfis é exibida se você tiver permissões para listar funções. Se você não tiver permissões para listar perfis, insira o nome do recurso da Amazon (ARN) do perfil que você deseja usar. Se não houver perfis de serviço existentes, a opção de Usar um perfil de serviço existente não estará disponível. 2. Veja a função de serviço escolhendo o link externo Exibir no IAM. Por padrão, AWS Entity Resolution não tenta atualizar a política de função existente para adicionar as permissões necessárias.

e. (Opcional) Para ativar tags para o recurso, escolha Adicionar nova tag e insira o par de chave e valor.

f. Escolha Próximo.

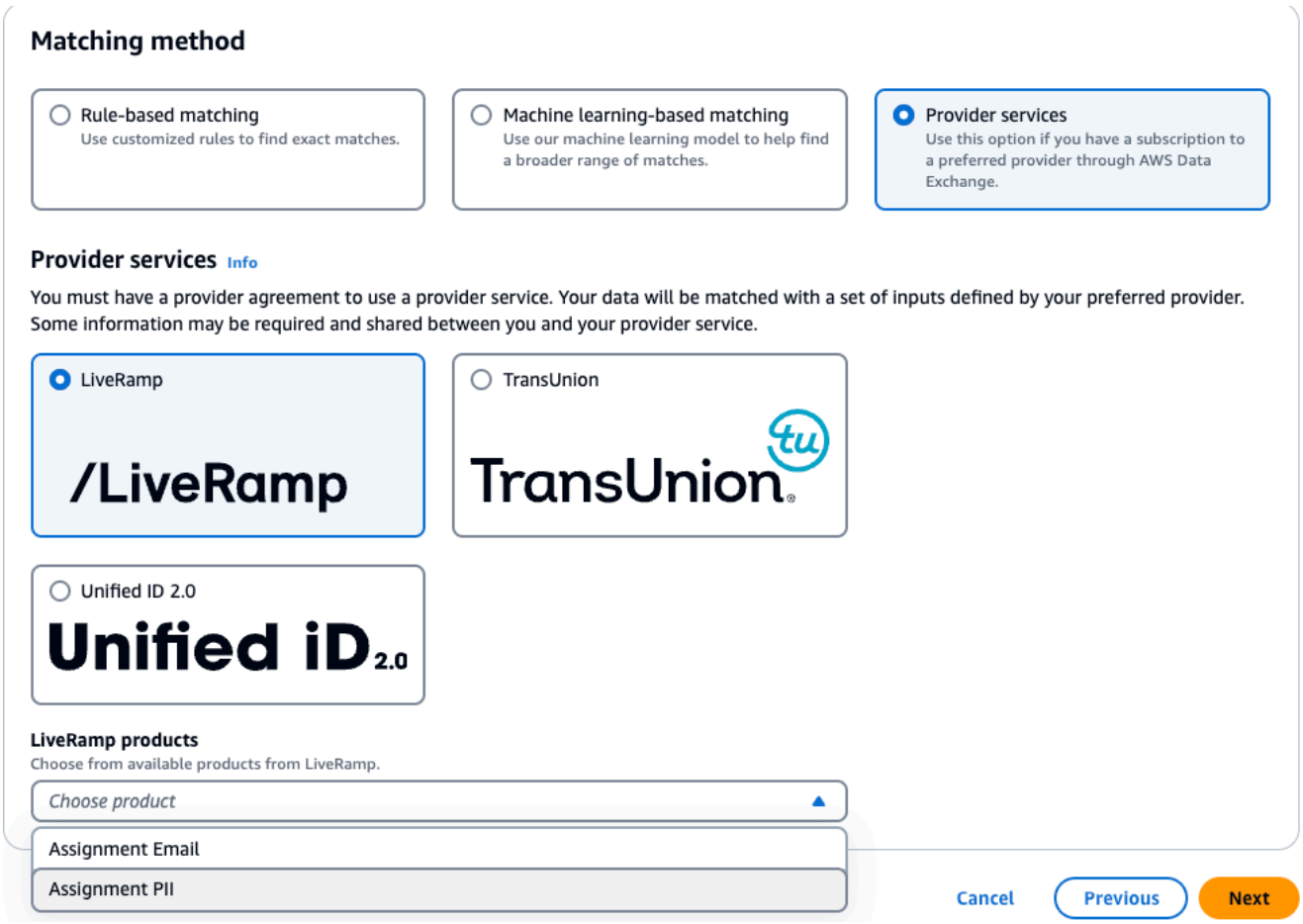
5. Para a Etapa 2: Escolha a técnica de correspondência:

   a. Em Método de correspondência, escolha Serviços do provedor.

   b. Para serviços do provedor, escolha LiveRamp.

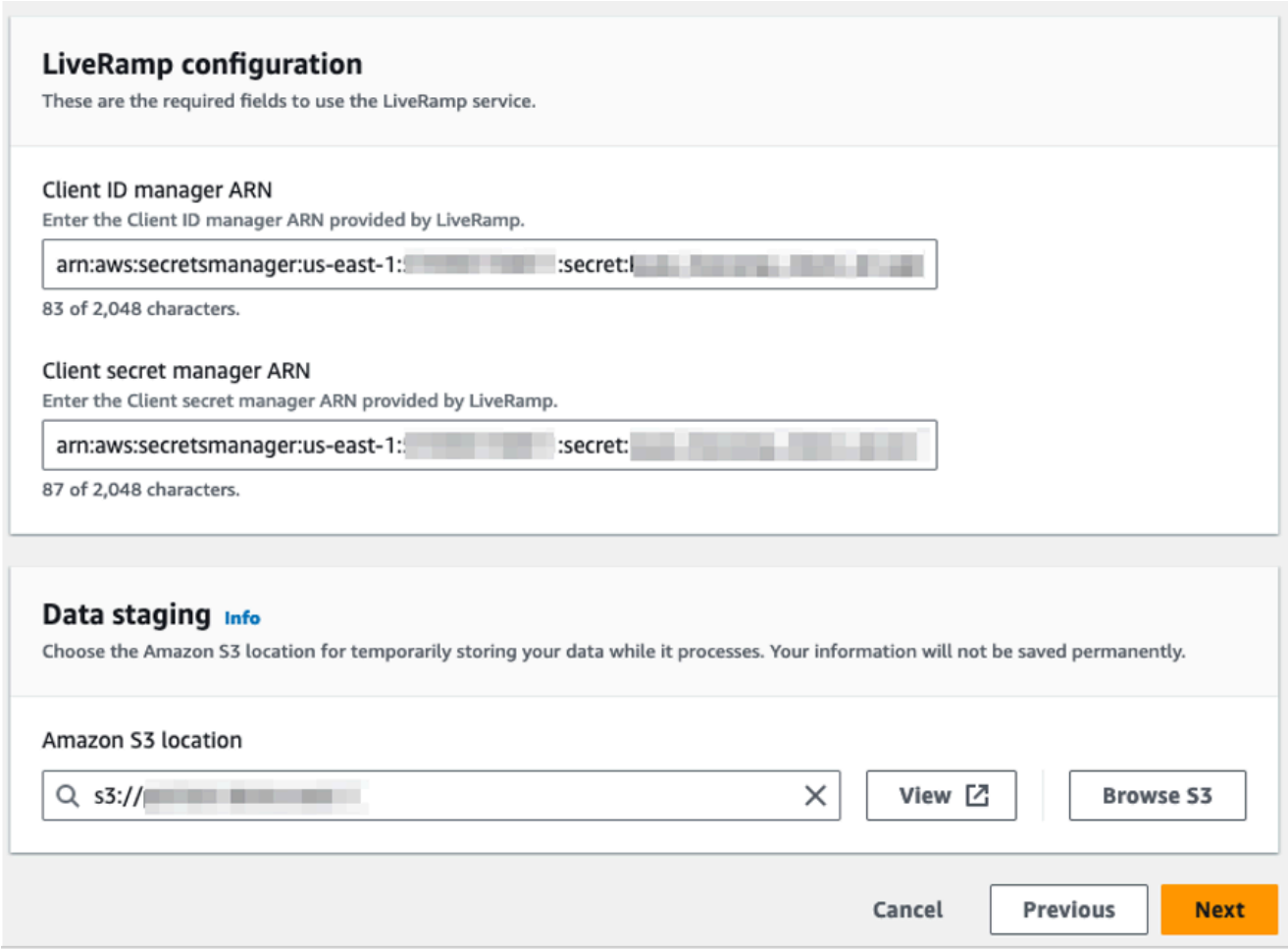
> **Note**
>
> Certifique-se de que o formato e a normalização do arquivo de entrada de dados estejam alinhados com as diretrizes do serviço do provedor.
> Para obter mais informações sobre as diretrizes de formatação do arquivo de entrada para o fluxo de trabalho correspondente, consulte Executar resolução de identidade por meio do ADX na LiveRamp documentação.

c. Para LiveRamp produtos, escolha um produto na lista suspensa.



> **Note**
>
> Se você escolher Atribuição PII, deverá fornecer pelo menos uma coluna sem identificador ao realizar a resolução da entidade. Por exemplo, GÊNERO.

d. Para LiveRamp configuração, insira um ARN do gerenciador de ID do cliente e um ARN do gerenciador secreto do cliente.



e. Para preparação de dados, escolha o local do Amazon S3 para o armazenamento temporário de seus dados enquanto eles são processados.

Você deve ter permissão para a localização do Amazon S3 de armazenamento de dados. Para ter mais informações, consulte the section called “Crie uma função de trabalho de fluxo de trabalho para AWS Entity Resolution”.

f. Escolha Próximo.

6. Para a Etapa 3: Especifique a saída de dados:

a. Em Destino e formato de saída de dados, escolha a localização do Amazon S3 para a saída de dados e se o formato dos dados será dados normalizados ou dados originais.

b. Em Criptografia, se você optar por Personalizar as configurações de criptografia, insira o ARN da AWS KMS chave.

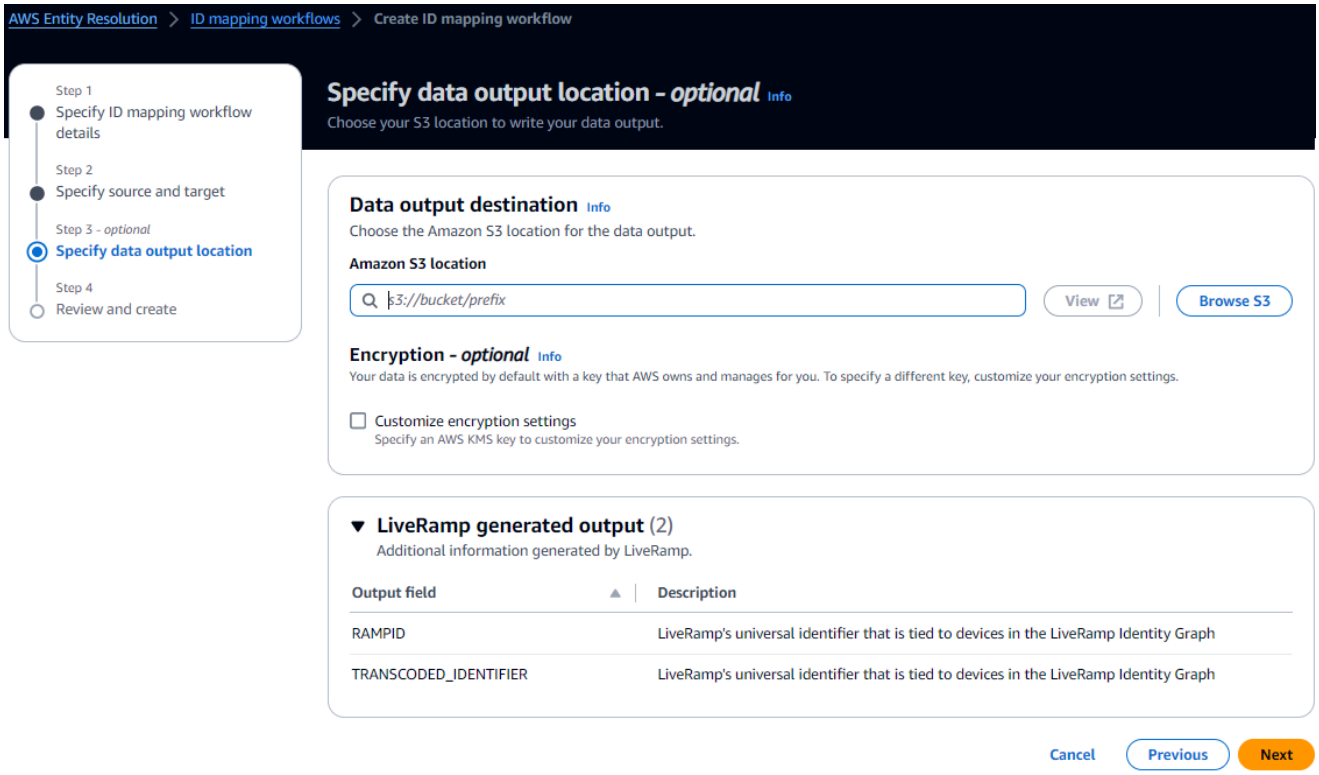
c. Visualize a saída LiveRamp gerada.

Essas são as informações adicionais geradas pelo LiveRamp.

d. Para Saída de dados, visualize todos os campos incluídos e determine se você deseja incluir, ocultar ou mascarar campos.

> **Note**
>
> Se você tiver escolhido LiveRamp, devido aos filtros de LiveRamp privacidade que removem as Informações de Identificação Pessoal (PII), alguns campos exibirão um estado de saída de Indisponível.

Se você deseja…	A seguir, escolha…
Incluir campos	Mantenha o estado de saída como Incluído.
Ocultar campos (excluir da saída)	Escolha o campo Saída e, em seguida, escolha Ocultar.
Campos de máscara	Escolha o campo Saída e, em seguida, escolha Saída de hash.
Redefinir as configurações anteriores	Escolha Redefinir.



e. Escolha Próximo.

7. Para a Etapa 4: Revise e crie:

   a. Revise as seleções feitas nas etapas anteriores e edite, se necessário.

   b. Escolha Criar e executar.

      Uma mensagem aparece indicando que o fluxo de trabalho correspondente foi criado e que o trabalho foi iniciado.

8. Na página de detalhes do fluxo de trabalho correspondente, na guia Métricas, veja o seguinte em Métricas do último trabalho:

   - O Job ID.
   - O status da tarefa de fluxo de trabalho correspondente: Em fila, em andamento, concluída, com falha
   - O tempo concluído para o trabalho do fluxo de trabalho.
   - O número de registros processados.
   - O número de registros não processados.
   - Os IDs de correspondência exclusivos gerados.

- O número de registros de entrada.

Você também pode visualizar as métricas de trabalho para trabalhos de fluxo de trabalho correspondentes que foram executados anteriormente no Histórico de trabalhos.

9. Após a conclusão do trabalho de fluxo de trabalho correspondente (o status é concluído), você pode acessar a guia Saída de dados e selecionar sua localização no Amazon S3 para visualizar os resultados.

Agora está tudo pronto para:

- Editar um fluxo de trabalho correspondente
- Excluir um fluxo de trabalho correspondente

Criando um fluxo de trabalho correspondente com TransUnion

Se você tiver uma assinatura do TransUnion serviço, poderá melhorar a compreensão do cliente vinculando, combinando e aprimorando os registros relacionados ao cliente armazenados em canais diferentes com chaves eletrônicas TransUnion pessoais e domésticas e mais de 200 atributos de dados.

O TransUnion serviço fornece identificadores conhecidos como IDs TransUnion individuais e domésticos. TransUnionfornece atribuição de ID (também conhecida como codificação) de identificadores conhecidos, como nome, endereço, número de telefone e endereço de e-mail.

Esse fluxo de trabalho requer um bucket de preparação de dados do Amazon S3 no qual você deseja que a saída do fluxo de trabalho correspondente seja gravada temporariamente. Antes de criar um fluxo de trabalho correspondente com TransUnion, adicione as seguintes permissões ao intervalo de preparação de dados.

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

Substitua cada um <user input placeholder>por suas próprias informações.

balde de preparação	Bucket Amazon S3 que armazena temporari amente seus dados enquanto executa um fluxo de trabalho baseado em serviços do provedor.

Para criar um fluxo de trabalho correspondente com TransUnion:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com seu Conta da AWS (se ainda não tiver feito isso).

2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Na página Fluxos de trabalho correspondentes, no canto superior direito, escolha Criar fluxo de trabalho correspondente.
4. Para a Etapa 1: Especificar os detalhes correspondentes do fluxo de trabalho, faça o seguinte:

   a. Insira um nome de fluxo de trabalho correspondente e uma Descrição opcional.

   b. Em Entrada de dados, escolha um AWS Glue banco de dados na lista suspensa, selecione a AWS Glue tabela e, em seguida, selecione o mapeamento do esquema correspondente.

      Você pode adicionar até 20 entradas de dados.

   c. A opção Normalizar dados é selecionada por padrão, para que as entradas de dados sejam normalizadas antes da correspondência. Se você não quiser normalizar dados, desmarque a opção Normalizar dados.

   d. Especifique as permissões de Acesso ao serviço selecionando Criar e usar um novo perfil de serviço ou Usar um perfil de serviço existente.

Se você escolher...	Então
Criar e usar um novo perfil de serviço	• AWS Entity Resolution cria uma função de serviço com a política necessária para essa tabela. • O nome do perfil de serviço padrão é `entityresolution-matching-workflow-<timestamp>` . • Você deve ter permissões para criar perfis e anexar políticas. • Se seus dados de entrada estiverem criptografados, você poderá escolher a opção Esses dados são criptografados com uma chave KMS e, em seguida, inserir uma AWS KMS chave que será usada para descriptografar sua entrada de dados.

Se você escolher...	Então
Use um perfil de serviço existente	1. Escolha um nome do perfil de serviço existente na lista suspensa. A lista de perfis é exibida se você tiver permissões para listar funções. Se você não tiver permissões para listar perfis, insira o nome do recurso da Amazon (ARN) do perfil que você deseja usar. Se não houver perfis de serviço existentes, a opção de Usar um perfil de serviço existente não estará disponível. 2. Veja a função de serviço escolhendo o link externo Exibir no IAM. Por padrão, AWS Entity Resolution não tenta atualizar a política de função existente para adicionar as permissões necessárias.

e. (Opcional) Para ativar tags para o recurso, escolha Adicionar nova tag e insira o par de chave e valor.

f. Escolha Próximo.

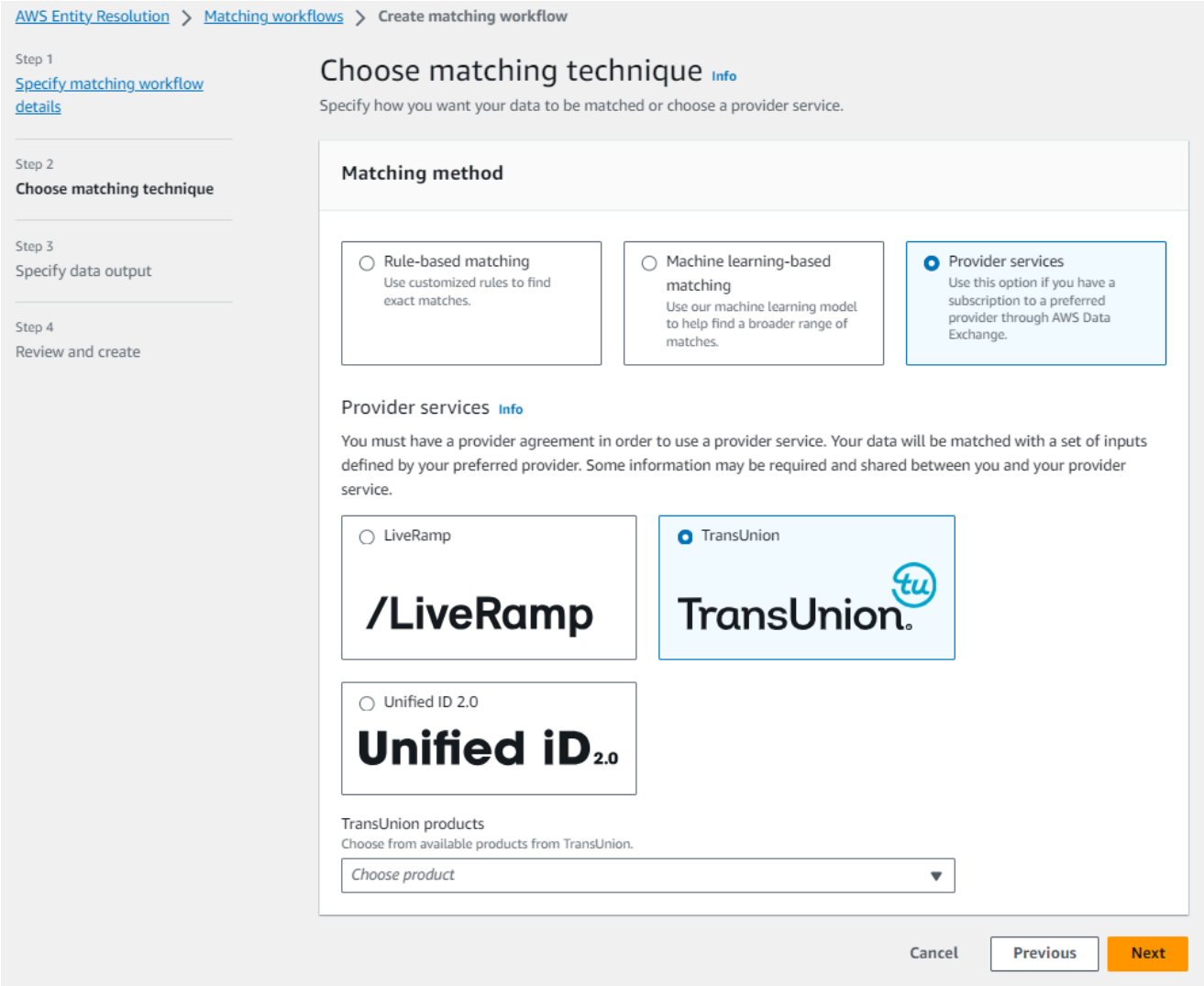
5. Para a Etapa 2: Escolha a técnica de correspondência:

a. Em Método de correspondência, escolha Serviços do provedor.

b. Para serviços do provedor, escolha TransUnion.

> **Note**
>
> Certifique-se de que o formato e a normalização do arquivo de entrada de dados estejam alinhados com as diretrizes do serviço do provedor.

c. Para TransUnion produtos, escolha um produto na lista suspensa.



d. Para preparação de dados, escolha o local do Amazon S3 para o armazenamento temporário de seus dados enquanto eles são processados.

Você deve ter permissão para a localização do Amazon S3 de armazenamento de dados. Para ter mais informações, consulte the section called “Crie uma função de trabalho de fluxo de trabalho para AWS Entity Resolution”.

6. Escolha Próximo.
7. Para a Etapa 3: Especifique a saída de dados:
   a. Em Destino e formato de saída de dados, escolha a localização do Amazon S3 para a saída de dados e se o formato dos dados será dados normalizados ou dados originais.
   b. Em Criptografia, se você optar por Personalizar as configurações de criptografia, insira o ARN da AWS KMS chave.
   c. Visualize a saída TransUnion gerada.

      Essas são as informações adicionais geradas pelo TransUnion.
   d. Para Saída de dados, visualize todos os campos incluídos e determine se você deseja incluir, ocultar ou mascarar campos.

Se você deseja…	A seguir, escolha…
Incluir campos	Mantenha o estado de saída como Incluído.
Ocultar campos (excluir da saída)	Escolha o campo Saída e, em seguida, escolha Ocultar.
Campos de máscara	Escolha o campo Saída e, em seguida, escolha Saída de hash.
Redefinir as configurações anteriores	Escolha Redefinir.

   e. Para a saída gerada pelo sistema, visualize todos os campos incluídos.
   f. Escolha Próximo.
8. Para a Etapa 4: Revise e crie:
   a. Revise as seleções feitas nas etapas anteriores e edite, se necessário.
   b. Escolha Criar e executar.

      Uma mensagem aparece indicando que o fluxo de trabalho correspondente foi criado e que o trabalho foi iniciado.

9. Na página de detalhes do fluxo de trabalho correspondente, na guia Métricas, veja o seguinte em Métricas do último trabalho:

   - O Job ID.
   - O status da tarefa de fluxo de trabalho correspondente: Em fila, em andamento, concluída, com falha
   - O tempo concluído para o trabalho do fluxo de trabalho.
   - O número de registros processados.
   - O número de registros não processados.
   - Os IDs de correspondência exclusivos gerados.
   - O número de registros de entrada.

   Você também pode visualizar as métricas de trabalho para trabalhos de fluxo de trabalho correspondentes que foram executados anteriormente no Histórico de trabalhos.
10. Após a conclusão do trabalho de fluxo de trabalho correspondente (o status é concluído), você pode acessar a guia Saída de dados e selecionar sua localização no Amazon S3 para visualizar os resultados.

Agora está tudo pronto para:

- Editar um fluxo de trabalho correspondente
- Excluir um fluxo de trabalho correspondente

Criando um fluxo de trabalho correspondente com o UID 2.0

Se você tiver uma assinatura do serviço Unified ID 2.0, poderá ativar campanhas publicitárias com identidade determinística e confiar na interoperabilidade com muitos participantes habilitados para UID2 em todo o ecossistema de publicidade. Para obter mais informações, consulte Visão geral do Unified ID 2.0.

O serviço Unified ID 2.0 fornece UID 2 bruto, que é usado para criar campanhas publicitárias na plataforma The Trade Desk. O UID 2.0 é gerado usando uma estrutura de código aberto.

Em um fluxo de trabalho, você pode usar um **`Email Address`** ou **`Phone number`** para a geração bruta de UID2, mas não ambos. Se ambos estiverem presentes no mapeamento do esquema, o fluxo de trabalho escolherá o **`Email Address`** e o **`Phone number`** será um campo de passagem.

Para oferecer suporte a ambos, crie um novo mapeamento de esquema onde **`Phone number`** está mapeado, mas não **`Email Address`** está. Em seguida, crie um segundo fluxo de trabalho usando esse novo mapeamento de esquema.

> **Note**
>
> Os UID2s brutos são criados pela adição de sais de baldes de sal que são girados aproximadamente uma vez por ano, fazendo com que o UID2 bruto também seja rotacionado com ele, portanto, é recomendável que você atualize os UID2s brutos diariamente. Para obter mais informações, consulte https://unifiedid.com/docs/getting-started/gs-faqs # how-often-should-uid 2 s-be-refreshed-for -incremental-updates

Para criar um fluxo de trabalho correspondente com o UID 2.0:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Na página Fluxos de trabalho correspondentes, no canto superior direito, escolha Criar fluxo de trabalho correspondente.
4. Para a Etapa 1: Especificar os detalhes correspondentes do fluxo de trabalho, faça o seguinte:
   a. Insira um nome de fluxo de trabalho correspondente e uma Descrição opcional.
   b. Em Entrada de dados, escolha um AWS Glue banco de dados na lista suspensa, selecione a AWS Glue tabela e, em seguida, selecione o mapeamento do esquema correspondente.

      Você pode adicionar até 20 entradas de dados.
   c. Deixe a opção Normalizar dados selecionada, para que as entradas de dados (**`Email Address`**ou**`Phone number`**) sejam normalizadas antes da correspondência.

      Para obter mais informações sobre **`Email Address`** normalização, consulte Normalização de endereço de e-mail na documentação do UID 2.0.

      Para obter mais informações sobre **`Phone number`** normalização, consulte Normalização do número de telefone na documentação do UID 2.0.
   d. Especifique as permissões de Acesso ao serviço selecionando Criar e usar um novo perfil de serviço ou Usar um perfil de serviço existente.

Se você escolher...	Então
Criar e usar um novo perfil de serviço	• AWS Entity Resolution cria uma função de serviço com a política necessária para essa tabela. • O nome do perfil de serviço padrão é `entityresolution-matching-workflow-<timestamp>` . • Você deve ter permissões para criar perfis e anexar políticas. • Se seus dados de entrada estiverem criptografados, você poderá escolher a opção Esses dados são criptografados com uma chave KMS e, em seguida, inserir uma AWS KMS chave que será usada para descriptografar sua entrada de dados.

Se você escolher...	Então
Use um perfil de serviço existente	1. Escolha um nome do perfil de serviço existente na lista suspensa. A lista de perfis é exibida se você tiver permissões para listar funções. Se você não tiver permissões para listar perfis, insira o nome do recurso da Amazon (ARN) do perfil que você deseja usar. Se não houver perfis de serviço existentes, a opção de Usar um perfil de serviço existente não estará disponível. 2. Veja a função de serviço escolhendo o link externo Exibir no IAM. Por padrão, AWS Entity Resolution não tenta atualizar a política de função existente para adicionar as permissões necessárias.

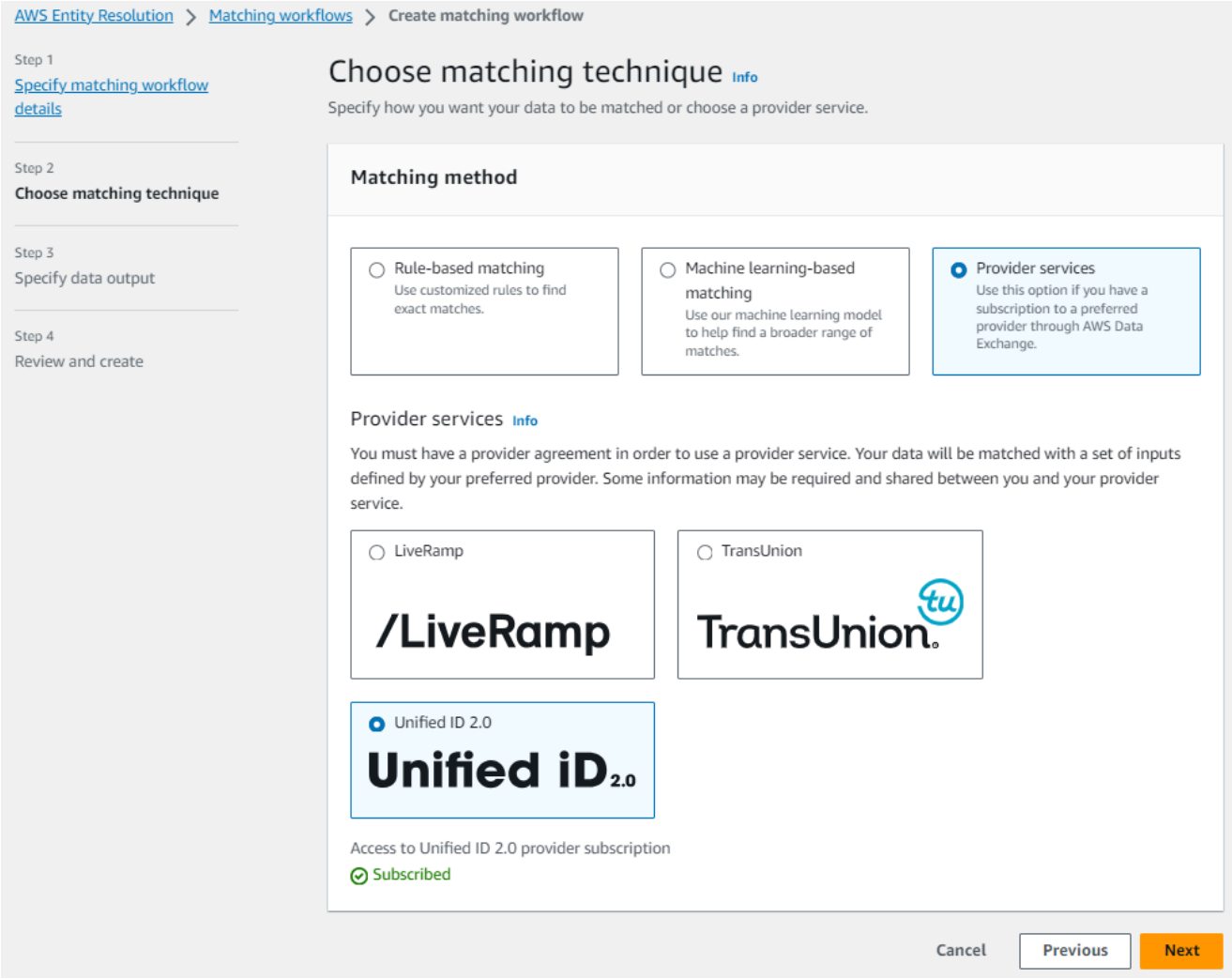
e. (Opcional) Para ativar tags para o recurso, escolha Adicionar nova tag e insira o par de chave e valor.

f. Escolha Próximo.

5. Para a Etapa 2: Escolha a técnica de correspondência:

a. Em Método de correspondência, escolha Serviços do provedor.

b. Para serviços de provedor, escolha Unified ID 2.0.



c. Escolha Próximo.

6. Para a Etapa 3: Especifique a saída de dados:

   a. Em Destino e formato de saída de dados, escolha a localização do Amazon S3 para a saída de dados e se o formato dos dados será dados normalizados ou dados originais.

   b. Em Criptografia, se você optar por Personalizar as configurações de criptografia, insira o ARN da AWS KMS chave.

   c. Veja a saída gerada pelo Unified ID 2.0.

      Esta é uma lista de todas as informações adicionais geradas pelo UID 2.0

   d. Para Saída de dados, visualize todos os campos incluídos e determine se você deseja incluir, ocultar ou mascarar campos.

Se você deseja…	A seguir, escolha…
Incluir campos	Mantenha o estado de saída como Incluído.
Ocultar campos (excluir da saída)	Escolha o campo Saída e, em seguida, escolha Ocultar.
Campos de máscara	Escolha o campo Saída e, em seguida, escolha Saída de hash.
Redefinir as configurações anteriores	Escolha Redefinir.

e. Para a saída gerada pelo sistema, visualize todos os campos incluídos.

f. Escolha Próximo.

7. Para a Etapa 4: Revise e crie:

   a. Revise as seleções feitas nas etapas anteriores e edite, se necessário.

   b. Escolha Criar e executar.

      Uma mensagem aparece indicando que o fluxo de trabalho correspondente foi criado e que o trabalho foi iniciado.

8. Na página de detalhes do fluxo de trabalho correspondente, na guia Métricas, veja o seguinte em Métricas do último trabalho:

   - O Job ID.
   - O status da tarefa de fluxo de trabalho correspondente: Em fila, em andamento, concluída, com falha
   - O tempo concluído para o trabalho do fluxo de trabalho.
   - O número de registros processados.
   - O número de registros não processados.
   - Os IDs de correspondência exclusivos gerados.
   - O número de registros de entrada.

Você também pode visualizar as métricas de trabalho para trabalhos de fluxo de trabalho correspondentes que foram executados anteriormente no Histórico de trabalhos.

9. Após a conclusão do trabalho de fluxo de trabalho correspondente (o status é concluído), você pode acessar a guia Saída de dados e selecionar sua localização no Amazon S3 para visualizar os resultados.

Agora está tudo pronto para:

- Editar um fluxo de trabalho correspondente
- Excluir um fluxo de trabalho correspondente

Execute um fluxo de trabalho correspondente

Depois de criar um fluxo de trabalho de correspondência baseado em regras ou baseado em aprendizado de máquina com o tipo de processamento Manual, você pode executar um trabalho de fluxo de trabalho correspondente.

> **Note**
>
> Se você criar um fluxo de trabalho correspondente com o tipo de processamento automático, seus trabalhos de fluxo de trabalho correspondentes serão executados sempre que uma entrada de dados for atualizada.

AWS Entity Resolution lê seus dados do local ou locais especificados e encontra uma correspondência entre dois ou mais registros em seus dados. Em seguida, ele atribui uma ID de correspondência aos registros no conjunto de dados correspondente.

- Se você especificou a técnica de correspondência baseada em regras, também AWS Entity Resolution atribuirá o número da regra aplicada que gerou a correspondência.
- Se você especificou a técnica de correspondência baseada em aprendizado de máquina, também AWS Entity Resolution atribuirá a porcentagem do nível de confiança da correspondência.

AWS Entity Resolution em seguida, grava os arquivos de saída de dados em um local que você escolher.

Um fluxo de trabalho pode ter várias execuções e os resultados (acertos ou erros) são gravados em uma pasta com `jobId` o nome.

A saída de dados contém um arquivo para correspondências bem-sucedidas e um arquivo para erros. A saída de dados pode conter vários campos. Os resultados bem-sucedidos são gravados em uma `success` pasta e a pasta conterá vários arquivos, cada um contendo um subconjunto dos registros bem-sucedidos. Da mesma forma, os erros são gravados em uma `error` pasta com vários campos, cada um contendo um subconjunto dos registros de erro. Para obter mais informações sobre a solução de problemas de erros, consulteSolução de problemas de fluxos de trabalho.

Para executar um fluxo de trabalho correspondente:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Escolha o fluxo de trabalho correspondente.
4. Na página de detalhes do fluxo de trabalho correspondente, no canto superior direito, escolha Executar fluxo de trabalho.

   É exibida uma mensagem indicando que o trabalho foi iniciado.
5. Na guia Métricas, em Histórico de trabalhos, veja o seguinte:

   - O status do trabalho de fluxo de trabalho correspondente: Em andamento, concluído, com falha
   - O número de registros processados.
   - O número de correspondências encontradas.
   - O número de registros exclusivos.
   - A duração do trabalho.
   - O Job ID.
6. Após a conclusão do trabalho de fluxo de trabalho correspondente (o status é concluído), você pode acessar a guia Saída de dados e selecionar sua localização no Amazon S3 para visualizar os resultados.

Próximas etapas

Agora está tudo pronto para:

- Editar um fluxo de trabalho correspondente
- Excluir um fluxo de trabalho correspondente

Criação de um namespace de ID

Um namespace de ID é um invólucro em torno de sua tabela de dados que você usa para fornecer metadados que explicam seus dados e técnicas de correspondência e como usá-los em um fluxo de trabalho de mapeamento de ID.

Há dois tipos de namespaces de ID: Origem e Destino.

- A Fonte contém configurações para os dados de origem que são AWS Entity Resolution processados em um fluxo de trabalho de mapeamento de ID.
- O Target contém uma configuração dos dados de destino para os quais todas as fontes resolvem.

Você pode definir os dados de entrada que deseja resolver em dois Contas da AWS em um fluxo de trabalho de mapeamento de ID. Um participante cria uma fonte de namespace de ID e outro cria um destino de namespace de ID. Depois que os participantes criarem a origem e o destino, você poderá executar um fluxo de trabalho de mapeamento de ID para traduzir os dados da origem para o destino.

Os tópicos a seguir orientam você por um conjunto de etapas para criar os namespaces de ID de origem e destino e, em seguida, especificar sua saída de dados no Amazon Simple Storage Service (Amazon S3).

> **Note**
>
> AWS Entity Resolution atualmente oferece LiveRamp transcodificação para o método de namespace ID quando você cria um namespace ID.

Tópicos

Crie uma fonte de namespace de ID

Este tópico descreve o processo de criação de uma fonte de namespace de ID no AWS Entity Resolution console. Essa é a fonte dos dados em um fluxo de trabalho de mapeamento de ID.

> **Note**
>
> Se os dados de entrada forem a fonte, eles deverão ter um mapeamento de esquema e um AWS Glue banco de dados associado.

Para criar uma fonte de namespace de ID

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Preparação de dados, escolha Namespaces de ID.
3. Na página de namespaces de ID, no canto superior direito, escolha Criar namespace de ID.
4. Para obter detalhes, faça o seguinte:
   a. Em Nome do namespace ID, insira um nome exclusivo.
   b. (Opcional) Em Descrição, insira uma descrição opcional.
   c. Para o tipo de namespace de ID, escolha Origem.
5. Veja o método do namespace ID.

   > **Note**
   >
   > AWS Entity Resolution atualmente oferece o serviço de LiveRamp provedor como um método de namespace de ID. Se você tiver uma assinatura LiveRamp, o status aparecerá como Assinado. Para obter mais informações sobre como assinar LiveRamp, consulteAssine um serviço de provedor em AWS Data Exchange.

6. Em Entrada de dados, escolha o AWS Glue banco de dados, a AWS Glue tabela e o mapeamento do esquema na lista suspensa.

   Você pode adicionar até 20 entradas de dados.
7. Para especificar as permissões de acesso ao serviço, escolha Criar e usar uma nova função de serviço ou Usar uma função de serviço existente.

Se você escolher...	Então
Criar e usar um novo perfil de serviço	AWS Entity Resolution cria uma função de serviço com a política necessária para essa tabela. O nome padrão da função de serviço é `entityresolution-id-mapping-workflow-<timestamp>` . Você deve ter permissões para criar perfis e anexar políticas. Se seus dados de entrada estiverem criptografados, escolha a opção Esses dados são criptografados por uma chave KMS. Em seguida, insira uma AWS KMS chave usada para descriptografar sua entrada de dados.

Se você escolher...	Então
Use um perfil de serviço existente	Escolha um nome do perfil de serviço existente na lista suspensa. Se você tiver permissões para listar funções, a lista de funções será exibida. Se você não tiver permissões para listar funções, poderá inserir o Amazon Resource Name (ARN) da função que deseja usar. Se não houver funções de serviço existentes, a opção Usar uma função de serviço existente não estará disponível. Por padrão, AWS Entity Resolutio n não tenta atualizar a política de função existente para adicionar as permissões necessárias.

8. (Opcional) Para ativar tags para o recurso, escolha Adicionar nova tag e, em seguida, insira o par de chave e valor.
9. Escolha Criar namespace de ID.

Criar um destino de namespace de ID

Este tópico descreve o processo de criação de um destino de namespace de ID no AWS Entity Resolution console. Esse é o destino dos dados em um fluxo de trabalho de mapeamento de ID. Todas as fontes são direcionadas para o alvo.

Para criar um destino de namespace de ID

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Preparação de dados, escolha Namespaces de ID.
3. Na página de namespaces de ID, no canto superior direito, escolha Criar namespace de ID.
4. Para obter detalhes, faça o seguinte:
   a. Em Nome do namespace ID, insira um nome exclusivo.
   b. (Opcional) Em Descrição, insira uma descrição opcional.
   c. Para o tipo de namespace de ID, escolha Target.
5. Veja o método do namespace ID.

> **Note**
>
> AWS Entity Resolution atualmente oferece o serviço de LiveRamp provedor como um método de namespace de ID.
> Se você tiver uma assinatura LiveRamp, o status aparecerá como Assinado.
> Para obter mais informações sobre como assinar LiveRamp, consulteAssine um serviço de provedor em AWS Data Exchange.

6. Em Domínio de destino, insira o identificador de domínio LiveRamp do cliente destinado à transcodificação que LiveRamp fornece.
7. (Opcional) Para ativar tags para o recurso, escolha Adicionar nova tag e, em seguida, insira o par de chave e valor.
8. Escolha Criar namespace de ID.

Depois de criar os namespaces de ID necessários para um fluxo de trabalho de mapeamento de ID em dois Contas da AWS, você está pronto para criar o fluxo de trabalho de mapeamento de ID.

Criando um fluxo de trabalho de mapeamento de ID

O fluxo de trabalho de mapeamento de ID no momento AWS Entity Resolution está integrado ao LiveRamp. Se você tiver uma assinatura do LiveRamp serviço, poderá criar um fluxo de trabalho de mapeamento de ID LiveRamp para realizar a transcodificação. Com a LiveRamp transcodificação, você pode traduzir um conjunto de RAMPIDs de origem em qualquer RAMPID de destino. Ao usar o RampID como um token para representar seus clientes, você pode evitar o compartilhamento de dados do cliente diretamente com plataformas de publicidade.

Você pode realizar o mapeamento de ID entre dois conjuntos de dados sozinho Conta da AWS ou em dois conjuntos de dados diferentes Contas da AWS. Sua fonte e destino de entrada de dados dependem do tipo de mapeamento de ID que você deseja realizar.

Para obter mais informações, consulte Executar tradução por meio do ADX no site da LiveRamp documentação.

Tópicos

Pré-requisito

Esse fluxo de trabalho de mapeamento de ID requer um bucket de preparação de dados do Amazon Simple Storage Service (Amazon S3) no qual você deseja gravar temporariamente a saída do fluxo de trabalho de mapeamento de ID. Antes de criar um fluxo de trabalho de mapeamento de ID com LiveRamp, adicione a seguinte política de permissões, que permite acessar o intervalo de preparação de dados.

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

Na política de permissões anterior, substitua cada uma <user input placeholder>por suas próprias informações.

balde de preparação	O bucket do Amazon S3 que armazena temporariamente seus dados enquanto executa um fluxo de trabalho baseado em serviços do provedor.

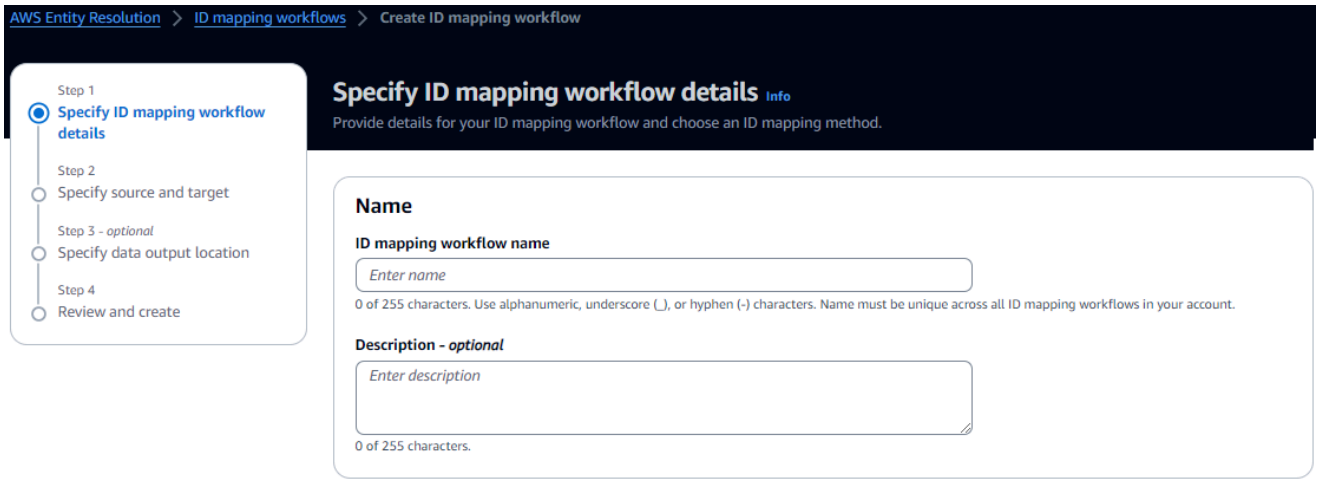
Criando um fluxo de trabalho de mapeamento de ID para um Conta da AWS

Depois de concluir as etapas de configuração e criar um mapeamento de esquema, você pode criar um ou mais fluxos de trabalho de mapeamento de ID para traduzir um conjunto de RAMPIDs de origem para outro usando RAMPIDs mantidos ou derivados.

Para criar um fluxo de trabalho de mapeamento de ID para um Conta da AWS

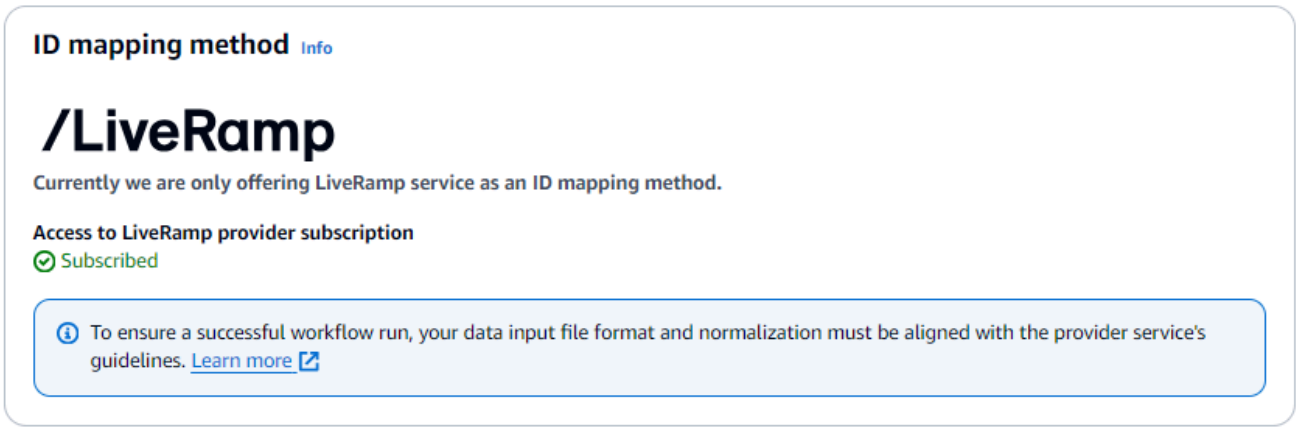
1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Mapeamento de ID.
3. Na página Fluxos de trabalho de mapeamento de ID, no canto superior direito, escolha Criar fluxo de trabalho de mapeamento de ID.
4. Para a Etapa 1: Especificar detalhes do fluxo de trabalho de mapeamento de ID, faça o seguinte:

   a. Insira um nome de fluxo de trabalho de mapeamento de ID e uma Descrição opcional.



   b. Veja o método de mapeamento de ID.

      AWS Entity Resolution atualmente oferece o serviço do LiveRamp provedor como um método de mapeamento de ID. Se você tiver uma assinatura LiveRamp, o status aparecerá como Assinado. Para obter mais informações sobre como assinar LiveRamp, consulteAssine um serviço de provedor em AWS Data Exchange.



> **Note**
>
> Certifique-se de que o formato do arquivo de entrada de dados esteja alinhado com as diretrizes do serviço do provedor. Para obter mais informações sobre as diretrizes de formatação LiveRamp do arquivo de entrada, consulte Executar tradução por meio do ADX no site da LiveRamp documentação.

c. Para LiveRamp configuração, insira os seguintes valores que LiveRamp fornecem:

- Gerenciador de ID de cliente ARN
- Gerenciador secreto do cliente ARN

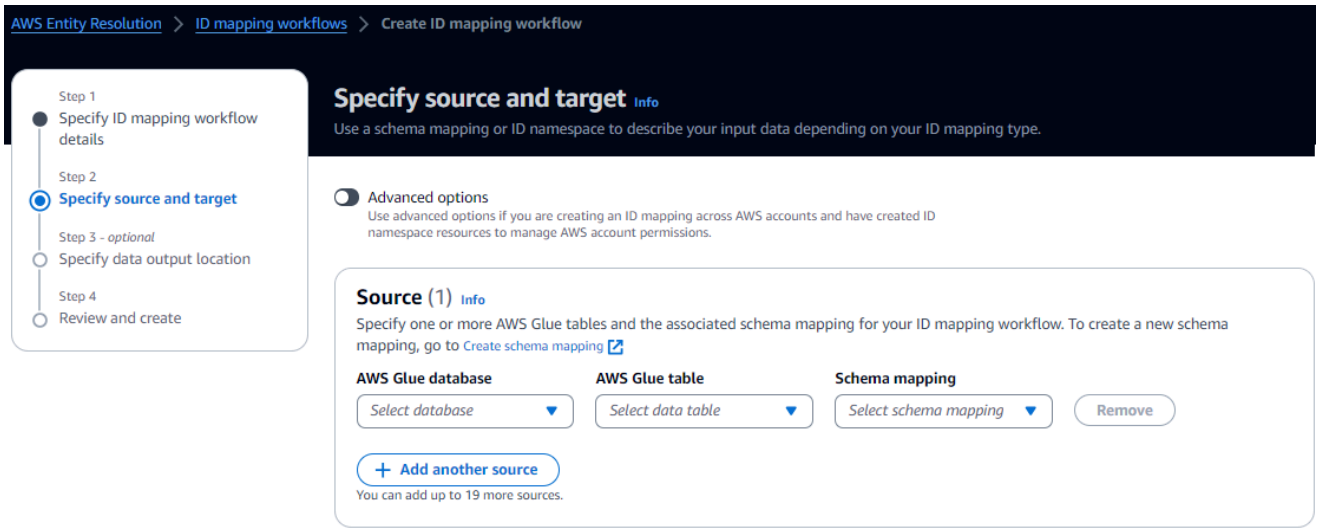
d. (Opcional) Para ativar tags para o recurso, escolha Adicionar nova tag e, em seguida, insira o par de chave e valor.

e. Escolha Próximo.

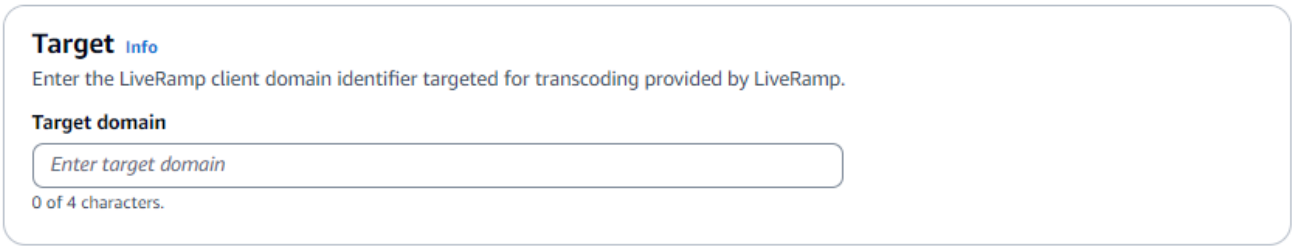
5. Para a Etapa 2: Especificar a origem e o destino, faça o seguinte:

a. Em Origem, selecione um AWS Gluebanco de dados na lista suspensa, selecione a AWS Glue tabela e, em seguida, selecione o mapeamento do esquema correspondente.

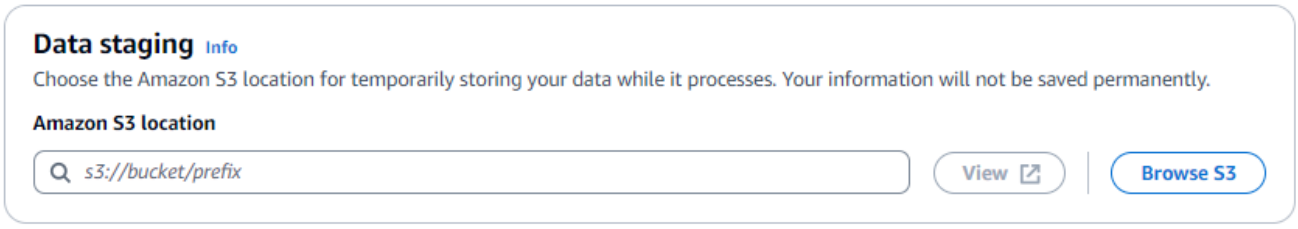
   Você pode adicionar até 19 entradas de dados.



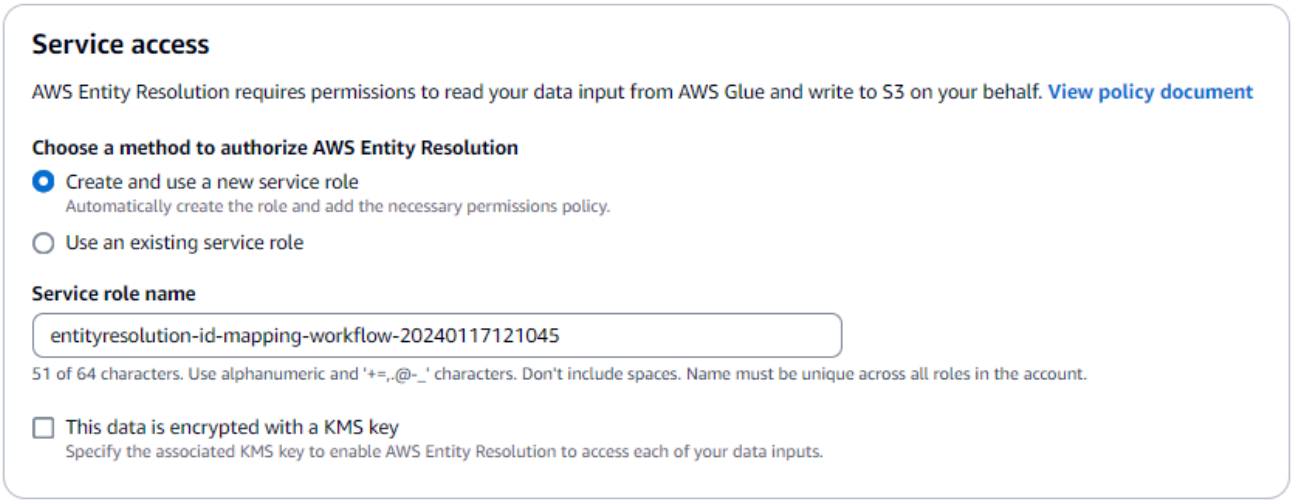
b. Em Target, insira o identificador de domínio LiveRamp do cliente destinado à transcodificação que LiveRamp fornece.



c. Para preparação de dados, escolha o local do Amazon S3 em que você deseja gravar temporariamente a saída do fluxo de trabalho de mapeamento de ID.



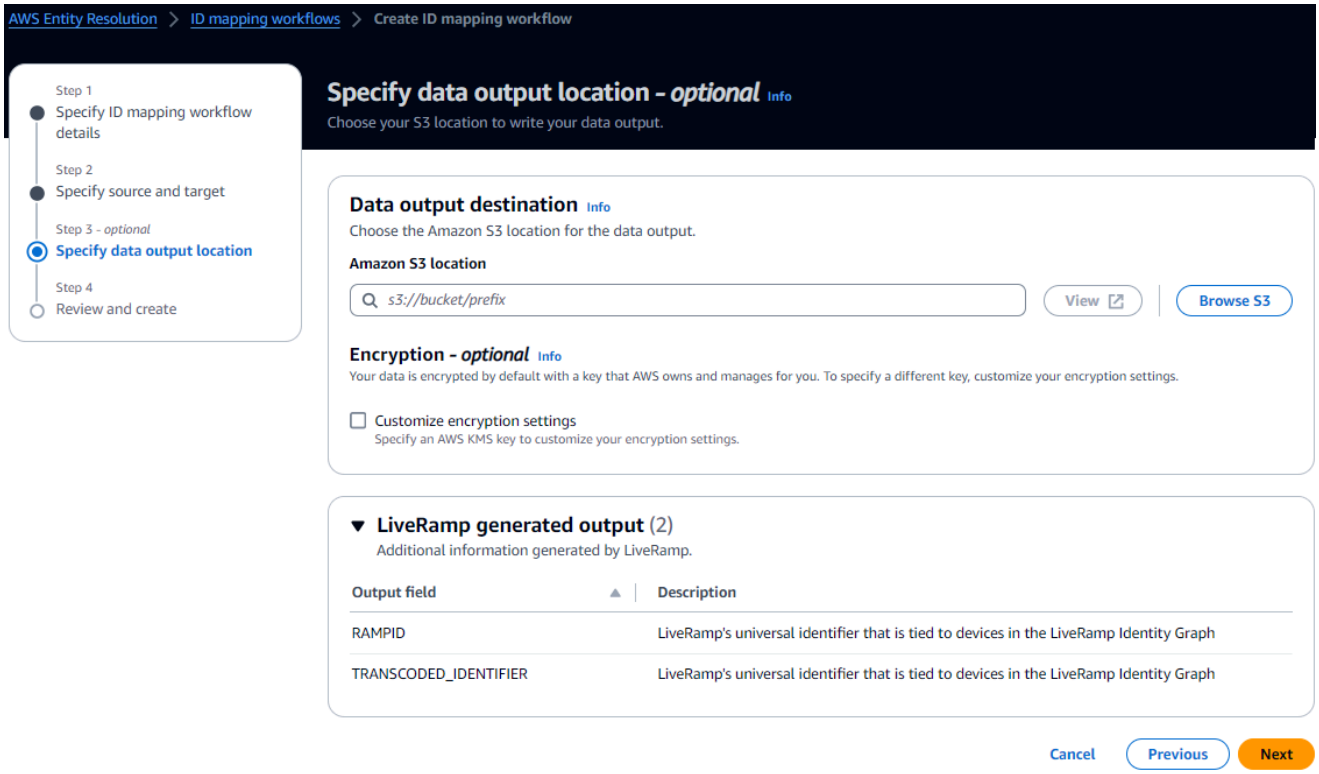
d. Para especificar as permissões de acesso ao serviço, escolha Criar e usar uma nova função de serviço ou Usar uma função de serviço existente.



Se você escolher...	Então
Criar e usar um novo perfil de serviço	AWS Entity Resolution cria uma função de serviço com a política necessária para essa tabela. O nome padrão da função de serviço é `entityresolution-id-mapping-workflow-<timestamp>` . Você deve ter permissões para criar perfis e anexar políticas. Se seus dados de entrada estiverem criptografados, escolha a opção Esses dados são criptografados por uma chave KMS. Em seguida, insira uma AWS KMS chave usada para descriptografar sua entrada de dados.

Se você escolher...	Então
Use um perfil de serviço existente	Escolha um nome do perfil de serviço existente na lista suspensa. Se você tiver permissões para listar funções, a lista de funções será exibida. Se você não tiver permissões para listar funções, poderá inserir o Amazon Resource Name (ARN) da função que deseja usar. Se não houver funções de serviço existentes, a opção Usar uma função de serviço existente não estará disponível. Por padrão, AWS Entity Resolutio n não tenta atualizar a política de função existente para adicionar as permissões necessárias.

6. Escolha Próximo.
7. Para a Etapa 3: Especificar o local de saída de dados — opcional, faça o seguinte:
   a. Para Destino de saída de dados, faça o seguinte:
      i. Escolha a localização do Amazon S3 para a saída de dados.
      ii. Em Criptografia, se você optar por Personalizar as configurações de criptografia, insira o ARN da AWS KMS chave ou escolha Criar uma AWS KMS chave.
   b. Visualize a saída LiveRamp gerada.
   c. Escolha Próximo.



8. Para a Etapa 4: revisar e criar, faça o seguinte:

   a. Revise as seleções feitas nas etapas anteriores e edite-as, se necessário.

   b. Escolha Criar.

      Uma mensagem aparece indicando que o fluxo de trabalho de mapeamento de ID foi criado.

Depois de criar o fluxo de trabalho de mapeamento de ID, você está pronto para executar um fluxo de trabalho de mapeamento de ID

Criação de um fluxo de trabalho de mapeamento de ID em dois Contas da AWS

Pré-requisito

A criação de um fluxo de trabalho de mapeamento de ID entre dois Contas da AWS exige permissão LiveRamp para acessar o bucket do S3 e a chave gerenciada pelo cliente AWS Key Management Service (AWS KMS). Antes de criar um fluxo de trabalho de mapeamento de ID entre dois Contas da

AWS LiveRamp, adicione a seguinte política de permissão, que permite LiveRamp acessar o bucket do S3 e a chave gerenciada pelo 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"
            }
        }
    }]
}
```

Na política de permissões anterior, substitua cada uma <user input placeholder>por suas próprias informações.

<KMSKeyARN>	O ARN de uma chave gerenciada pelo AWS KMS cliente.

Crie um fluxo de trabalho de mapeamento de ID

Antes de criar um fluxo de trabalho de mapeamento de ID entre dois Contas da AWS, você deve primeiro fazer o seguinte:

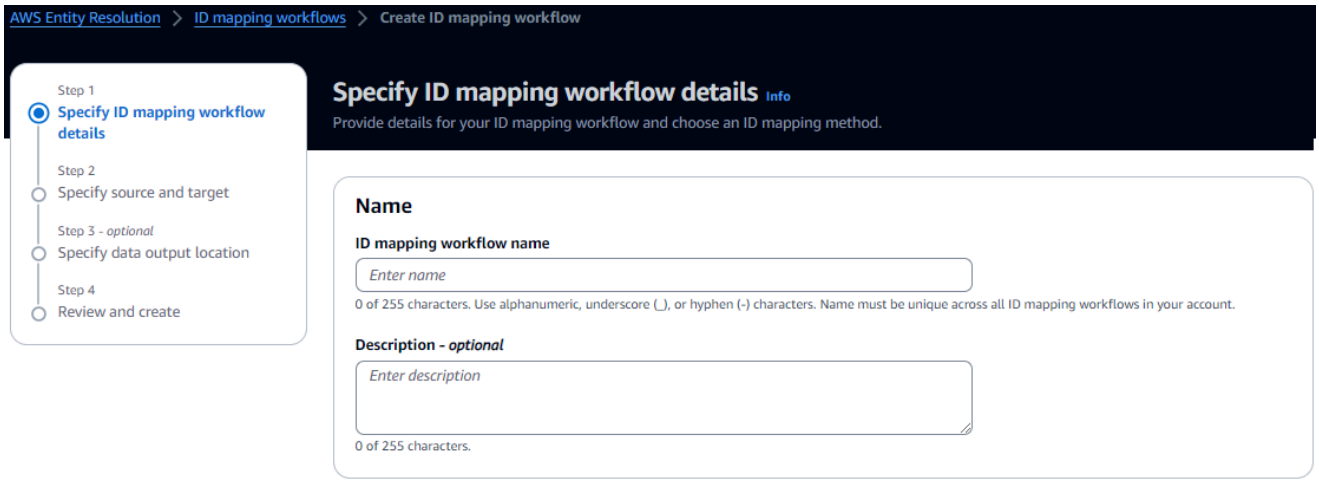
- Preencha o pré-requisito para adicionar as permissões à chave gerenciada pelo cliente.
- Conclua as tarefas em Conf AWS Entity Resolution iguração.
- Crie uma fonte de namespace de ID.
- Crie um destino de namespace de ID.

Depois de concluir as tarefas listadas anteriormente, você pode criar um ou mais fluxos de trabalho de mapeamento de ID para traduzir um conjunto de RAMPIDs de origem para outro usando RAMPIDs mantidos ou derivados.

Para criar um fluxo de trabalho de mapeamento de ID em dois Contas da AWS

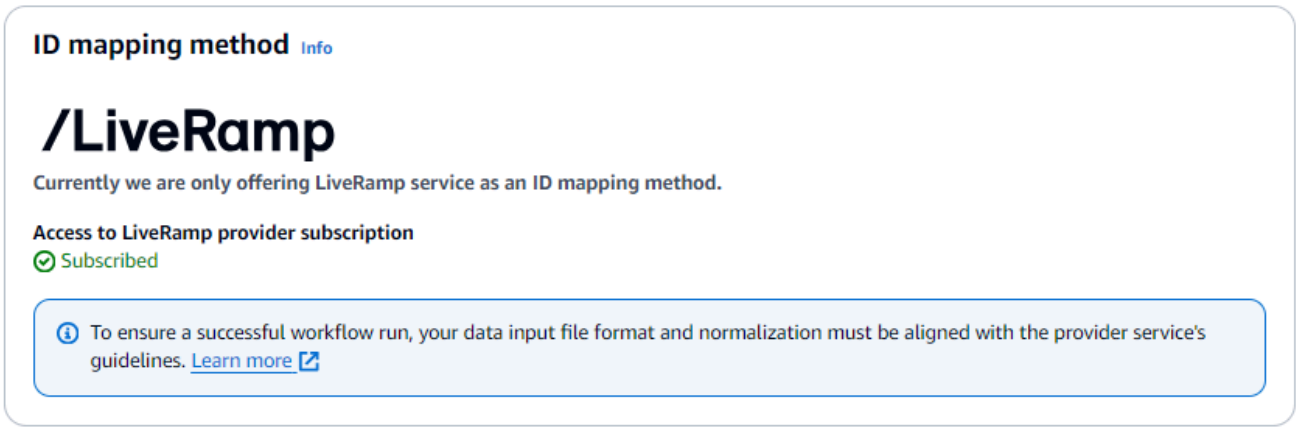
1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Mapeamento de ID.
3. Na página Fluxos de trabalho de mapeamento de ID, no canto superior direito, escolha Criar fluxo de trabalho de mapeamento de ID.
4. Para a Etapa 1: Especificar detalhes do fluxo de trabalho de mapeamento de ID, faça o seguinte:

    a. Insira um nome de fluxo de trabalho de mapeamento de ID e uma Descrição opcional.



    b. Veja o método de mapeamento de ID.

    AWS Entity Resolution atualmente oferece o serviço do LiveRamp provedor como um método de mapeamento de ID. Se você tiver uma assinatura LiveRamp, o status aparecerá como Assinado. Para obter mais informações sobre como assinar LiveRamp, consulteAssine um serviço de provedor em AWS Data Exchange.



> **Note**
>
> Certifique-se de que o formato do arquivo de entrada de dados esteja alinhado com as diretrizes do serviço do provedor. Para obter mais informações sobre as diretrizes de formatação LiveRamp do arquivo de entrada, consulte Executar tradução por meio do ADX no site da LiveRamp documentação.

c. Para LiveRamp configuração, insira os seguintes valores que LiveRamp fornecem:

- Gerenciador de ID de cliente ARN
- Gerenciador secreto do cliente ARN

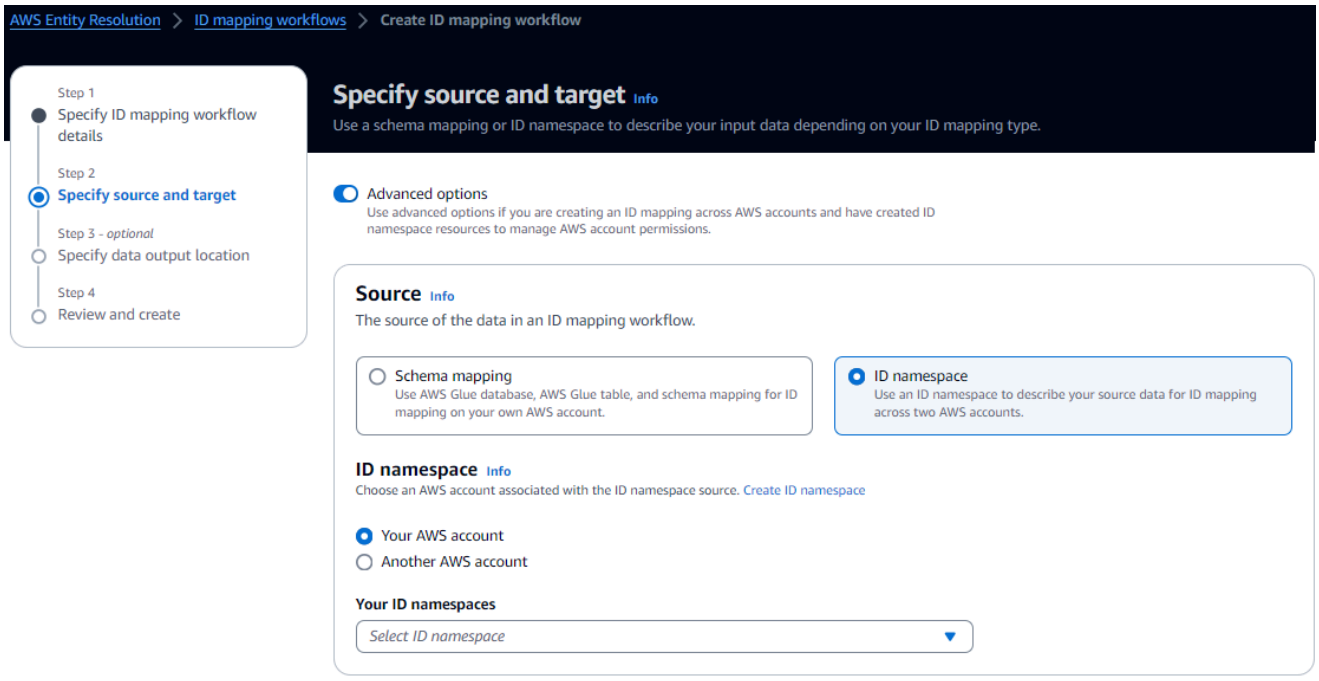
d. (Opcional) Para ativar tags para o recurso, escolha Adicionar nova tag e, em seguida, insira o par de chave e valor.

e. Escolha Próximo.

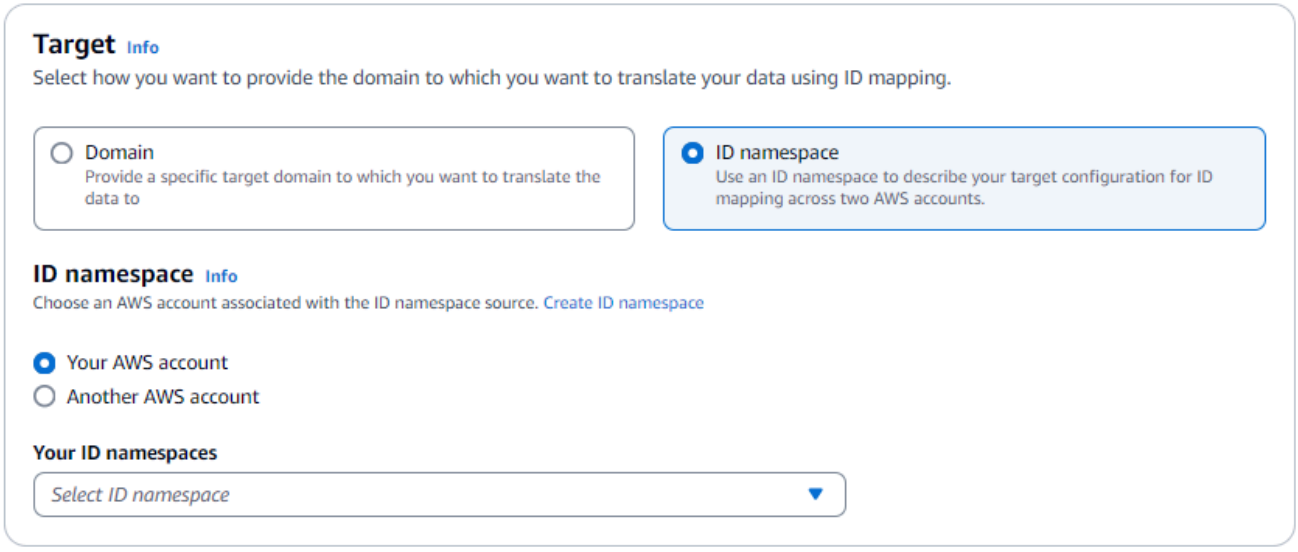
5. Para a Etapa 2: Especificar a origem e o destino, faça o seguinte:

a. Ative as opções avançadas.

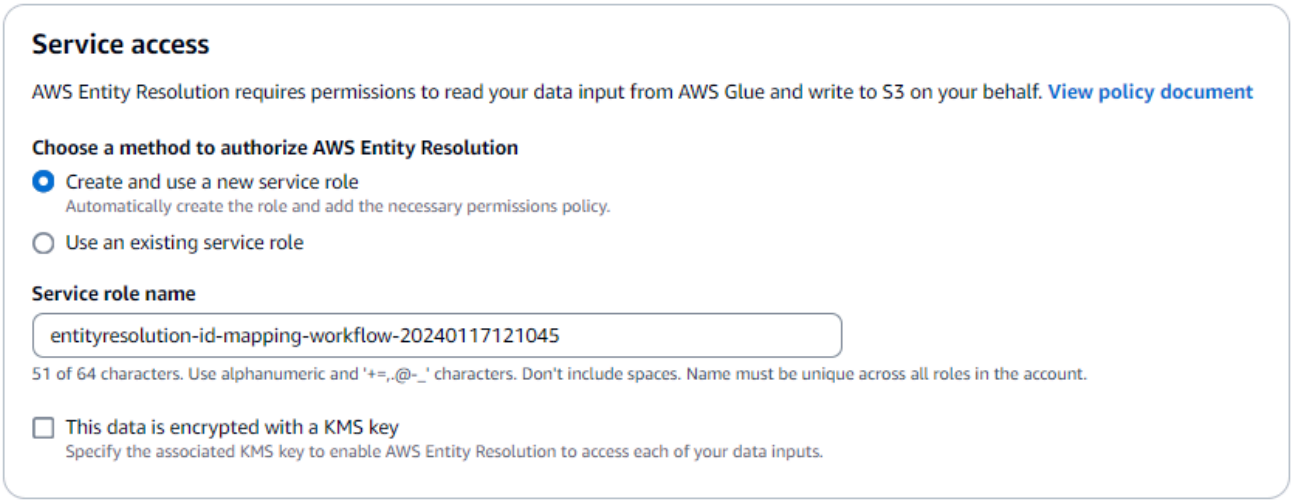
b. Em Source, escolha ID namespace.



c. Em Target, escolha o namespace ID.



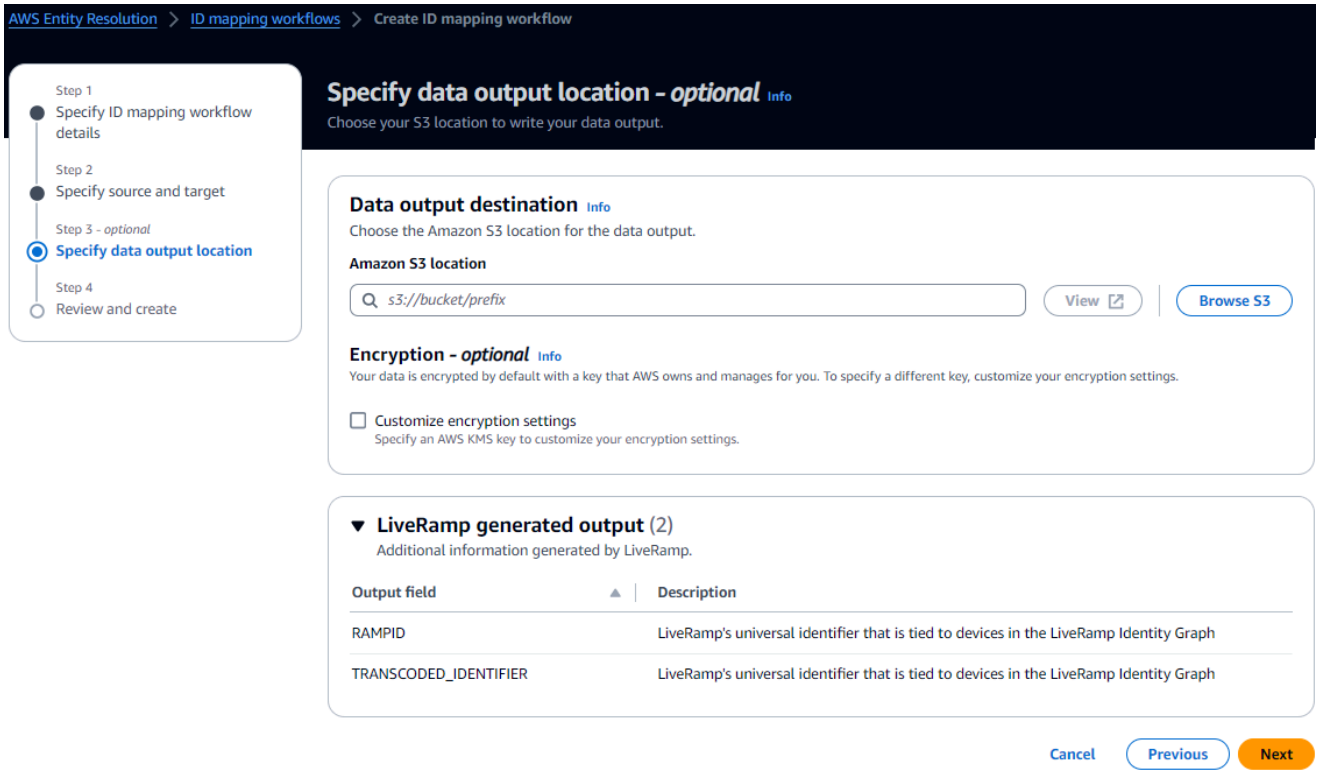
d. Para especificar as permissões de acesso ao serviço, escolha Criar e usar uma nova função de serviço ou Usar uma função de serviço existente.



Se você escolher...	Então
Criar e usar um novo perfil de serviço	AWS Entity Resolution cria uma função de serviço com a política necessária para essa tabela. O nome padrão da função de serviço é `entityresolution-id-mapping-workflow-<timestamp>` . Você deve ter permissões para criar perfis e anexar políticas. Se seus dados de entrada estiverem criptografados, escolha a opção Esses dados são criptografados por uma chave KMS. Em seguida, insira uma AWS KMS chave usada para descriptografar sua entrada de dados.

Se você escolher...	Então
Use um perfil de serviço existente	Escolha um nome do perfil de serviço existente na lista suspensa. Se você tiver permissões para listar funções, a lista de funções será exibida. Se você não tiver permissões para listar funções, poderá inserir o Amazon Resource Name (ARN) da função que deseja usar. Se não houver funções de serviço existentes, a opção Usar uma função de serviço existente não estará disponível. Por padrão, AWS Entity Resolutio n não tenta atualizar a política de função existente para adicionar as permissões necessárias.

6. Escolha Próximo.
7. Para a Etapa 3: Especificar o local de saída de dados — opcional, faça o seguinte:
   a. Para Destino de saída de dados, faça o seguinte:
      i. Escolha a localização do Amazon S3 para a saída de dados.
      ii. Em Criptografia, se você optar por Personalizar as configurações de criptografia, insira o ARN da AWS KMS chave ou escolha Criar uma AWS KMS chave.
   b. Visualize a saída LiveRamp gerada.
   c. Escolha Próximo.



8. Para a Etapa 4: revisar e criar, faça o seguinte:

   a. Revise as seleções feitas nas etapas anteriores e edite-as, se necessário.

   b. Escolha Criar.

      Uma mensagem aparece indicando que o fluxo de trabalho de mapeamento de ID foi criado.

Depois de criar o fluxo de trabalho de mapeamento de ID, você estará pronto para executar um fluxo de trabalho de mapeamento de ID.

Executar um fluxo de trabalho de mapeamento de ID

Depois de criar um fluxo de trabalho de mapeamento de ID para um Conta da AWS ou criar um fluxo de trabalho de mapeamento de ID em dois Contas da AWS, você pode executar o fluxo de trabalho de mapeamento de ID.

Para executar um fluxo de trabalho de mapeamento de ID

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.

2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Mapeamento de ID.
3. Escolha o fluxo de trabalho de mapeamento de ID.
4. Na página de detalhes do fluxo de trabalho de mapeamento de ID, no canto superior direito, escolha Executar.
5. Na página de detalhes do fluxo de trabalho correspondente, na guia Métricas, veja o seguinte em Métricas do último trabalho:

   - O Job ID
   - O tempo concluído para o trabalho de fluxo de trabalho
   - O status da tarefa de fluxo de trabalho correspondente: Em fila, em andamento, concluída, com falha
   - O número de registros processados
   - O número de registros não processados
   - O número de registros de entrada

   Em Histórico de tarefas, você também pode visualizar as métricas de tarefas de fluxo de trabalho de mapeamento de ID executadas anteriormente.
6. Após a conclusão do trabalho do fluxo de trabalho de mapeamento de ID (o status é Concluído), escolha Saída de dados e, em seguida, escolha sua localização no Amazon S3 para visualizar os resultados.

   Depois de obter seu arquivo CSV, você pode unir o. `RAMPID` com o. `TRANSCODED_ID`

Executando um fluxo de trabalho de mapeamento de ID com um novo destino de saída

Depois de criar um fluxo de trabalho de mapeamento de ID para um Conta da AWS ou criar um fluxo de trabalho de mapeamento de ID em dois Contas da AWS, você pode escolher um local diferente do S3 para gravar sua saída de dados.

Para executar um fluxo de trabalho de mapeamento de ID com um novo destino de saída

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Mapeamento de ID.

3. Escolha o fluxo de trabalho de mapeamento de ID.
4. Na página de detalhes do fluxo de trabalho de mapeamento de ID, no canto superior direito, escolha Executar com novo destino de saída na lista suspensa Executar fluxo de trabalho.
5. Para Destino de saída de dados, faça o seguinte:

   a. Escolha a localização do Amazon S3 para a saída de dados.

   b. Em Criptografia, se você optar por Personalizar as configurações de criptografia, insira o ARN da AWS KMS chave ou escolha Criar uma AWS KMS chave.
6. Para especificar as permissões de acesso ao serviço, escolha Criar e usar uma nova função de serviço ou Usar uma função de serviço existente.

Se você escolher...	Então
Criar e usar um novo perfil de serviço	AWS Entity Resolution cria uma função de serviço com a política necessária para essa tabela. O nome padrão da função de serviço é `entityresolution-id-mapping-workflow-<timestamp>` . Você deve ter permissões para criar perfis e anexar políticas. Se seus dados de entrada estiverem criptografados, escolha a opção Esses dados são criptografados por uma chave KMS. Em seguida, insira uma AWS KMS chave usada para descriptografar sua entrada de dados.
Use um perfil de serviço existente	Escolha um nome do perfil de serviço existente na lista suspensa.

Se você escolher...	Então
	Se você tiver permissões para listar funções, a lista de funções será exibida. Se você não tiver permissões para listar funções, poderá inserir o Amazon Resource Name (ARN) da função que deseja usar. Se não houver funções de serviço existentes, a opção Usar uma função de serviço existente não estará disponível. Por padrão, AWS Entity Resolution não tenta atualizar a política de função existente para adicionar as permissões necessárias.

7. Escolha Executar.
8. Na página de detalhes do fluxo de trabalho correspondente, na guia Métricas, veja o seguinte em Métricas do último trabalho:

   - O Job ID
   - O tempo concluído para o trabalho de fluxo de trabalho
   - O status da tarefa de fluxo de trabalho correspondente: Em fila, em andamento, concluída, com falha
   - O número de registros processados
   - O número de registros não processados
   - O número de registros de entrada

   Em Histórico de tarefas, você também pode visualizar as métricas de tarefas de fluxo de trabalho de mapeamento de ID executadas anteriormente.

9. Após a conclusão do trabalho do fluxo de trabalho de mapeamento de ID (o status é Concluído), escolha Saída de dados e, em seguida, escolha sua localização no Amazon S3 para visualizar os resultados.

   Depois de obter seu arquivo CSV, você pode unir o. `RAMPID` com o. `TRANSCODED_ID`

Gerenciando AWS Entity Resolution

Os tópicos a seguir explicam como gerenciar fluxos de trabalho usando o AWS Entity Resolution console.

Para obter informações sobre como gerenciar o AWS Entity Resolution uso dos AWS SDKs, consulte a Referência da AWS Entity Resolution API.

Tópicos

Gerenciando mapeamentos de esquema

Os tópicos a seguir explicam como gerenciar mapeamentos de esquema usando o console. AWS Entity Resolution

Tópicos

Clonar um mapeamento de esquema

Você pode clonar um mapeamento de esquema se quiser usar uma configuração existente para criar um novo mapeamento de esquema.

Para clonar um mapeamento de esquema:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.

2. No painel de navegação esquerdo, em Preparação de dados, escolha Mapeamentos do esquema.
3. Escolha o mapeamento do esquema.
4. Escolha Clonar.
5. Na página Especificar detalhes do esquema, faça as alterações necessárias e escolha Avançar.
6. Na página Escolher técnica de correspondência, faça as alterações necessárias e escolha Avançar.
7. Na página Campos de entrada do mapa, faça as alterações necessárias e escolha Avançar.
8. Na página Dados do grupo, faça as alterações necessárias e escolha Avançar.
9. Na página Revisar e salvar, faça as alterações necessárias e escolha Clonar mapeamento do esquema.

Editar um mapeamento de esquema

Você só pode editar um mapeamento de esquema antes de associá-lo a um fluxo de trabalho. Depois de associar um mapeamento de esquema a um fluxo de trabalho, você não pode editá-lo. Você pode clonar um mapeamento de esquema se quiser usar uma configuração existente para criar um novo mapeamento de esquema.

Para editar um mapeamento de esquema:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Preparação de dados, escolha Mapeamentos do esquema.
3. Escolha o mapeamento do esquema.
4. Selecione a opção Editar.
5. Na página Especificar detalhes do esquema, faça as alterações necessárias e escolha Avançar.
6. Na página Escolher técnica de correspondência, faça as alterações necessárias e escolha Avançar.
7. Na página Campos de entrada do mapa, faça as alterações necessárias e escolha Avançar.
8. Na página Dados do grupo, faça as alterações necessárias e escolha Avançar.
9. Na página Revisar e salvar, faça as alterações necessárias e escolha Editar mapeamento do esquema.

Excluir um mapeamento de esquema

Você não pode excluir um mapeamento de esquema quando ele está associado a um fluxo de trabalho correspondente. Primeiro, você deve remover o mapeamento do esquema de todos os fluxos de trabalho correspondentes associados antes de excluí-lo.

Para excluir um mapeamento de esquema:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Preparação de dados, escolha Mapeamentos do esquema.
3. Escolha o mapeamento do esquema.
4. Escolha Excluir.
5. Confirme a exclusão e escolha Excluir.

Gerenciando fluxos de trabalho correspondentes

Depois de criar um fluxo de trabalho de correspondência baseada em regras, correspondência baseada em aprendizado de máquina ou correspondência baseada em serviços do provedor, você pode gerenciar fluxos de trabalho correspondentes das seguintes maneiras.

Tópicos

- Editar um fluxo de trabalho correspondente
- Excluir um fluxo de trabalho correspondente
- Encontre um ID de correspondência para um fluxo de trabalho de correspondência baseado em regras
- Excluir registros de um fluxo de trabalho de correspondência baseado em regras ou em ML

Editar um fluxo de trabalho correspondente

Para editar um fluxo de trabalho correspondente:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.

2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Escolha o fluxo de trabalho correspondente.
4. Na página de detalhes do fluxo de trabalho correspondente, no canto superior direito, escolha Editar.
5. Na página Especificar detalhes do fluxo de trabalho correspondente, faça as alterações necessárias e escolha Avançar.
6. Na página Escolher técnica de correspondência, faça as alterações necessárias e escolha Avançar.
7. Na página Especificar saída de dados, faça as alterações necessárias e escolha Avançar.
8. Na página Revisar e salvar, faça as alterações necessárias e escolha Salvar.

Excluir um fluxo de trabalho correspondente

Para excluir um fluxo de trabalho correspondente:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Escolha o fluxo de trabalho correspondente.
4. Na página de detalhes do fluxo de trabalho correspondente, no canto superior direito, escolha Excluir.
5. Confirme a exclusão e escolha Excluir.

Encontre um ID de correspondência para um fluxo de trabalho de correspondência baseado em regras

Depois de executar um fluxo de trabalho de correspondência baseado em regras, você pode encontrar a ID de correspondência correspondente e a regra associada aos registros processados.

Para encontrar uma ID de correspondência para um fluxo de trabalho de correspondência baseado em regras:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.

2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Escolha o fluxo de trabalho de correspondência baseado em regras que foi processado (o status do trabalho é Concluído).
4. Na página de detalhes do fluxo de trabalho correspondente, escolha a guia Localizar ID de correspondência.
5. Execute um destes procedimentos:

Se...	Então…
Há somente um mapeamento de esquema associado a esse fluxo de trabalho.	Visualize o mapeamento do esquema selecionado por padrão.
Há mais de um mapeamento de esquema associado a esse fluxo de trabalho.	Escolha o mapeamento do esquema na lista suspensa.

6. Expanda as regras de correspondência.
7. Insira um valor para cada chave de correspondência.

   A opção Normalizar dados é selecionada por padrão, para que as entradas de dados sejam normalizadas antes da correspondência. Se você não quiser normalizar dados, desmarque a opção Normalizar dados.

   > **Tip**
   >
   > Insira o máximo de valores possível para ajudar a encontrar o Match ID.

8. Escolha Look up.
9. Veja o ID de correspondência correspondente e a regra associada que foi usada para correspondência.

Excluir registros de um fluxo de trabalho de correspondência baseado em regras ou em ML

Se precisar estar em conformidade com os regulamentos de gerenciamento de dados, você pode excluir os registros de um fluxo de trabalho de correspondência baseado em regras ou baseado em ML.

Para excluir registros de um fluxo de trabalho de correspondência baseado em regras ou em ML

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Correspondência.
3. Escolha o fluxo de trabalho de correspondência baseado em regras ou em ML.
4. Na página de detalhes do fluxo de trabalho correspondente, escolha Excluir IDs exclusivos na lista suspensa Ações.
5. Insira o ID exclusivo que você deseja excluir na seção IDs exclusivos.

   Você pode inserir até 10 IDs exclusivos.
6. Especifique a fonte de entrada da qual excluir os IDs exclusivos.

   Se houver somente uma fonte de entrada para o fluxo de trabalho, a fonte de entrada será listada por padrão.

   Se você especificar apenas uma fonte de entrada, os IDs exclusivos em outras fontes de entrada não serão afetados.
7. Escolha Excluir IDs exclusivos.

Gerenciando namespaces de ID

Você pode gerenciar namespaces de ID das seguintes maneiras.

Tópicos

- Editar um namespace de ID
- Excluir um namespace de ID
- Adicionar ou atualizar uma política de recursos

Editar um namespace de ID

Você só pode editar um namespace de ID antes de associá-lo a um fluxo de trabalho de mapeamento de ID. Depois de associar um namespace de ID a um fluxo de trabalho de mapeamento de ID, você não pode editá-lo.

Para editar um namespace de ID:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, em Preparação de dados, escolha Namespaces de ID.
3. Escolha o namespace de ID.
4. Selecione a opção Editar.
5. Na página Editar namespace ID, faça as alterações necessárias e escolha Salvar.

Excluir um namespace de ID

Você não pode excluir um namespace de ID quando ele está associado a um fluxo de trabalho de mapeamento de ID. Primeiro, você deve remover o mapeamento de esquema de todos os fluxos de trabalho associados a um mapeamento de ID antes de excluí-lo.

Para excluir um namespace de ID:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, em Preparação de dados, escolha Namespaces de ID.
3. Escolha o namespace de ID.
4. Escolha Excluir.
5. Confirme a exclusão e escolha Excluir.

Adicionar ou atualizar uma política de recursos

Uma política de recursos permite que o criador do recurso de mapeamento de ID acesse seu recurso de namespace de ID.

Para adicionar ou atualizar uma política de recursos

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha namespaces de ID.
3. Escolha o namespace de ID.
4. Na página de detalhes do namespace ID, escolha a guia Permissões.

5. Na seção Política de recursos, escolha Editar.
6. Adicione ou atualize a política no editor JSON.
7. Escolha Salvar alterações.

Gerenciando fluxos de trabalho de mapeamento de ID

Você pode gerenciar fluxos de trabalho de mapeamento de ID das seguintes maneiras.

Tópicos

Editar um fluxo de trabalho de mapeamento de ID

Para editar um fluxo de trabalho de mapeamento de ID:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Mapeamento de ID.
3. Escolha o fluxo de trabalho de mapeamento de ID.
4. Na página de detalhes do fluxo de trabalho de mapeamento de ID, no canto superior direito, escolha Editar.
5. Na página Especificar detalhes do fluxo de trabalho de mapeamento de ID, faça as alterações necessárias e escolha Avançar.
6. Na página Especificar saída de dados, faça as alterações necessárias e escolha Avançar.
7. Na página Revisar e salvar, faça as alterações necessárias e escolha Salvar.

Excluir um fluxo de trabalho de mapeamento de ID

Para excluir um fluxo de trabalho de mapeamento de ID:

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.

2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Mapeamento de ID.
3. Escolha o fluxo de trabalho de mapeamento de ID.
4. Na página de detalhes do fluxo de trabalho de mapeamento de ID, no canto superior direito, escolha Excluir.
5. Confirme a exclusão e escolha Excluir.

Adicionar ou atualizar uma política de recursos

Uma política de recursos permite que o criador do recurso de mapeamento de ID acesse seu recurso de namespace de ID.

Para adicionar ou atualizar uma política de recursos

1. Faça login no AWS Management Console e abra o AWS Entity Resolution console com o seu Conta da AWS, caso ainda não tenha feito isso.
2. No painel de navegação esquerdo, em Fluxos de trabalho, escolha Mapeamento de ID.
3. Escolha o fluxo de trabalho de mapeamento de ID.
4. Na página de detalhes do fluxo de trabalho de mapeamento de ID, escolha a guia Permissões.
5. Na seção Política de recursos, escolha Editar.
6. Adicione ou atualize a política no editor JSON.
7. Escolha Salvar alterações.

Solução de problemas de fluxos de trabalho

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao executar fluxos de trabalho.

Eu recebi um arquivo de erro.

Os registros no arquivo de erro podem ser criados pelos seguintes motivos:

- O ID exclusivo é:
  - nulo
  - ausente em uma linha de dados
  - ausente em um registro na tabela de dados

  - repetido em outra linha de dados na tabela de dados
  - não especificado
  - não é exclusivo na mesma fonte
  - não é exclusivo em várias fontes
  - sobrepõe-se a todas as fontes
- Um dos campos no mapeamento do esquema inclui um nome reservado:
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - ID da partida
  - HashingProtocol
  - ConfidenceLevel
  - Origem

Se o registro no arquivo de erro for criado devido aos motivos listados anteriormente, você será cobrado, pois isso incorrerá no custo de processamento do serviço. Se o registro no arquivo de erro for causado por um erro interno do servidor, você não será cobrado.

Segurança em AWS Entity Resolution

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de datacenters e arquiteturas de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa os Serviços da AWS na Nuvem AWS. A AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Entity Resolution, consulte Serviços da AWS em escopo por programa de conformidade
- Segurança na nuvem: sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o AWS Entity Resolution. Os tópicos a seguir mostram como configurar o AWS Entity Resolution para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros Serviços da AWS que ajudam você a monitorar e proteger os recursos do AWS Entity Resolution.

Tópicos

Proteção de dados em AWS Entity Resolution

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Entity Resolution. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle

sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a AWS postagem do blog Shared Responsibility Model and GDPR no AWS Blog de segurança da.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com AWS Entity Resolution ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia de dados em repouso para AWS Entity Resolution

AWS Entity Resolution fornece criptografia por padrão para proteger dados confidenciais do cliente em repouso usando chaves AWS de criptografia próprias.

Chaves de propriedade da AWS — AWS Entity Resolution usa essas chaves por padrão para criptografar automaticamente dados de identificação pessoal. Você não pode visualizar, gerenciar ou usar chaves de propriedade da AWS , tampouco auditar seu uso. No entanto, você não precisa realizar nenhuma ação para proteger as chaves que criptografam seus dados. Para obter mais informações, consulte AWS owned keys no Guia do desenvolvedor do AWS Key Management Service .

A criptografia de dados em repouso por padrão ajuda a reduzir a sobrecarga operacional e a complexidade envolvidas na proteção de dados confidenciais. Ao mesmo tempo, você pode usá-lo para criar aplicativos seguros que atendam aos rigorosos requisitos regulamentares e de conformidade de criptografia.

Como alternativa, você também pode fornecer uma chave KMS gerenciada pelo cliente para criptografia ao criar seu recurso de fluxo de trabalho correspondente.

Chaves gerenciadas pelo cliente — AWS Entity Resolution suporta o uso de uma chave KMS simétrica gerenciada pelo cliente que você cria, possui e gerencia para permitir a criptografia de seus dados confidenciais. Como você tem controle total dessa camada de criptografia, você pode realizar tarefas como:

- Estabelecer e manter as políticas de chave
- Estabelecer e manter subsídios e políticas do IAM
- Habilitar e desabilitar políticas de chaves
- Alternar os materiais de criptografia de chaves
- Adicionar etiquetas
- Criar aliases de chaves
- Programar a exclusão de chaves

Para obter mais informações, consulte a chave gerenciada pelo cliente no Guia do AWS Key Management Service desenvolvedor.

Para obter mais informações sobre AWS KMS, consulte O que é o AWS Key Management Service?

Gerenciamento de chaves

Como AWS Entity Resolution usa subsídios em AWS KMS

AWS Entity Resolution exige uma concessão para usar sua chave gerenciada pelo cliente. Quando você cria um fluxo de trabalho correspondente criptografado com uma chave gerenciada pelo cliente, AWS Entity Resolution cria uma concessão em seu nome enviando uma CreateGrantsolicitação para AWS KMS. As concessões AWS KMS são usadas para dar AWS Entity Resolution acesso a uma chave KMS em uma conta de cliente. AWS Entity Resolution exige que a concessão use sua chave gerenciada pelo cliente para as seguintes operações internas:

- Envie GenerateDataKeysolicitações AWS KMS para gerar chaves de dados criptografadas pela chave gerenciada pelo cliente.
- Envie solicitações de descriptografia para AWS KMS descriptografar as chaves de dados criptografadas para que elas possam ser usadas para criptografar seus dados.

É possível revogar o acesso à concessão, ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, AWS Entity Resolution não conseguirá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afeta as operações que dependem desses dados. Por exemplo, se você remover o acesso ao serviço à sua chave por meio da concessão e tentar iniciar um trabalho para um fluxo de trabalho correspondente criptografado com uma chave de cliente, a operação retornará um `AccessDeniedException` erro.

Criar uma chave gerenciada pelo cliente

Você pode criar uma chave simétrica gerenciada pelo cliente usando o AWS Management Console, ou as AWS KMS APIs.

Para criar uma chave simétrica gerenciada pelo cliente

AWS Entity Resolution suporta criptografia usando chaves KMS de criptografia simétrica. Siga as etapas para criar uma chave simétrica gerenciada pelo cliente no Guia do desenvolvedor AWS Key Management Service .

Declaração de política chave

As políticas de chaves controlam o acesso à chave gerenciada pelo cliente. Cada chave gerenciada pelo cliente deve ter exatamente uma política de chaves, que contém declarações que determinam quem pode usar a chave e como pode usá-la. Ao criar a chave gerenciada pelo cliente, você pode

especificar uma política de chaves. Para obter mais informações, consulte Gerenciamento do acesso às chaves gerenciadas pelo cliente no Guia do AWS Key Management Service desenvolvedor.

Para usar sua chave gerenciada pelo cliente com seus AWS Entity Resolution recursos, as seguintes operações de API devem ser permitidas na política de chaves:

- `kms:DescribeKey`— fornece informações como o ARN da chave, a data de criação (e a data de exclusão, se aplicável), o estado da chave e a data de origem e expiração (se houver) do material da chave. Ele inclui campos, como`KeySpec`, que ajudam você a distinguir diferentes tipos de chaves KMS. Ele também exibe o uso da chave (criptografia, assinatura ou geração e verificação de MACs) e os algoritmos que a chave KMS suporta. AWS Entity Resolution valida que `KeySpec` é `SYMMETRIC_DEFAULT` e `KeyUsage` é`ENCRYPT_DECRYPT`.
- `kms:CreateGrant`: adiciona uma concessão a uma chave gerenciada pelo cliente. Concede acesso de controle a uma chave KMS especificada, o que permite o acesso AWS Entity Resolution necessário às operações de concessão. Para obter mais informações, consulte Usar concessões no Guia do desenvolvedor do AWS Key Management Service .

Isso permite AWS Entity Resolution fazer o seguinte:

- Ligar para `GenerateDataKey` para gerar uma chave de dados criptografada e armazená-la, porque a chave de dados não é usada imediatamente para criptografar.
- Ligue `Decrypt` para usar a chave de dados criptografada armazenada para acessar os dados criptografados.
- Configure uma entidade principal aposentada para permitir que o serviço para `RetireGrant`.

Veja a seguir exemplos de declarações de política que você pode adicionar 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"
        }
      }
}
```

Permissões para usuários

Quando você configura uma chave KMS como a chave padrão para criptografia, a política de chave KMS padrão permite que qualquer usuário com acesso às ações necessárias do KMS use essa chave KMS para criptografar ou descriptografar recursos. Você deve conceder permissão aos usuários para executar as seguintes ações para usar a criptografia de chave KMS gerenciada pelo cliente:

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

Durante uma `CreateMatchingWorkflow`solicitação, AWS Entity Resolution enviará uma DescribeKeye uma CreateGrantsolicitação para AWS KMS em seu nome. Isso exigirá que a entidade do IAM que faz a `CreateMatchingWorkflow` solicitação com uma chave KMS gerenciada pelo cliente tenha as `kms:DescribeKey` permissões na política de chaves do KMS.

Durante uma `StartIdMappingJob`solicitação `CreateIdMappingWorkflow`e, AWS Entity Resolution enviará uma CreateGrantsolicitação DescribeKeye uma para AWS KMS em seu nome. Isso exigirá que a entidade do IAM que faz a `StartIdMappingJob` solicitação `CreateIdMappingWorkflow` e com uma chave KMS gerenciada pelo cliente tenha as `kms:DescribeKey` permissões na política de chaves do KMS. Os provedores poderão acessar a chave gerenciada pelo cliente para descriptografar os dados no bucket do Amazon S3 AWS Entity Resolution .

A seguir estão exemplos de declarações de política que você pode adicionar para que os provedores descriptografem os dados no bucket do Amazon S3: AWS Entity Resolution

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

Substitua cada um <user input placeholder>por suas próprias informações.

<KMSKeyARN>	AWS KMS Nome do recurso da Amazon.

Da mesma forma, a entidade do IAM que invoca a `StartMatchingJobAPI` não deve ter `kms:Decrypt` nenhuma `kms:GenerateDataKey` permissão na chave KMS gerenciada pelo cliente fornecida no fluxo de trabalho correspondente.

Para obter mais informações sobre a especificação de permissões em uma política, consulte o Guia do AWS Key Management Service desenvolvedor.

Para obter mais informações sobre como solucionar problemas de acesso por chave, consulte o Guia do AWS Key Management Service desenvolvedor.

Especificando uma chave gerenciada pelo cliente para AWS Entity Resolution

Você pode especificar uma chave gerenciada pelo cliente para fornecer uma segunda camada de criptografia para os seguintes recursos:

Fluxo de trabalho correspondente — Ao criar um recurso de fluxo de trabalho correspondente, você pode especificar a chave de dados inserindo um KMSarn, que é AWS Entity Resolution usado para criptografar os dados pessoais identificáveis armazenados pelo recurso.

KMSArn — Insira um ARN de chave, que é um identificador de chave para uma chave gerenciada pelo cliente. AWS KMS

Você pode especificar uma chave gerenciada pelo cliente como uma criptografia de segunda camada para os seguintes recursos se estiver criando ou executando um fluxo de trabalho de mapeamento de ID em dois Contas da AWS:

Fluxo de trabalho de mapeamento de ID ou Iniciar fluxo de trabalho de mapeamento de ID — Ao criar um recurso de fluxo de trabalho de mapeamento de ID ou iniciar um trabalho de fluxo de trabalho de mapeamento de ID, você pode especificar a chave de dados inserindo um KMSARN, que AWS Entity Resolution usa para criptografar os dados pessoais identificáveis armazenados pelo recurso.

KMSArn — Insira um ARN de chave, que é um identificador de chave para uma chave gerenciada pelo cliente. AWS KMS

Monitorando suas chaves de criptografia para o AWS Entity Resolution serviço

Ao usar uma chave gerenciada pelo AWS KMS cliente com seus recursos AWS Entity Resolution de serviço, você pode usar a AWS CloudTrail ou a Amazon CloudWatch Logs para rastrear solicitações AWS Entity Resolution enviadas para AWS KMS.

Os exemplos a seguir são AWS CloudTrail eventos para`CreateGrant`, `GenerateDataKeyDecrypt`, e `DescribeKey` para monitorar AWS KMS operações chamadas por AWS Entity Resolution para acessar dados criptografados pela chave gerenciada pelo cliente:

Tópicos

- CreateGrant
- DescribeKey
- GenerateDataKey
- Decrypt

CreateGrant

Quando você usa uma chave gerenciada pelo AWS KMS cliente para criptografar seu recurso de fluxo de trabalho correspondente, AWS Entity Resolution envia uma `CreateGrant` solicitação em seu nome para acessar a chave KMS no seu. Conta da AWS A concessão AWS Entity Resolution criada é específica para o recurso associado à chave gerenciada pelo AWS KMS cliente. Além disso, AWS Entity Resolution usa a `RetireGrant` operação para remover uma concessão quando você exclui um recurso.

O evento de exemplo a seguir registra a operação `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 usa a `DescribeKey` operação para verificar se a chave gerenciada pelo AWS KMS cliente associada ao seu recurso correspondente existe na conta e na região.

O evento de exemplo a seguir registra a `DescribeKey` operação.

```
{
    "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

Quando você habilita uma chave gerenciada pelo AWS KMS cliente para seu recurso de fluxo de trabalho correspondente, AWS Entity Resolution envia uma `GenerateDataKey` solicitação por meio do Amazon Simple Storage Service (Amazon S3) AWS KMS para especificar a chave gerenciada AWS KMS pelo cliente para o recurso.

O evento de exemplo a seguir registra a `GenerateDataKey` operação.

```
{
    "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

Quando você habilita uma chave gerenciada pelo AWS KMS cliente para seu recurso de fluxo de trabalho correspondente, AWS Entity Resolution envia uma `Decrypt` solicitação por meio do

Amazon Simple Storage Service (Amazon S3) AWS KMS para especificar a chave gerenciada AWS KMS pelo cliente para o recurso.

O evento de exemplo a seguir registra a `Decrypt` operação.


```
{
    "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"
}
```

Considerações

AWS Entity Resolution não oferece suporte à atualização de um fluxo de trabalho correspondente com uma nova chave KMS gerenciada pelo cliente. Nesses casos, você pode criar um novo fluxo de trabalho com a chave KMS gerenciada pelo cliente.

Saiba mais

Os recursos a seguir fornecem mais informações sobre a criptografia de dados em repouso.

Para obter mais informações sobre os conceitos básicos do AWS Key Management Service, consulte o Guia do AWS Key Management Service desenvolvedor.

Para obter mais informações sobre as melhores práticas de segurança do AWS Key Management Service, consulte o Guia do AWS Key Management Service desenvolvedor.

Acesso AWS Entity Resolution usando um endpoint de interface ()AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre sua VPC e. AWS Entity Resolution Você pode acessar AWS Entity Resolution como se estivesse em sua VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias na sua VPC não precisam de endereços IP públicos para acessar o AWS Entity Resolution.

Você estabelece essa conectividade privada criando um endpoint de interface, desenvolvido pelo AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Estas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao AWS Entity Resolution.

Para obter mais informações, consulte Acesso Serviços da AWS por meio AWS PrivateLink do AWS PrivateLink Guia.

Considerações para AWS Entity Resolution

Antes de configurar um endpoint de interface para AWS Entity Resolution, consulte Considerações no AWS PrivateLink Guia.

AWS Entity Resolution suporta fazer chamadas para todas as suas ações de API por meio do endpoint da interface.

Não há suporte para políticas de endpoint de VPC. AWS Entity Resolution Por padrão, o acesso total a AWS Entity Resolution é permitido por meio do endpoint da interface. Como alternativa, você pode associar um grupo de segurança às interfaces de rede do endpoint para controlar o tráfego a AWS Entity Resolution por meio do endpoint da interface.

Crie um endpoint de interface para AWS Entity Resolution

Você pode criar um endpoint de interface para AWS Entity Resolution usar o console Amazon VPC ou AWS Command Line Interface o AWS CLI(). Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink .

Crie um endpoint de interface para AWS Entity Resolution usar o seguinte nome de serviço:

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

Se você habilitar o DNS privado para o endpoint da interface, poderá fazer solicitações de API a AWS Entity Resolution usando seu nome DNS regional padrão. Por exemplo, `entityresolution.us-east-1.amazonaws.com`.

Criar uma política de endpoint para o endpoint da interface

Política de endpoint é um recurso do IAM que você pode anexar ao endpoint de interface. A política de endpoint padrão permite acesso total AWS Entity Resolution por meio do endpoint da interface. Para controlar o acesso AWS Entity Resolution permitido pela sua VPC, anexe uma política de endpoint personalizada ao endpoint da interface.

Uma política de endpoint especifica as seguintes informações:

- As entidades principais que podem realizar ações (Contas da AWS, usuários do IAM e perfis do IAM).
- As ações que podem ser executadas.
- Os recursos nos quais as ações podem ser executadas.

Para obter mais informações, consulte Controlar o Acesso a Serviços Usando Políticas de Endpoint no AWS PrivateLink Guia.

Exemplo: política de VPC endpoint para ações AWS Entity Resolution

O exemplo a seguir refere-se a uma política de endpoint personalizada. Quando você anexa essa política ao seu endpoint de interface, ela concede acesso às AWS Entity Resolution ações listadas para todos os diretores em todos os recursos.

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

Gerenciamento de identidade e acesso para AWS Entity Resolution

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Entity Resolution os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

> **Note**
>
> AWS Entity Resolution suporta políticas de várias contas. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Tópicos

- Público
- Autenticando com identidades
- Gerenciando acesso usando políticas
- Como AWS Entity Resolution funciona com o IAM

- Exemplos de políticas baseadas em identidade para o AWS Entity Resolution
- AWS políticas gerenciadas para AWS Entity Resolution
- Solução de problemas AWS Entity Resolution de identidade e acesso

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS Entity Resolution.

Usuário do serviço — Se você usar o AWS Entity Resolution serviço para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS Entity Resolution recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no AWS Entity Resolution, consulte Solução de problemas AWS Entity Resolution de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS Entity Resolution recursos da sua empresa, provavelmente tem acesso total AWS Entity Resolution a. É seu trabalho determinar quais AWS Entity Resolution recursos e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS Entity Resolution, consulteComo AWS Entity Resolution funciona com o IAM.

Administrador do IAM: Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar acesso ao AWS Entity Resolution. Para ver exemplos de políticas AWS Entity Resolution baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para o AWS Entity Resolution

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos

de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Utilizar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade.

Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte "O que é o Centro de Identidade do IAM?" no Guia do usuário AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de

serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) no Guia do usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do Usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS Entity Resolution funciona com o IAM

Antes de usar o IAM para gerenciar o acesso AWS Entity Resolution, saiba com quais recursos do IAM estão disponíveis para uso AWS Entity Resolution.

Recursos do IAM que você pode usar com AWS Entity Resolution

Atributo do IAM	AWS Entity Resolution apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Sim
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Perfis vinculados ao serviço	Não

Para ter uma visão de alto nível de como AWS Entity Resolution e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para AWS Entity Resolution

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para AWS Entity Resolution

Para ver exemplos de políticas AWS Entity Resolution baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS Entity Resolution

Políticas baseadas em recursos dentro AWS Entity Resolution

É compatível com políticas baseadas em atributos	Sim

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para

o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para AWS Entity Resolution

Oferece compatibilidade com ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de AWS Entity Resolution ações, consulte Ações definidas por AWS Entity Resolution na Referência de autorização de serviço.

As ações de política AWS Entity Resolution usam o seguinte prefixo antes da ação:

```
entityresolution
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

Para ver exemplos de políticas AWS Entity Resolution baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS Entity Resolution

Recursos políticos para AWS Entity Resolution

Oferece compatibilidade com recursos de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de AWS Entity Resolution recursos e seus ARNs, consulte Recursos definidos por AWS Entity Resolution na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo AWS Entity Resolution.

Para ver exemplos de políticas AWS Entity Resolution baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS Entity Resolution

Chaves de condição de política para AWS Entity Resolution

Suporta chaves de condição de política específicas de serviço	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de AWS Entity Resolution condição, consulte Chaves de condição AWS Entity Resolution na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Entity Resolution.

Para ver exemplos de políticas AWS Entity Resolution baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS Entity Resolution

ACLs em AWS Entity Resolution

Oferece compatibilidade com ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS Entity Resolution

Oferece compatibilidade com ABAC (tags em políticas)	Parcial

O controle de acesso baseado em recurso (ABAC) é uma estratégia de autorização que define permissões com base em recursos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS Entity Resolution

Oferece compatibilidade com credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para AWS Entity Resolution

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.

Funções de serviço para AWS Entity Resolution

Oferece compatibilidade com funções de serviço	Sim

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper AWS Entity Resolution a funcionalidade. Edite as funções de serviço somente quando AWS Entity Resolution fornecer orientação para fazer isso.

Funções vinculadas a serviços para AWS Entity Resolution

Oferece suporte a perfis vinculados ao serviço	Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço .

Exemplos de políticas baseadas em identidade para o AWS Entity Resolution

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS Entity Resolution . Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por AWS Entity Resolution, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição AWS Entity Resolution na Referência de autorização de serviço.

Tópicos

- Melhores práticas de política
- Usar o console do AWS Entity Resolution
- Permitir que usuários visualizem suas próprias permissões

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS Entity Resolution recursos em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do Usuário do IAM.
- Aplique permissões de privilégio mínimo –- ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as

ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do Usuário do IAM.

- Use condições nas políticas do IAM para restringir ainda mais o acesso –- você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: Condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Usar o console do AWS Entity Resolution

Para acessar o AWS Entity Resolution console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS Entity Resolution recursos em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o AWS Entity Resolution console, anexe também a política AWS Entity Resolution *ConsoleAccess* ou a política *ReadOnly* AWS gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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 gerenciadas para AWS Entity Resolution

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

AWS política gerenciada: AWSEntityResolutionConsoleFullAccess

É possível anexar a política `AWSEntityResolutionConsoleFullAccess` a suas identidades do IAM.

Essa política concede acesso total aos AWS Entity Resolution endpoints e recursos.

Essa política também permite determinado acesso de leitura a informações relacionadas, Serviços da AWS como S3 AWS Glue, Marcação, AWS KMS para que o console possa exibir opções e usar as selecionadas para realizar ações de resolução de entidades. Alguns recursos são reduzidos para conter o nome `entityresolution` do serviço.

Como AWS Entity Resolution depende de uma função passada para realizar ações em AWS recursos relacionados, essa política também concede as permissões para selecionar e transmitir a função desejada.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `EntityResolutionAccess`— Permite que os diretores tenham acesso total aos AWS Entity Resolution endpoints e recursos.
- `GlueSourcesConsoleDisplay`— Concede acesso às AWS Glue tabelas de listagem como opções de fonte de dados e ao esquema de importação da tabela de uma fonte de dados para a experiência do usuário.
- `S3BucketsConsoleDisplay`— Concede acesso para listar todos os buckets do S3 como opções de fonte de dados.
- `S3SourcesConsoleDisplay`— Concede acesso para exibir buckets do S3 como opções de fonte de dados.
- `TaggingConsoleDisplay`— Concede acesso à leitura de chaves e valores de marcação.
- `KMSConsoleDisplay`— Concede acesso para descrever chaves e listar aliases para AWS Key Management Service descriptografar e criptografar fontes de dados.
- `ListRolesToPickForPassing`— Concede acesso para listar todas as funções para que o usuário possa escolher a função a ser passada.
- `PassRoleToEntityResolutionService`— Concede acesso para passar uma função restrita ao AWS Entity Resolution serviço.
- `ManageEventBridgeRules`— Concede acesso para criar, atualizar e excluir a EventBridge regra da Amazon para receber notificações do S3.
- `ADXReadAccess`— Concede acesso AWS Data Exchange para verificar se o cliente tem um direito ou uma assinatura.

```
{
    "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 gerenciada: AWSEntityResolutionConsoleReadOnlyAccess

Você pode anexar `AWSEntityResolutionConsoleReadOnlyAccess` às entidades do IAM.

Essa política concede acesso somente para leitura a AWS Entity Resolution endpoints e recursos.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `EntityResolutionRead`— Permite que os diretores tenham acesso somente de leitura aos AWS Entity Resolution endpoints e recursos.

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

AWS Entity Resolution atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Entity Resolution desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS Entity Resolution documento.

Alteração	Descrição	Data
`AWSEntityResolutionConsoleFullAccess` : atualizar para uma política existente.	Adicionado `ADXReadAccess` e `ManageEventBridgeRules` para ativar a opção de serviços do provedor no fluxo de trabalho correspondente.	16 de outubro de 2023
AWS Entity Resolution começou a rastrear alterações	AWS Entity Resolution começou a rastrear as mudanças em suas políticas AWS gerenciadas.	18 de agosto de 2023

Solução de problemas AWS Entity Resolution de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Entity Resolution um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AWS Entity Resolution
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Entity Resolution recursos

Não estou autorizado a realizar uma ação em AWS Entity Resolution

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um recurso do *`my-example-widget`* fictício, mas não tem as permissões fictícias do `entityresolution:`*`GetWidget`*.

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

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso *`my-example-widget`* usando a ação `entityresolution:`*`GetWidget`*.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Entity Resolution.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS Entity Resolution. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Entity Resolution recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o

perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS Entity Resolution compatível com esses recursos, consulteComo AWS Entity Resolution funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Validação de conformidade para AWS Entity Resolution

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.

- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no AWS Entity Resolution

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, throughputs elevadas e em redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura globalAWS.

Além da infraestrutura global da AWS, o AWS Entity Resolution oferece vários recursos para ajudar a oferecer suporte às suas necessidades de resiliência de dados e backup.

Monitoramento AWS Entity Resolution

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Entity Resolution suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar AWS Entity Resolution, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por você ou em seu nome Conta da AWS e entrega os arquivos de log em um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário da AWS CloudTrail.

Tópicos

Registrando chamadas de AWS Entity Resolution API usando AWS CloudTrail

AWS Entity Resolution é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS Entity Resolution. CloudTrail captura todas as chamadas de API AWS Entity Resolution como eventos. As chamadas capturadas incluem chamadas do AWS Entity Resolution console e chamadas de código para as operações AWS Entity Resolution da API. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. AWS Entity Resolution Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS Entity Resolution, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

AWS Entity Resolution informações em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre em AWS Entity Resolution, essa atividade é registrada em um CloudTrail evento junto com outros

eventos AWS de serviço no histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua Conta da AWS, incluindo eventos para AWS Entity Resolution, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas AWS Entity Resolution as ações são registradas CloudTrail e documentadas na Referência da AWS Entity Resolution API.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail userIdentity.

Entendendo as entradas do arquivo de AWS Entity Resolution log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações

sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Criação de recursos de resolução de entidades da AWS com AWS CloudFormation

O AWS Entity Resolution é integrado com AWS CloudFormation um serviço que ajuda você a modelar e configurar seus AWS recursos para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os AWS recursos que você deseja (como AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e AWS::EntityResolution::PolicyStatement) e AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar seus recursos de resolução de entidades da AWS de forma consistente e repetida. Descreva seus recursos uma vez e, em seguida, provisione os mesmos recursos repetidamente em várias Contas da AWS regiões.

Resolução e AWS CloudFormation modelos de entidades da AWS

Para provisionar e configurar recursos para a resolução de entidades da AWS e serviços relacionados, você deve entender AWS CloudFormation os modelos. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation Para obter mais informações, consulte O que é o Designer AWS CloudFormation ? no Manual do usuário do AWS CloudFormation .

A resolução de entidades da AWS oferece suporte à criação AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e AWS::EntityResolution::PolicyStatement à entrada AWS CloudFormation. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e AWS::EntityResolution::PolicyStatement, consulte a referência do tipo de recurso de resolução de entidades da AWS no Guia do AWS CloudFormation usuário.

Os seguintes modelos estão disponíveis:

- Fluxo de trabalho correspondente

  Crie um `MatchingWorkflow` objeto que armazene a configuração da tarefa de processamento de dados a ser executada.

  Para obter mais informações, consulte os tópicos a seguir.

  AWS::EntityResolution::MatchingWorkflow no AWS CloudFormation Guia do usuário

  CreateMatchingWorkflow na Referência de API do AWS Entity Resolution
- Mapeamento de esquemas

  Crie um mapeamento de esquema, que define o esquema da tabela de registros do cliente de entrada.

  Para obter mais informações, consulte os tópicos a seguir.

  AWS::EntityResolution::SchemaMapping no AWS CloudFormation Guia do usuário

  CreateSchemaMapping na Referência de API do AWS Entity Resolution
- Workflow de mapeamento de ID

  Crie um `IdMappingWorkflow` objeto que armazene a configuração da tarefa de processamento de dados a ser executada.

  Para obter mais informações, consulte os tópicos a seguir.

  AWS::EntityResolution::IdMappingWorkflow no AWS CloudFormation Guia do usuário

  CreateIdMappingWorkflow na Referência de API do AWS Entity Resolution
- Namespace de ID

  Crie um `IdNamespace` objeto, que armazene os metadados explicando o conjunto de dados e como usá-lo.

  Para obter mais informações, consulte os tópicos a seguir.

  AWS::EntityResolution::IdNamespace no AWS CloudFormation Guia do usuário

  CreateIdNamespace na Referência de API do AWS Entity Resolution
- PolicyStatement

Crie um objeto `PolicyStatement`.

Para obter mais informações, consulte os tópicos a seguir.

AWS::EntityResolution::PolicyStatement no AWS CloudFormation Guia do usuário

AddPolicyStatement na Referência de API do AWS Entity Resolution

Saiba mais sobre AWS CloudFormation

Para saber mais sobre isso AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- AWS CloudFormation Guia do usuário
- Referência da API do AWS CloudFormation
- AWS CloudFormation Guia do usuário da interface de linha de comando

Cotas para AWS Entity Resolution

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada um. AWS service (Serviço da AWS) A menos que especificado de outra forma, cada cota é específica da região . Você pode solicitar aumentos para algumas cotas, mas outras cotas não podem ser aumentadas.

Para ver as cotas de AWS Entity Resolution, abra o console Service Quotas. No painel de navegação, escolha Serviços AWS e selecione AWS Entity Resolution.

Para solicitar o aumento da cota, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no serviço de cotas, use o formulário de aumento de limite.

Você Conta da AWS tem as seguintes cotas relacionadas a. AWS Entity Resolution

Nome	Padrão	Ajustável	Descrição
Trabalhos simultâneos de mapeamento de ID	1	Não	O número máximo de trabalhos de mapeamento de ID que podem ser processados simultaneamente no atual Região da AWS.
Trabalhos correspondentes simultâneos	1	Não	O número máximo de trabalhos correspondentes que podem ser processados simultaneamente no atual Região da AWS.
Trabalhos simultâneos de correspondência de serviços do provedor	1	Não	O número máximo de trabalhos correspondentes ao serviço do provedor que podem ser processados simultaneamente no atual Região da AWS.
Entrada de dados	20	Não	Esta é a lista de tabelas de entrada que você deseja usar em um fluxo de trabalho de correspondência. Cada entrada corresponde a uma coluna

Nome	Padrão	Ajustável	Descrição
			em sua tabela AWS Glue de dados de entrada, que contém o nome da coluna e informações adicionais que são AWS Entity Resolution usadas para fins de correspondência. As entradas devem conter uma ID exclusiva mais pelo menos um campo de entrada adicional.
Dados de saída	750	Não	Essa é uma lista de `OutputAttribute` objetos, cada um com os campos Nome e Hashed. Cada um desses objetos representa uma coluna a ser incluída na tabela AWS Glue de saída e se você deseja que os valores na coluna sejam criptografados.
Esquema de dados	25	Não	O número máximo de campos de entrada do esquema de dados.
Fluxos de trabalho de mapeamento de	10	Sim	O número máximo de fluxos de trabalho de mapeamento de ID que você pode criar Conta da AWS neste momento Região da AWS.
Namespaces de ID	10	Sim	O número máximo de namespaces de ID que você pode criar Conta da AWS neste momento. Região da AWS
IDs de correspondência	500	Não	O número máximo de registros que podem ser consolidados em um MatchID por carga de trabalho.

Nome	Padrão	Ajustável	Descrição
Regra de correspondência	15	Não	Para correspondência baseada em regras, esse é o número da regra aplicada que gerou um conjunto de registros correspondente. Isso faz parte da correspondência dos metadados do fluxo de trabalho que serão incluídos na saída.
Fluxos de trabalho correspondentes	10	Sim	O número máximo de fluxos de trabalho de correspondência.
Número de regras por fluxo de trabalho	15	Não	O número máximo de regras por fluxo de trabalho de correspondência.
Taxa de solicitações de API `GetMatchId`	50	Sim	O número máximo de solicitações de `GetCustomerID` API por segundo.
Mapeamentos de esquema	50	Sim	O número máximo de mapeamentos de esquema que você pode criar nessa conta na região atual. AWS

Nome	Padrão	Ajustável	Descrição
Chaves de correspondência exclusivas por conjunto de regras	15	Não	O número máximo de chaves de correspondência exclusivas por conjunto de regras. Uma chave de correspondência instrui AWS Entity Resolution quais campos de entrada devem ser considerados como dados semelhantes e quais devem ser considerados como dados diferente s. Isso ajuda a configurar AWS Entity Resolution automaticamente as regras de correspondência baseadas em regras e a comparar dados semelhant es armazenados em diferentes campos de entrada.

Cotas de controle de utilização da API

Recurso	Padrão	Descrição
Taxa de solicitações de `GetMatchId`	50 TPS	Número máximo de chamadas de `GetMatchId` API por segundo.

Histórico de documentos do Guia AWS Entity Resolution do usuário

A tabela a seguir descreve as versões de documentação do AWS Entity Resolution.

Para receber notificações sobre atualizações dessa documentação, você pode se inscrever em o feed RSS. Para assinar as atualizações de RSS, você deve ter um plug-in de RSS habilitado para o navegador que está usando.

Alteração	Descrição	Data
Fluxo de trabalho correspondente — atualização	Agora, os clientes podem excluir os registros de um fluxo de trabalho de correspondência baseado em regras ou em ML para ajudar a cumprir os regulamentos de gerenciamento de dados.	8 de abril de 2024
Fluxo de trabalho de mapeamento de ID — atualização	Agora, os clientes podem usar um fluxo de trabalho de mapeamento de ID em vários Contas da AWS.	2 de abril de 2024
CloudFormation Recursos da AWS — Recursos novos e atualizados	A AWS Entity Resolution adicionou os seguintes recursos: `AWS::EntityResolution::IdNamespace` `AWS::EntityResolution::PolicyStatement` e atualizou o seguinte recurso:`AWS::EntityResolution::IdMappingWorkflow` .	2 de abril de 2024
Encontre o ID da partida	Agora, os clientes podem encontrar o Match ID	25 de março de 2024

	correspondente e a regra associada para um fluxo de trabalho processado baseado em regras.	
Fluxo de trabalho correspondente — atualização	AWS Entity Resolution agora oferece suporte à atribuição de RAMPID baseada em PII no fluxo de trabalho de correspondência baseado em LiveRamp serviços do provedor.	12 de fevereiro de 2024
AWS PrivateLink	AWS Entity Resolution agora oferece suporte adicional à segurança de dados, ajudando AWS PrivateLink os clientes a acessar de forma privada os serviços hospedados em AWS.	20 de outubro de 2023
AWS CloudFormation Recursos — Recursos novos e atualizados	AWS Entity Resolution adicionou o seguinte recurso: `AWS::EntityResolution:IdMappingWorkflow` e atualizou os seguintes recursos: `AWS::EntityResolution::MatchingWorkflow` `AWS::EntityResolution::Schemamapping` e.	19 de outubro de 2023

Atualizar a política existente	As seguintes novas permissões foram adicionadas à política `AWSEntityResolutionConsoleFullAccess` gerenciada: `ADXReadAccess` `ManageEventBridgeRules` e.	16 de outubro de 2023
Mapeamento do esquema — atualização	Agora, os clientes podem editar e atualizar um esquema de dados existente.	16 de outubro de 2023
Fluxo de trabalho correspondente — atualização	Agora, os clientes podem selecionar um serviço de provedor de dados preferencial para ajudar a combinar e vincular seus dados.	16 de outubro de 2023
Workflow de mapeamento de ID	Os clientes podem usar esse novo fluxo de trabalho para especificar detalhes do mapeamento de ID, escolher o método de mapeamento de ID desejado e especificar campos de entrada e saída de dados.	16 de outubro de 2023
AWS CloudFormation integração	AWS Entity Resolution agora se integra com AWS CloudFormation.	24 de agosto de 2023
AWS atualização de política gerenciada - Novas políticas	AWS Entity Resolution adicionou duas novas políticas gerenciadas.	18 de agosto de 2023
Lançamento inicial	Versão inicial do Guia AWS Entity Resolution do usuário	26 de julho de 2023

AWS Entity Resolution Glossário

Nome do recurso da Amazon (ARN)

Um identificador exclusivo para AWS recursos. Os ARNs são necessários quando você precisa especificar um recurso de forma inequívoca em todos eles AWS Entity Resolution, como em AWS Entity Resolution políticas, tags do Amazon Relational Database Service (Amazon RDS) e chamadas de API.

Processamento automático

Uma opção de cadência de processamento para uma tarefa de fluxo de trabalho correspondente que permite que ela seja executada automaticamente quando a entrada de dados é alterada.

Essa opção está disponível somente para correspondência baseada em regras.

Por padrão, a cadência de processamento de uma tarefa de fluxo de trabalho correspondente é definida como Manual, o que permite que ela seja executada sob demanda. Você pode configurar o processamento automático para executar automaticamente sua tarefa de fluxo de trabalho correspondente quando a entrada de dados for alterada. Isso mantém a saída correspondente do fluxo de trabalho up-to-date.

AWS KMS key ARN

Este é o seu nome de recurso AWS KMS da Amazon (ARN) para criptografia em repouso. Se não for fornecido, o sistema usará uma chave KMS AWS Entity Resolution gerenciada.

Texto não criptografado

Dados que não estão protegidos criptograficamente.

Nível de confiança (ConfidenceLevel)

Para correspondência de ML, esse é o nível de confiança aplicado AWS Entity Resolution quando o ML identifica um conjunto de registros correspondente. Isso faz parte dos metadados correspondentes do fluxo de trabalho que serão incluídos na saída.

Descriptografia

O processo de transformar dados criptografados de volta à sua forma original. Só será possível realizar se você tiver acesso à chave secreta.

Criptografia

O processo de codificação de dados em um formato que parece aleatório usando um valor secreto chamado chave. É impossível determinar o texto sem formatação original sem acesso à chave.

Group name

O nome do grupo faz referência a todo o grupo de campos de entrada e pode ajudá-lo a agrupar dados analisados para fins de correspondência.

Por exemplo, se houver três campos de entrada: **`first_name`**`middle_name`,, e**`last_name`**, você pode agrupá-los inserindo o nome do grupo **`full_name`** para correspondência e saída.

Hash

O hashing significa aplicar um algoritmo criptográfico que produz uma sequência irreversível e exclusiva de caracteres de tamanho fixo, chamada de hash. AWS Entity Resolution usa o protocolo de hash Secure Hash Algorithm de 256 bits (SHA256) e produzirá uma cadeia de caracteres de 32 bytes. Em AWS Entity Resolution, você pode escolher se deseja fazer o hash dos valores de dados em sua saída.

Protocolo de hash () HashingProtocol

AWS Entity Resolution usa o protocolo de hash Secure Hash Algorithm de 256 bits (SHA256) e produzirá uma cadeia de caracteres de 32 bytes. Isso faz parte dos metadados correspondentes do fluxo de trabalho que serão incluídos na saída.

Workflow de mapeamento de ID

O processo que você configura para especificar os dados de entrada para traduzir seus IDs e como você deseja que o mapeamento de ID seja executado.

AWS Entity Resolution atualmente é compatível com LiveRamp o método de mapeamento de ID. Você deve ter uma assinatura do LiveRamp Through AWS Data Exchange para usar o fluxo de trabalho de mapeamento de ID.

Para ter mais informações, consulte Assine um serviço de provedor em AWS Data Exchange.

Namespace de ID

Um recurso AWS Entity Resolution que contém metadados que explicam conjuntos de dados em vários Contas da AWS e como usar esses conjuntos de dados em um fluxo de trabalho de mapeamento de ID.

Há dois tipos de namespaces de ID: e. SOURCE TARGET O SOURCE contém configurações para os dados de origem que serão processados em um fluxo de trabalho de mapeamento de ID. O TARGET contém uma configuração dos dados de destino para os quais todas as fontes resolverão. Para definir os dados de entrada que você deseja resolver em dois Contas da AWS, crie uma fonte de namespace de ID e um destino de namespace de ID para traduzir seus dados de um set () para outro ()SOURCE. TARGET

Depois que você e outro membro criarem namespaces de ID e executarem um fluxo de trabalho de mapeamento de ID, você poderá participar de uma colaboração AWS Clean Rooms para executar uma união de várias tabelas na tabela de mapeamento de ID e analisar os dados.

Para mais informações, consulte o Guia do usuário do AWS Clean Rooms.

Campo de entrada

Um campo de entrada corresponde ao nome de uma coluna da sua tabela AWS Glue de dados de entrada.

ARN da fonte de entrada (ARN) InputSource

O Amazon Resource Name (ARN) que foi gerado para uma entrada de AWS Glue tabela. Isso faz parte da correspondência dos metadados do fluxo de trabalho que serão incluídos na saída.

Tipo de entrada

O tipo de dados de entrada. Você o seleciona em uma lista pré-configurada de valores, como nome, endereço, número de telefone ou endereço de e-mail. O tipo de entrada informa AWS

Entity Resolution que tipo de dados você está apresentando, permitindo que sejam classificados e normalizados adequadamente.

Correspondência baseada em aprendizado de máquina

A correspondência baseada em aprendizado de máquina (correspondência de ML) encontra correspondências em seus dados que podem estar incompletas ou podem não ter a mesma aparência. A correspondência de ML é um processo predefinido que tentará combinar registros em todos os dados inseridos. A correspondência de ML retorna uma ID de correspondência e um nível de confiança para cada conjunto de dados correspondente.

Processamento manual

Uma opção de cadência de processamento para uma tarefa de fluxo de trabalho correspondente que permite que ela seja executada sob demanda.

Essa opção é definida por padrão e está disponível tanto para correspondência baseada em regras quanto para correspondência baseada em aprendizado de máquina.

Combinação de muitos para muitos

A any-to-many correspondência M compara várias instâncias de dados semelhantes. Os valores nos campos de entrada aos quais foi atribuída a mesma chave de correspondência serão comparados entre si, independentemente de estarem no mesmo campo de entrada ou em campos de entrada diferentes.

Por exemplo, você pode ter vários campos de entrada de número de telefone, como `mobile_phone` e `home_phone` que tenham a mesma tecla de correspondência “Telefone”. Use a many-to-many correspondência para comparar dados no campo `mobile_phone` de entrada com dados no campo `mobile_phone` de entrada e dados no campo `home_phone` de entrada.

As regras de correspondência avaliam dados em vários campos de entrada com a mesma chave de correspondência com uma operação (ou), e a one-to-many correspondência compara valores em vários campos de entrada. Isso significa que, se alguma combinação de `mobile_phone` ou `home_phone` corresponder entre dois registros, a tecla de correspondência “Telefone” retornará uma correspondência. Para combinar, tecle “Telefone” para encontrar uma correspondência, `Record One mobile_phone = Record Two mobile_phone` OR `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 da partida (MatchID)

Para correspondência baseada em regras e correspondência de ML, essa é a ID gerada AWS Entity Resolution e aplicada a cada conjunto de registros correspondente. Isso faz parte dos metadados correspondentes do fluxo de trabalho que serão incluídos na saída.

Tecla de correspondência (MatchKey)

A chave de correspondência instrui AWS Entity Resolution quais campos de entrada devem ser considerados como dados semelhantes e quais devem ser considerados como dados diferentes. Isso ajuda a configurar AWS Entity Resolution automaticamente as regras de correspondência baseadas em regras e a comparar dados semelhantes armazenados em diferentes campos de entrada.

Se houver vários tipos de informações de número de telefone, como um `mobile_phone` campo de `home_phone` entrada e um campo de entrada em seus dados, que você gostaria de comparar, forneça a ambos a tecla de correspondência “Telefone”. Em seguida, a correspondência baseada em regras pode ser configurada para comparar dados usando instruções “ou” em todos os campos de entrada com a tecla de correspondência “Telefone” (consulte as definições de correspondência um-para-um e correspondência muito-para-muitos na seção Fluxo de trabalho de correspondência).

Se você quiser que a correspondência baseada em regras considere diferentes tipos de informações de números de telefone de forma completamente separada, você pode criar chaves de correspondência mais específicas, como “Celular_Telefone” e “Home_Phone”. Em seguida, ao configurar um fluxo de trabalho de correspondência, você pode especificar como cada chave de correspondência telefônica será usada na correspondência baseada em regras.

Se não MatchKey for especificado para um campo de entrada específico, ele não poderá ser usado na correspondência, mas poderá ser realizado pelo processo de fluxo de trabalho correspondente e poderá ser gerado, se desejado.

Nome da chave de correspondência

O nome atribuído a uma chave de correspondência.

Regra de partida (MatchRule)

Para correspondência baseada em regras, esse é o número da regra aplicada que gerou um conjunto de registros correspondente. Isso faz parte dos metadados correspondentes do fluxo de trabalho que serão incluídos na saída.

Correspondência

O processo de combinar e comparar dados de diferentes campos de entrada, tabelas ou bancos de dados e determinar quais deles são semelhantes — ou “coincidem” — com base na satisfação de determinados critérios de correspondência (por exemplo, por meio de regras ou modelos de correspondência).

Fluxo de trabalho correspondente

O processo que você configurou para especificar os dados de entrada a serem combinados e como a correspondência deve ser realizada.

Descrição do fluxo de trabalho correspondente

Uma descrição opcional do fluxo de trabalho correspondente que você pode optar por inserir. As descrições ajudam a diferenciar os fluxos de trabalho correspondentes se você criar mais de um.

Nome do fluxo de trabalho correspondente

O nome do fluxo de trabalho correspondente que você especifica.

> **Note**
>
> Os nomes de fluxo de trabalho correspondentes devem ser exclusivos. Eles não podem ter o mesmo nome ou um erro será retornado.

Metadados de fluxo de trabalho correspondentes

Informações geradas e enviadas AWS Entity Resolution durante um trabalho de fluxo de trabalho correspondente. Essas informações são necessárias na saída.

Normalização () ApplyNormalization

Escolha se deseja normalizar os dados de entrada conforme definido no esquema. A normalização padroniza os dados removendo espaços extras e caracteres especiais e padronizando para o formato minúsculo.

Por exemplo, se um campo de entrada tiver um tipo de `PHONE_NUMBER` entrada e os valores na tabela de entrada estiverem formatados como`(123) 456-7890`, AWS Entity Resolution normalizará os valores para. `1234567890`

As seções a seguir descrevem as regras de normalização.

Tópicos

Nome

- TRIM = Remove os espaços em branco à esquerda e à direita
- MINÚSCULAS = Todos os caracteres alfa são minúsculos
- CONVERT_ACCENT = Letra acentuada oculta em letra normal
- REMOVE_ALL_NON_ALPHA = Remove todos os caracteres não alfa [A-zA-z]

E-mail

- TRIM = Remove os espaços em branco à esquerda e à direita
- MINÚSCULAS = Todos os caracteres alfa são minúsculos
- CONVERT_ACCENT = Letra acentuada oculta em letra normal
- REMOVE_ALL_NON_EMAIL_CHARS = Remove todos os caracteres [a-zA-z0-9] e [.@-] non-alpha-numeric

Telefone

- TRIM = Remove os espaços em branco à esquerda e à direita
- REMOVE_ALL_NON_NUMERIC = Remove todos os caracteres não numéricos [0-9]
- REMOVE_ALL_LEADING_ZEROES=Remove todos os zeros iniciais

Endereço

- TRIM = Remove os espaços em branco à esquerda e à direita
- MINÚSCULAS = Todos os caracteres alfa são minúsculos
- CONVERT_ACCENT = Letra acentuada oculta em letra normal
- REMOVE_ALL_NON_ALPHA = Remove todos os caracteres não alfa [A-zA-z]
- RENAME_WORDS usando ADDRESS_RENAME_WORD_MAP = substituir palavras na string de endereço por palavras de ADDRESS_RENAME_WORD_MAP
- RENAME_DELIMITERS usando ADDRESS_RENAME_DELIMITER_MAP = substituir delimitadores na string de endereço pela string de ADDRESS_RENAME_DELIMITER_MAP
- RENAME_DIRECTIONS usando ADDRESS_RENAME_DIRECTION_MAP = substituir delimitadores na string de endereço pela string de ADDRESS_RENAME_DIRECTION_MAP
- RENAME_NUMBERS usando ADDRESS_RENAME_NUMBER_MAP = substituir números na string de endereço pela string de ADDRESS_RENAME_NUMBER_MAP
- RENAME_SPECIAL_CHARS usando ADDRESS_RENAME_SPECIAL_CHAR_MAP = substituir caracteres especiais na string de endereço pela string de ADDRESS_RENAME_SPECIAL_CHAR_MAP

ENDEREÇO_RENOME_MAPA_PALAVRA_DE_ENDEREÇO

Essas são as palavras que serão renomeadas ao normalizar a string de endereço.

```
"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"
```

MAPA_DELIMITADOR_DELIMITADOR DE ENDEREÇOS

Esses são os delimitadores que serão renomeados ao normalizar a string de endereço.

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

ENDEREÇO_RENOME_MAPA_DIREÇÃO_DE_ENDEREÇO

Esses são os identificadores de direção que serão renomeados ao normalizar a string de endereço.

```
"east": "e",
"north": "n",
"south": "s",
"west": "w",
"northeast": "ne",
```

```
"northwest": "nw",
"southeast": "se",
"southwest": "sw"
```

ENDEREÇO_RENOME_NÚMERO_MAPA_DO_ENDEREÇO

Essas são as sequências numéricas que serão renomeadas ao normalizar a sequência de endereço.

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

ADDRESS_RENAME_SPECIAL_CHAR_MAP

Essas são as cadeias de caracteres especiais que serão renomeadas ao normalizar a cadeia de endereços.

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

Hashado

- TRIM = Remove os espaços em branco à esquerda e à direita

ID de origem

- TRIM = Remove os espaços em branco à esquerda e à direita

Correspondência individual

O ne-to-one matching compara instâncias únicas de dados semelhantes. Os campos de entrada com a mesma chave de correspondência e valores no mesmo campo de entrada serão comparados entre si.

Por exemplo, você pode ter vários campos de entrada de número de telefone, como `mobile_phone` e `home_phone` que tenham a mesma tecla de correspondência “Telefone”. Use a one-to-one correspondência para comparar dados no campo `mobile_phone` de entrada com dados no campo `mobile_phone` de entrada e para comparar dados no campo `home_phone` de entrada com dados no campo `home_phone` de entrada. Os dados no campo `mobile_phone` de entrada não serão comparados com os dados no campo `home_phone` de entrada.

As regras de correspondência avaliam dados em vários campos de entrada com a mesma chave de correspondência com uma operação (ou), e a one-to-many correspondência compara valores em um único campo de entrada. Isso significa que se `mobile_phone` ou `home_phone` corresponder entre dois registros, a tecla de correspondência “Telefone” retornará uma correspondência. Para combinar, tecle “Telefone” para encontrar uma correspondência, `Record One mobile_phone = Record Two mobile_phone` OU`Record One home_phone = Record Two home_phone`.

As regras de correspondência avaliam dados em campos de entrada com chaves de correspondência diferentes com uma operação (e). Se você quiser que a correspondência baseada em regras considere diferentes tipos de informações de números de telefone de forma completamente separada, você pode criar chaves de correspondência mais específicas, como “mobile_phone” e “home_phone”. Se você quiser usar as duas teclas de correspondência em uma regra para encontrar correspondências, `Record One mobile_phone = Record Two mobile_phone` AND`Record One home_phone = Record Two home_phone`.

Saída

Uma lista de OutputAttributeobjetos, cada um com os campos Nome e Hashed. Cada um desses objetos representa uma coluna a ser incluída na tabela AWS Glue de saída e se você deseja que os valores na coluna sejam criptografados.

Saídas 3path

O destino do S3 no qual AWS Entity Resolution gravará a tabela de saída.

OutputSourceConfig

Uma lista de OutputSource objetos, cada um com os campos Outputs3Path e Output. ApplyNormalization

Correspondência baseada em serviços de provedores

A correspondência baseada em serviços de provedores é um processo projetado para combinar, vincular e aprimorar seus registros com provedores de serviços de dados preferenciais e conjuntos de dados licenciados. Você deve ter uma assinatura AWS Data Exchange com o serviço do provedor para usar essa técnica de correspondência.

AWS Entity Resolution atualmente se integra aos seguintes provedores de serviços de dados:

- LiveRamp
- TransUnion
- UID 2.0

Correspondência baseada em regras

A correspondência baseada em regras é um processo projetado para encontrar correspondências exatas. A correspondência baseada em regras é um conjunto hierárquico de regras de correspondência em cascata, sugerido por AWS Entity Resolution, com base nos dados que você insere e totalmente configurável por você. Todas as chaves de correspondência fornecidas nos critérios da regra devem corresponder exatamente para que os dados comparados sejam declarados como correspondências e para que os metadados associados sejam gerados. A correspondência baseada em regras retorna uma ID de correspondência e um número de regra para cada conjunto de dados correspondente.

Recomendamos definir regras que possam identificar uma entidade de forma exclusiva. Ordene suas regras para encontrar combinações mais precisas primeiro.

Por exemplo, digamos que você tenha duas regras, Regra 1 e Regra 2.

Essas regras têm as seguintes chaves de correspondência:

- A regra 1 inclui nome completo e endereço
- A regra 2 inclui nome completo, endereço e telefone

Como a Regra 1 é executada primeiro, nenhuma correspondência será encontrada pela Regra 2 porque todas teriam sido encontradas pela Regra 1.

Para encontrar correspondências diferenciadas por telefone, reordene as regras, assim:

- A regra 2 inclui nome completo, endereço e telefone
- A regra 1 inclui nome completo e endereço

Schema

O termo usado para uma estrutura ou layout que define como um conjunto de dados é organizado e conectado.

Descrição do esquema

Uma descrição opcional do esquema que você pode escolher inserir. As descrições ajudam a diferenciar os mapeamentos de esquema se você criar mais de um.

Nome do esquema

O nome do esquema.

> **Note**
>
> Os nomes dos esquemas devem ser exclusivos. Eles não podem ter o mesmo nome ou um erro será retornado.

Mapeamento de esquemas

O mapeamento de esquema AWS Entity Resolution é o processo pelo qual você AWS Entity Resolution informa como interpretar seus dados para correspondência. Você define o esquema da tabela de dados de entrada que AWS Entity Resolution deseja ler em um fluxo de trabalho correspondente.

ARN de mapeamento de esquema

O Amazon Resource Name (ARN) gerado para o mapeamento do esquema.

ID exclusivo

Um identificador exclusivo que você designa e que deve ser atribuído a cada linha de dados de entrada AWS Entity Resolution lida.

Example

Por exemplo: **`Primary_key`**, **`Row_ID`** ou **`Record_ID`**.

A coluna ID exclusiva é obrigatória.

O ID exclusivo deve ser um identificador exclusivo em uma única tabela.

Em tabelas diferentes, o ID exclusivo pode ter valores duplicados.

Quando o fluxo de trabalho correspondente for executado, o registro será rejeitado se a ID exclusiva:

- não está especificado
- não é exclusivo na mesma tabela
- sobrepõe-se em termos de nome de atributo nas fontes.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.