Guida per l'utente

AWS Entity Resolution

AWS Entity Resolution: Guida per l'utente

Table of Contents

Che cos'è AWS Entity Resolution?

AWS Entity Resolution è un servizio che consente di abbinare, collegare e migliorare i record correlati archiviati in più applicazioni, canali e archivi di dati. Puoi iniziare a utilizzare flussi di lavoro per la risoluzione delle entità flessibili, scalabili e in grado di connettersi alle applicazioni e ai provider di servizi dati esistenti.

AWS Entity Resolution offre tecniche di abbinamento avanzate, come la corrispondenza basata su regole, la corrispondenza basata sull'apprendimento automatico (abbinamento ML) e la corrispondenza guidata dai fornitori di servizi di dati. Queste tecniche possono aiutarti a collegare e migliorare in modo più accurato i record correlati di informazioni sui clienti, codici di prodotto o codici di dati aziendali.

Puoi utilizzarle AWS Entity Resolution per creare una visualizzazione unificata delle interazioni con i clienti collegando gli eventi recenti (come clic sugli annunci, abbandono del carrello e acquisti) a segnali pseudonimizzati dei tuoi fornitori di servizi di dati in un ID di entità univoco. Puoi anche monitorare meglio i prodotti che utilizzano codici diversi (ad esempio,) nei tuoi negozi. SKU UPC Puoi utilizzarli AWS Entity Resolution per controllare l'accuratezza della corrispondenza e proteggere meglio la sicurezza dei dati, riducendo al minimo lo spostamento dei dati.

Argomenti

Sei un utente alle prime armi AWS Entity Resolution ?

Se sei un utente principiante di AWS Entity Resolution, ti consigliamo di iniziare leggendo le seguenti sezioni:

- Caratteristiche di AWS Entity Resolution
- Accedendo AWS Entity Resolution
- Configurare AWS Entity Resolution

Caratteristiche di AWS Entity Resolution

AWS Entity Resolution include le seguenti funzionalità:

- Preparazione dei dati flessibile e personalizzabile

  AWS Entity Resolution legge i dati da utilizzare come input AWS Glue per l'elaborazione delle partite. È possibile specificare un massimo di 20 input di dati. AWS Entity Resolution elabora ogni riga della tabella di immissione dei dati come record, con un'entità univoca che funge da chiave primaria. AWS Entity Resolution può operare su set di dati crittografati. Definisci innanzitutto la mappatura dello schema AWS Entity Resolution per capire quali campi di input desideri utilizzare nel flusso di lavoro corrispondente. Puoi importare il tuo schema di dati, o blueprint, da un input di AWS Glue dati esistente. In alternativa, puoi creare il tuo schema personalizzato utilizzando un'interfaccia utente o un JSON editor interattivo. Per impostazione predefinita, normalizza AWS Entity Resolution anche gli input di dati prima della corrispondenza per migliorare l'elaborazione delle corrispondenze, ad esempio rimuovendo caratteri speciali e spazi aggiuntivi e formattando il testo in minuscolo. Se l'immissione dei dati è già normalizzata, puoi disattivare la normalizzazione. Forniamo anche una GitHub libreria, che puoi utilizzare per personalizzare ulteriormente il processo di normalizzazione dei dati in base alle tue esigenze.
- Flussi di lavoro configurabili per l'abbinamento delle entità

  Un flusso di lavoro per l'abbinamento delle entità è una sequenza di passaggi impostata per indicare AWS Entity Resolution come abbinare i dati di input e dove scrivere l'output dei dati consolidati. Puoi configurare uno o più flussi di lavoro di abbinamento per confrontare diversi input di dati e utilizzare diverse tecniche di abbinamento, come la corrispondenza basata su regole, la corrispondenza basata sull'apprendimento automatico o la corrispondenza guidata dai provider di servizi dati senza risoluzione delle entità o esperienza di apprendimento automatico. Puoi anche visualizzare lo stato del lavoro dei flussi di lavoro e delle metriche corrispondenti esistenti, come il numero di risorse, il numero di record elaborati e il numero di corrispondenze trovate.

  - eady-to-use Corrispondenza basata su regole R

    Questa tecnica di abbinamento include una serie di ready-to-use regole in AWS Management Console or AWS Command Line Interface ()AWS CLI. È possibile utilizzare queste regole per trovare i record correlati in base ai campi di immissione. Puoi anche personalizzare le regole aggiungendo o rimuovendo campi di input per ogni regola, eliminando le regole, riorganizzando la priorità delle regole e creando nuove regole. Puoi anche reimpostare le regole per riportarle alle configurazioni originali. L'output di dati nel bucket Amazon Simple Storage Service (Amazon

S3) contiene gruppi di corrispondenza generati utilizzando la tecnica di abbinamento AWS Entity Resolution basata su regole. A ogni gruppo di partite è associato il numero della regola utilizzato per generare la corrispondenza, in modo da aiutarti a comprendere la corrispondenza. Ad esempio, il numero della regola può dimostrare la precisione di ogni gruppo di partite in modo che la regola uno sia più precisa della regola due.

- Abbinamento preconfigurato basato sull'apprendimento automatico (abbinamento ML)

  Questa tecnica di abbinamento include un modello ML preconfigurato per trovare le corrispondenze tra tutti gli input di dati, in particolare i record basati sui consumatori. Il modello utilizza tutti i campi di input associati ai tipi di dati relativi a nome, indirizzo e-mail, numero di telefono, indirizzo e data di nascita. Il modello genera gruppi di partite di record correlati con un punteggio di confidenza per ogni gruppo che spiega la qualità della partita rispetto ad altri gruppi di partite. Il modello considera i campi di input mancanti e analizza l'intero record insieme per rappresentare un'entità. L'output di dati nel tuo bucket Amazon S3 presenta gruppi di corrispondenze AWS Entity Resolution generati utilizzando la corrispondenza ML. È qui che ogni gruppo di gioco ha un punteggio di confidenza associato di 0,0—1,0, che indica la precisione della partita.

- Abbinamento dei record con i fornitori di servizi di dati

  Con AWS Entity Resolution puoi abbinare, collegare e migliorare i tuoi record con i principali fornitori di servizi dati e set di dati autorizzati per espandere la tua capacità di comprendere, raggiungere e fornire assistenza ai tuoi clienti. Ad esempio, puoi aggiungere attributi ai tuoi dati per migliorare i tuoi record oppure puoi migliorare l'interoperabilità dei sistemi e delle piattaforme con cui lavori per raggiungere i tuoi obiettivi aziendali. Puoi utilizzare questo flusso di lavoro corrispondente con pochi clic, eliminando la necessità di creare e mantenere integrazioni proprietarie complesse. È necessario disporre di un contratto di licenza con questi fornitori di servizi di dati per sfruttare questa tecnica di abbinamento.

- Elaborazione manuale in blocco ed elaborazione incrementale automatica

  È possibile utilizzare l'elaborazione dei dati per convertire l'input o gli input dei dati in una tabella di output dei dati consolidata con record simili che hanno un ID di corrispondenza comune generato utilizzando le configurazioni del flusso di lavoro di corrispondenza delle entità. Utilizzando API and AWS Management Console o il AWS CLI, puoi eseguire l'elaborazione manuale in blocco su richiesta, in base alla pipeline di dati Extract, Transform e Load (ETL) esistente, che rielabora tutti i dati per eventuali nuove corrispondenze e aggiornamenti delle corrispondenze esistenti. Inoltre, per gli scenari di abbinamento basati su regole, puoi avviare l'elaborazione incrementale automatica in modo che non appena nuovi dati sono disponibili nel tuo bucket Amazon S3, il servizio legga i

nuovi record e li confronti con quelli esistenti. Ciò mantiene le tue corrispondenze aggiornate con eventuali modifiche ai dati di Amazon S3.

- Ricerca quasi in tempo reale

  La ricerca di qualsiasi campo di entità tramite l'AWS Entity Resolution GetMatchId APIoperazione consente di recuperare in modo sincrono un Match ID esistente. Puoi chiamare AWS Entity Resolution con informazioni di identificazione personale (PII) attributi acquisiti attraverso diverse fonti e canali. AWS Entity Resolution esegue l'hash di tali attributi per la protezione dei dati e recupera il match ID corrispondente per collegare e abbinare il cliente. Ad esempio, puoi ottenere una registrazione web con un nome, un'email e un indirizzo postale associati. Utilizza l' AWS Entity Resolution GetMatchId APIoperazione per scoprire se questo cliente o entità esiste già nei risultati corrispondenti memorizzati nel tuo bucket S3, insieme all'ID di corrispondenza dell'entità corrispondente ad esso associato. Dopo aver ottenuto l'Entity Match ID, puoi trovare le informazioni transazionali ad esso associate nelle applicazioni di origine, come i sistemi di gestione delle relazioni con i clienti (CRM) o della piattaforma dati dei clienti (). CDP

- Protezione dei dati e regionalizzazione fin dalla progettazione

  AWS Entity Resolution offre una funzionalità di crittografia predefinita che può aiutarti a proteggere i tuoi dati e ti fornisce una chiave di crittografia per ogni dato immesso nel servizio. Ad esempio, AWS Entity Resolution offre la flessibilità necessaria per utilizzare dati crittografati e sottoposti a hash sul lato server per eseguire flussi di lavoro di abbinamento basati su regole. AWS Entity Resolution supporta la regionalizzazione, il che significa che i flussi di lavoro corrispondenti vengono eseguiti per elaborare i dati nello stesso luogo in cui si utilizza il servizio. Regione AWS Puoi anche crittografare e applicare l'hash dei dati in uscita in Amazon S3 prima di utilizzare i dati risolti in altre applicazioni.

- Transcodifica multipartitica

  AWS Entity Resolution ti aiuta a definire le fonti di dati e le configurazioni corrispondenti tra più parti che desiderano utilizzare una collaborazione sui dati, come in. AWS Clean Rooms

Servizi correlati

Quanto segue AWS servizi è relativo a AWS Entity Resolution:

- Amazon S3

  Archivia i dati che inserisci AWS Entity Resolution in Amazon S3.

Per ulteriori informazioni, consulta Che cos'è Amazon S3? nella Guida per l'utente di Amazon Simple Storage Service.

- AWS Glue

  Crea AWS Glue tabelle dai tuoi dati in Amazon S3 per utilizzarle in. AWS Entity Resolution

  Per ulteriori informazioni, consulta What is AWS Glue? nella Guida per gli AWS Glue sviluppatori.

- AWS CloudTrail

  AWS Entity Resolution Utilizzalo con CloudTrail i log per migliorare l'analisi delle AWS servizio attività.

  Per ulteriori informazioni, consulta Registrazione delle chiamate AWS Entity Resolution API utilizzando AWS CloudTrail.

- AWS CloudFormation

  Crea le seguenti risorse in AWS CloudFormation: AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e AWS::EntityResolution::PolicyStatement

  Per ulteriori informazioni, consulta Crea risorse per la risoluzione delle AWS entità con AWS CloudFormation.

Accedendo AWS Entity Resolution

È possibile accedere AWS Entity Resolution tramite le seguenti opzioni:

- Direttamente tramite la AWS Entity Resolution console all'indirizzo https://console.aws.amazon.com/entityresolution/.
- Programmaticamente tramite. AWS Entity Resolution API Per ulteriori informazioni, vedere la Guida di riferimento.AWS Entity Resolution API
  - Se prevedi di chiamarlo AWS Entity Resolution API in AWS Lambda Runtime, crea il tuo pacchetto di distribuzione e includi la versione desiderata della AWS SDK libreria. Per ulteriori informazioni, consulta i seguenti esempi nella Guida per gli AWS Lambda sviluppatori:
    - Implementa le funzioni Java Lambda con archivi di JAR file.zip o di file
    - Lavorare con archivi di file.zip per le funzioni Python Lambda

Prezzi per AWS Entity Resolution

Per informazioni sui prezzi, consulta Prezzi di AWS Entity Resolution.

Configurare AWS Entity Resolution

Prima di utilizzarlo AWS Entity Resolution per la prima volta, registrati AWS e crea un utente amministratore per creare i ruoli.

Iscrizione a AWS

Se ne hai già uno Account AWS, salta questo passaggio.

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i AWS servizi nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Creazione di un utente amministratore

Per creare un utente amministratore, scegli una delle seguenti opzioni.

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
In IAM Identity Center (Consigliato)	Usa credenziali a breve termine per accedere a AWS. Ciò è in linea con le best practice per la sicurezza . Per informazioni sulle best practice, consulta la sezione Procedure consigliate per la sicurezza IAM nella Guida IAM per l'utente.	Segui le istruzioni riportate in Nozioni di base nella Guida per l'utente di AWS IAM Identity Center .	Configura l'accesso programmatico configurando l'uso AWS IAM Identity Center nella Guida AWS CLI per l'AWS Command Line Interface utente.
In IAM (Non consigliato)	Usa credenziali a lungo termine per accedere a AWS.	Seguendo le istruzioni riportate nella sezione Creazione del primo utente IAM amministratore e gruppo di utenti nella Guida IAM per l'utente.	Configura l'accesso programmatico gestendo le chiavi di accesso per IAM gli utenti nella Guida per l'IAMutente.

Creazione di un IAM ruolo per un utente della console

Completa la procedura seguente se utilizzi la AWS Entity Resolution console.

Per creare un ruolo IAM

1. Accedi alla IAM console (https://console.aws.amazon.com/iam/) con il tuo account amministratore.
2. In Access management (Gestione accessi), scegli Roles (Ruoli).

   È possibile utilizzare i ruoli per creare credenziali a breve termine, operazione consigliata per una maggiore sicurezza. Puoi anche scegliere Utenti per creare credenziali a lungo termine.
3. Scegliere Crea ruolo.
4. Nella procedura guidata di creazione del ruolo, per il tipo di entità attendibile, scegli. Account AWS
5. Mantieni selezionata l'opzione Questo account, quindi scegli Avanti.
6. Per Aggiungi autorizzazioni, scegli Crea politica.

   Si apre una nuova scheda.

   a. Seleziona la JSONscheda, quindi aggiungi le politiche in base alle abilità concesse all'utente della console. AWS Entity Resolution offre le seguenti politiche gestite basate su casi d'uso comuni:

      - AWS politica gestita: AWSEntityResolutionConsoleFullAccess
      - AWS politica gestita: AWSEntityResolutionConsoleReadOnlyAccess

   b. Scegli Avanti: tag, aggiungi tag (opzionale), quindi scegli Avanti: revisione.

   c. Per la politica di revisione, inserisci un nome e una descrizione e consulta il riepilogo.

   d. Scegli Create Policy (Crea policy).

      Hai creato una politica per un membro della collaborazione.

   e. Torna alla scheda originale e in Aggiungi autorizzazioni, inserisci il nome della politica che hai appena creato. (Potrebbe essere necessario ricaricare la pagina).

   f. Seleziona la casella di controllo accanto al nome della politica che hai creato, quindi scegli Avanti.
7. Per Nome, revisione e creazione, inserisci il nome e la descrizione del ruolo.

   a. Rivedi Seleziona entità attendibili, inserisci Account AWS la persona o le persone che assumeranno il ruolo (se necessario).

   b. Controlla le autorizzazioni in Aggiungi autorizzazioni e modificale se necessario.

c. Controlla i tag e aggiungi i tag se necessario.

d. Scegliere Crea ruolo.

Creazione di un ruolo lavorativo nel flusso di lavoro per AWS Entity Resolution

AWS Entity Resolution utilizza un ruolo lavorativo del flusso di lavoro per eseguire un flusso di lavoro. È possibile creare questo ruolo utilizzando la console se si dispone delle IAM autorizzazioni necessarie. Se non disponi `CreateRole` delle autorizzazioni, chiedi all'amministratore di creare il ruolo.

Per creare un ruolo lavorativo nel flusso di lavoro per AWS Entity Resolution

1. Accedi alla IAM console all'indirizzo https://console.aws.amazon.com/iam/con il tuo account amministratore.
2. In Access management (Gestione accessi), scegli Roles (Ruoli).

   È possibile utilizzare i ruoli per creare credenziali a breve termine, operazione consigliata per una maggiore sicurezza. Puoi anche scegliere Utenti per creare credenziali a lungo termine.
3. Scegliere Crea ruolo.
4. Nella procedura guidata di creazione del ruolo, per il tipo di entità attendibile, scegli Criteri di attendibilità personalizzati.
5. Copia e incolla la seguente politica di fiducia personalizzata nell'JSONeditor.

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

```
}
```

6. Scegli Next (Successivo).
7. Per Aggiungi autorizzazioni, scegli Crea politica.

   Viene visualizzata una nuova scheda.

   a. Copia e incolla la seguente politica nell'JSONeditor.

> **Note**
>
> La seguente policy di esempio supporta le autorizzazioni necessarie per leggere le risorse di dati corrispondenti come Amazon AWS Glue S3 e. Tuttavia, potrebbe essere necessario modificare questa politica a seconda di come hai configurato le tue fonti di dati.
> AWS Glue Le tue risorse e le risorse Amazon S3 sottostanti devono essere le stesse Regione AWS di. AWS Entity Resolution
> Non è necessario concedere AWS KMS autorizzazioni se le fonti di dati non sono crittografate o decrittografate.

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

Sostituisci ciascuno *{{user input placeholder}}* con le tue informazioni.

aws-region	Regione AWS delle tue risorse. AWS Glue Le tue risorse, le risorse e AWS KMS le risorse sottostanti di Amazon S3 devono essere le stesse Regione AWS di. AWS Entity Resolution
accountId	Il tuo Account AWS ID.
input-buckets	Bucket Amazon S3 che contengono gli oggetti dati sottostanti da AWS Glue cui AWS Entity Resolution verranno letti.
output-buckets	Bucket Amazon S3 in cui AWS Entity Resolution verranno generati i dati di output.
input-databases	AWS Glue database da cui AWS Entity Resolution leggerà.

b. (Facoltativo) Se il bucket Amazon S3 di input è crittografato utilizzando la KMS chiave del cliente, aggiungi quanto segue:

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

Sostituisci ciascuno *{{user input placeholder}}* con le tue informazioni.

aws-region	Regione AWS delle tue risorse. AWS Glue Le tue risorse, le risorse e AWS KMS le risorse sottostanti di Amazon S3 devono essere le stesse Regione AWS di. AWS Entity Resolution
accountId	Il tuo Account AWS ID.
inputKeys	Chiavi gestite AWS Key Management Service. Se le fonti di input sono crittogra fate, è AWS Entity Resolution necessario decrittografare i dati utilizzando la chiave.

c. (Facoltativo) Se i dati scritti nel bucket Amazon S3 di output devono essere crittografati, aggiungi quanto segue:

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

Sostituisci ciascuno *{{user input placeholder}}* con le tue informazioni.

aws-region	Regione AWS delle tue risorse. AWS Glue Le tue risorse, le risorse e AWS KMS le risorse sottostanti di Amazon S3 devono essere le stesse Regione AWS di. AWS Entity Resolution
accountId	Il tuo Account AWS ID.

outputKeys	Chiavi gestite AWS Key Management Service. Se è necessario crittografare le sorgenti di output, è `AWS Entity Resolution` necessario crittografare i dati di output utilizzando la chiave.

d. (Facoltativo) Se hai un abbonamento con un provider di servizi tramite AWS Data Exchange e desideri utilizzare un ruolo esistente per un flusso di lavoro basato sui servizi del provider, aggiungi quanto segue:

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

Sostituisci ogni *{{user input placeholder}}* con le tue informazioni.

aws-region	Il Regione AWS luogo in cui viene concessa la risorsa del provider. Puoi trovare questo valore nella risorsa ARN sulla AWS Data Exchange console. Ad esempio: `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
datasetId	L'ID del set di dati, trovato sulla AWS Data Exchange console.
revisionId	La revisione del set di dati, trovata sulla console. AWS Data Exchange

assetId	L'ID della risorsa, trovato sulla AWS Data Exchange console.

8. Torna alla scheda originale e in Aggiungi autorizzazioni, inserisci il nome della politica che hai appena creato. (Potrebbe essere necessario ricaricare la pagina).
9. Seleziona la casella di controllo accanto al nome della politica che hai creato, quindi scegli Avanti.
10. Per Nome, revisione e creazione, inserisci il nome e la descrizione del ruolo.

> **Note**
>
> Il nome del ruolo deve corrispondere allo schema delle `passRole` autorizzazioni concesse al membro che può passare `workflow job role` a creare un flusso di lavoro corrispondente.
> Ad esempio, se utilizzi la policy `AWSEntityResolutionConsoleFullAccess` gestita, ricordati di includere `entityresolution` nel tuo ruolo il nome.

    a. Rivedi Seleziona entità attendibili e modificale se necessario.
    b. Controlla le autorizzazioni in Aggiungi autorizzazioni e modificale se necessario.
    c. Controlla i tag e aggiungi i tag se necessario.
    d. Scegliere Crea ruolo.

È stato creato il ruolo lavorativo per AWS Entity Resolution il flusso di lavoro.

Preparare le tabelle dei dati di input

Nel AWS Entity Resolution, ciascuna delle tue tabelle di dati di input contiene record di origine. Questi record contengono identificatori dei consumatori come nome, cognome, indirizzo e-mail o numero di telefono. Questi record di origine possono essere abbinati ad altri record di origine forniti all'interno della stessa o di altre tabelle di dati di input. Ogni record deve avere un Record ID univoco (ID univoco) ed è necessario definirlo come chiave primaria durante la creazione di una mappatura dello schema all'interno. AWS Entity Resolution

Ogni tabella di dati di input è disponibile come AWS Glue tabella supportata da Amazon S3. Puoi utilizzare i tuoi dati proprietari già all'interno di Amazon S3 o importare tabelle di dati da altri provider SaaS di terze parti in Amazon S3. Dopo aver caricato i dati su Amazon S3, puoi utilizzare un AWS Glue crawler per creare una tabella di dati in. AWS Glue Data Catalog Puoi quindi utilizzare la tabella dati come input per. AWS Entity Resolution

Le sezioni seguenti descrivono come preparare dati di prime parti e dati di terze parti.

Argomenti

Preparazione dei dati di input di prime parti

I passaggi seguenti descrivono come preparare i dati di prime parti da utilizzare in un flusso di lavoro di abbinamento basato su regole, in un flusso di lavoro di abbinamento basato sull'apprendimento automatico o in un flussodi lavoro di mappatura degli ID.

Passaggio 1: salvare la tabella dei dati di input in un formato di dati supportato

Se hai già salvato i dati di input di prima parte in un formato di dati supportato, puoi saltare questo passaggio.

Per essere utilizzati AWS Entity Resolution, i dati di input devono essere in un formato che AWS Entity Resolution supporti. AWS Entity Resolution supporta i seguenti formati di dati:

- valore separato da virgole () CSV

- Parquet

Passaggio 2: carica la tabella dei dati di input su Amazon S3

Se disponi già di una tabella di dati di prime parti in Amazon S3, puoi saltare questo passaggio.

> **Note**
>
> I dati di input devono essere archiviati in Amazon Simple Storage Service (Amazon S3) Account AWS nello stesso Regione AWS ambiente in cui desideri eseguire il flusso di lavoro corrispondente.

Per caricare la tabella dei dati di input su Amazon S3

1. Accedi a AWS Management Console e apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Scegli Bucket, quindi scegli un bucket per archiviare la tabella di dati.
3. Scegli Carica, quindi segui le istruzioni.
4. Scegli la scheda Oggetti per visualizzare il prefisso in cui sono archiviati i dati. Prendi nota del nome della cartella.

   È possibile selezionare la cartella per visualizzare la tabella dei dati.

Fase 3: Creare una AWS Glue tabella

I dati di input in Amazon S3 devono essere catalogati AWS Glue e rappresentati come tabella. AWS Glue Per ulteriori informazioni su come creare una AWS Glue tabella con Amazon S3 come input, consulta Working with crawler on the AWS Glue console nella Developer Guide.AWS Glue

> **Note**
>
> AWS Entity Resolution non supporta tabelle partizionate.

In questo passaggio, configuri un crawler AWS Glue che esegue la scansione di tutti i file nel tuo bucket S3 e crea una tabella. AWS Glue

> **Note**
>
> AWS Entity Resolution attualmente non supporta le sedi Amazon S3 registrate con. AWS Lake Formation

Per creare una tabella AWS Glue

1. Accedi a AWS Management Console e apri la AWS Glue console all'indirizzo https://console.aws.amazon.com/glue/.
2. Dalla barra di navigazione, seleziona Crawlers.
3. Seleziona il tuo bucket S3 dall'elenco, quindi scegli Aggiungi crawler.
4. Nella pagina Aggiungi crawler, inserisci un nome per il crawler, quindi scegli Avanti.
5. Continua nella pagina Aggiungi crawler, specificando i dettagli.
6. Nella pagina Scegli un IAM ruolo, scegli Scegli un IAM ruolo esistente, quindi scegli Avanti.

   Puoi anche scegliere Crea un IAM ruolo o chiedere all'amministratore di creare il IAM ruolo, se necessario.
7. Per Crea una pianificazione per questo crawler, mantieni la frequenza predefinita (Esegui su richiesta), quindi scegli Avanti.
8. Per Configura l'output del crawler, accedi al AWS Glue database e scegli Avanti.
9. Controlla tutti i dettagli, quindi scegli Fine.
10. Nella pagina Crawler, seleziona la casella di controllo accanto al tuo bucket S3, quindi scegli Esegui crawler.
11. Al termine dell'esecuzione del crawler, nella barra di AWS Glue navigazione, scegli Database, quindi scegli il nome del database.
12. Nella pagina Database, scegli Tabelle in {nome del database}.

    a. Visualizza le tabelle nel AWS Glue database.

    b. Per visualizzare lo schema di una tabella, seleziona una tabella specifica.

    c. Prendi nota del nome del AWS Glue database e del nome della AWS Glue tabella.

Ora sei pronto per creare una mappatura dello schema. Per ulteriori informazioni, consulta Creazione di una mappatura dello schema.

Preparazione di dati di input di terze parti

I servizi dati di terze parti forniscono identificatori che possono essere abbinati agli identificatori noti.

AWS Entity Resolution attualmente supporta i seguenti servizi di fornitori di dati di terze parti:

Servizi per fornitori di dati

Nome dell'azienda	Disponibile Regioni AWS	Identificatore
LiveRamp	Stati Uniti orientali (Virginia settentrionale) (us-east-1), Stati Uniti orientali (Ohio) (us-east-2) e Stati Uniti occidentali (Oregon) (us-west-2)	ID della rampa
TransUnion	Stati Uniti orientali (Virginia settentrionale) (us-east-1), Stati Uniti orientali (Ohio) (us-east-2) e Stati Uniti occidentali (Oregon) (us-west-2)	TransUnion Individuo e famiglia IDs
ID unificato 2.0	Stati Uniti orientali (Virginia settentrionale) (us-east-1), Stati Uniti orientali (Ohio) (us-east-2) e Stati Uniti occidentali (Oregon) (us-west-2)	Disegna 2 UID

I passaggi seguenti descrivono come preparare i dati di terze parti per utilizzare un flusso di lavoro di abbinamento basato sui servizi del provider o un flusso di lavoro di mappatura degli ID basato sui servizi del provider.

Argomenti

- Fase 1: Abbonarsi a un servizio fornito da un provider su AWS Data Exchange
- Fase 2: Preparare tabelle di dati di terze parti
- Fase 3: Salvate la tabella dei dati di input in un formato di dati supportato
- Fase 4: caricare la tabella dei dati di input su Amazon S3
- Fase 5: Creare una AWS Glue tabella

Fase 1: Abbonarsi a un servizio fornito da un provider su AWS Data Exchange

Se hai un abbonamento a un provider di servizi tramite AWS Data Exchange, puoi eseguire un flusso di lavoro di abbinamento con uno dei seguenti servizi del provider per abbinare i tuoi identificatori noti al tuo provider preferito. I tuoi dati verranno abbinati a una serie di input definiti dal tuo provider preferito.

Per abbonarsi a un servizio offerto da un provider su AWS Data Exchange

1. Visualizza l'elenco dei fornitori su AWS Data Exchange. Sono disponibili i seguenti elenchi di fornitori:
   - LiveRamp
     - LiveRampRisoluzione dell'identità
     - LiveRampTranscodifica
   - TransUnion
     - TransUnion TruAudience Risoluzione e arricchimento delle identità senza trasferimento
     - TransUnion TruAudience Risoluzione delle identità senza trasferimento
   - ID unificato 2.0
     - Risoluzione delle identità con Unified ID 2.0
2. Completa uno dei seguenti passaggi, a seconda del tipo di offerta.
   - Offerta privata: se hai già una relazione con un fornitore, segui la procedura relativa ai prodotti e alle offerte privati nella Guida per l'AWS Data Exchange utente per accettare un'offerta privata su AWS Data Exchange.
   - Porta il tuo abbonamento: se disponi già di un abbonamento dati con un provider, segui la procedura relativa alle offerte Bring Your Own Subscription (BYOS) nella Guida per l'AWS Data Exchange utente per accettare un'BYOSofferta AWS Data Exchange.
3. Dopo esserti abbonato a un servizio fornito da un provider su AWS Data Exchange, puoi creare un flusso di lavoro corrispondente o un flusso di lavoro di mappatura degli ID con quel servizio del provider.

Per ulteriori informazioni su come accedere a un prodotto del fornitore che contieneAPIs, consulta Accedere a un API prodotto nella Guida per l'AWS Data Exchange utente.

Fase 2: Preparare tabelle di dati di terze parti

Ogni servizio di terze parti dispone di una serie diversa di consigli e linee guida per garantire un flusso di lavoro adeguato.

Per preparare tabelle di dati di terze parti, consulta la seguente tabella:

Servizio del fornitore	È necessario un ID univoco?	Azioni
LiveRamp	Sì	Assicurati quanto segue: • L'ID univoco può essere il tuo identificatore pseudonimo o un ID di riga. • Il formato e la normalizzazione del file di input dei dati sono in linea con le linee guida. LiveRamp Per ulteriori informazioni sulle linee guida di formattazione dei file di input per il flusso di lavoro corrispondente, consulta Perform Identity Resolution Through ADX nella documentazione. LiveRamp Per ulteriori informazioni sulle linee guida per la formattazione dei file di input per il flusso di lavoro di mappatura degli ID, consulta Perform Transcoding Through nella documentazione. ADX LiveRamp

Servizio del fornitore	È necessario un ID univoco?	Azioni

TransUnion	Sì	Verificate quanto segue:
		• Esiste un ID univoco per l'arricchimento TransUnion dei dati.
		Note
		Gli attributi di trasmissione possono persistere in input e output a. TransUnion Chiavi E domestiche e HHID sono specifiche dello spazio dei nomi del client.
		• **`Phone number`** deve essere composto da 10 cifre, senza caratteri speciali come spazi o trattini.
		• **`Addresses`** deve essere suddiviso in
		  • una singola riga di indirizzo (combina le righe di indirizzo 1 e 2, se presenti)
		  • città
		  • zip (o zip plus4), senza caratteri speciali come spazi o trattini
		  • stato, specificato come codice a 2 lettere 3

Servizio del fornitore	È necessario un ID univoco?	Azioni
		• **`Email addresses`** deve essere in testo semplice. • **`First Name`**può essere minuscolo o maiuscolo, i soprannomi sono supportati, ma i titoli e i suffissi devono essere esclusi. • **`Last Name`**può essere minuscolo o maiuscolo, le iniziali centrali devono essere escluse.

Servizio del fornitore	È necessario un ID univoco?	Azioni
ID unificato 2.0	Sì	Assicurati quanto segue: • L'ID univoco non può essere un hash. • UID2supporta sia l'e-mail che il numero di telefono per la UID2 generazione. Tuttavia, se entrambi i valori sono presenti nella mappatura dello schema, il flusso di lavoro duplica ogni record nell'output. Un record utilizza l'e-mail per la UID2 generazione e il secondo record utilizza il numero di telefono. Se i dati includono una combinazione di e-mail e numeri di telefono e non desideri che i record vengano duplicati nell'output, l'approccio migliore consiste nel creare un flusso di lavoro separato per ciascuno di essi, con mappature dello schema separate. In questo scenario, esegui i passaggi due volte: crea un flusso di lavoro per le e-mail e uno separato per i numeri di telefono. **Note** Un indirizzo email o un numero di telefono specifico

Servizio del fornitore	È necessario un ID univoco?	Azioni
		, in un momento specifico , restituisce lo stesso UID2 valore grezzo, indipendentemente da chi ha effettuato la richiesta. UID2sLe materie crude si ottengono aggiungendo i sali contenuti nei secchi di sale, che vengono fatti ruotare all'incirca una volta all'anno, facendo UID2 ruotare anche la materia prima. I diversi secchi di sale ruotano in momenti diversi durante l'anno. AWS Entity Resolution attualmente non tiene traccia della rotazione dei secchi salati e crudiUID2s, per cui si consiglia di rigenerare quotidianamente quello crudo. UID2s Per ulteriori informazioni, vedi Con che frequenza deve UID2s essere aggiornato per gli aggiornamenti incrementali? nella documentazione UID 2.0.

Fase 3: Salvate la tabella dei dati di input in un formato di dati supportato

Se hai già salvato i dati di input di terze parti in un formato di dati supportato, puoi saltare questo passaggio.

Per essere utilizzati AWS Entity Resolution, i dati di input devono essere in un formato che AWS Entity Resolution supporti. AWS Entity Resolution supporta i seguenti formati di dati:

- valore separato da virgole () CSV

> **Note**
>
> LiveRamp supporta solo file. CSV

- Parquet

Fase 4: caricare la tabella dei dati di input su Amazon S3

Se hai già una tabella di dati di terze parti in Amazon S3, puoi saltare questo passaggio.

> **Note**
>
> I dati di input devono essere archiviati in Amazon Simple Storage Service (Amazon S3) Account AWS nello stesso Regione AWS ambiente in cui desideri eseguire il flusso di lavoro corrispondente.

Per caricare la tabella dei dati di input su Amazon S3

1. Accedi a AWS Management Console e apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Scegli Bucket, quindi scegli un bucket per archiviare la tabella di dati.
3. Scegli Carica, quindi segui le istruzioni.
4. Scegli la scheda Oggetti per visualizzare il prefisso in cui sono archiviati i dati. Prendi nota del nome della cartella.

   È possibile selezionare la cartella per visualizzare la tabella dei dati.

Fase 5: Creare una AWS Glue tabella

I dati di input in Amazon S3 devono essere catalogati AWS Glue e rappresentati come tabella. AWS Glue Per ulteriori informazioni su come creare una AWS Glue tabella con Amazon S3 come input, consulta Working with crawler on the AWS Glue console nella Developer Guide.AWS Glue

> **Note**
>
> AWS Entity Resolution non supporta tabelle partizionate.

In questo passaggio, configuri un crawler AWS Glue che esegue la scansione di tutti i file nel tuo bucket S3 e crea una tabella. AWS Glue

> **Note**
>
> AWS Entity Resolution attualmente non supporta le sedi Amazon S3 registrate con. AWS Lake Formation

Per creare una tabella AWS Glue

1. Accedi a AWS Management Console e apri la AWS Glue console all'indirizzo https://console.aws.amazon.com/glue/.
2. Dalla barra di navigazione, seleziona Crawlers.
3. Seleziona il tuo bucket S3 dall'elenco, quindi scegli Aggiungi crawler.
4. Nella pagina Aggiungi crawler, inserisci un nome per il crawler, quindi scegli Avanti.
5. Continua nella pagina Aggiungi crawler, specificando i dettagli.
6. Nella pagina Scegli un IAM ruolo, scegli Scegli un IAM ruolo esistente, quindi scegli Avanti.

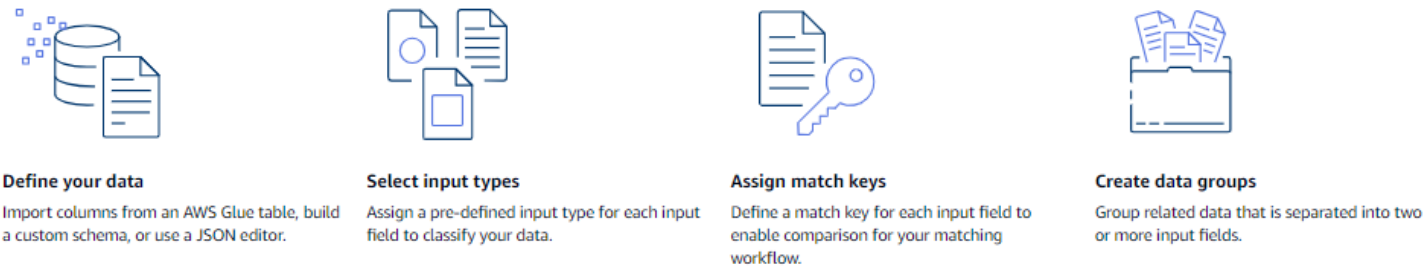
   Puoi anche scegliere Crea un IAM ruolo o chiedere all'amministratore di creare il IAM ruolo, se necessario.
7. Per Crea una pianificazione per questo crawler, mantieni la frequenza predefinita (Esegui su richiesta), quindi scegli Avanti.
8. Per Configura l'output del crawler, accedi al AWS Glue database e scegli Avanti.
9. Esamina tutti i dettagli, quindi scegli Fine.

10. Nella pagina Crawler, seleziona la casella di controllo accanto al tuo bucket S3, quindi scegli Esegui crawler.
11. Al termine dell'esecuzione del crawler, nella barra di AWS Glue navigazione, scegli Database, quindi scegli il nome del database.
12. Nella pagina Database, scegli Tabelle in {nome del database}.
    a. Visualizza le tabelle nel AWS Glue database.
    b. Per visualizzare lo schema di una tabella, seleziona una tabella specifica.
    c. Prendi nota del nome del AWS Glue database e del nome della AWS Glue tabella.

Definire i dati di input utilizzando la mappatura dello schema

Una mappatura dello schema definisce i dati di input che desideri risolvere. Fornisce inoltre metadati sui dati di input, come i tipi di attributi delle colonne (tipi di input) e le colonne su cui eseguire la corrispondenza.

Quando si crea una mappatura dello schema, si definiscono innanzitutto i campi di input e i tipi di input, quindi si definiscono le chiavi di corrispondenza e i dati relativi al gruppo. Il diagramma seguente riassume come creare una mappatura dello schema.



Prima di creare una mappatura dello schema, è necessario impostare AWS Entity Resolution e preparare le tabelle di dati. Per ulteriori informazioni, consulta Configurare AWS Entity Resolution e Preparare le tabelle dei dati di input.

Dopo aver creato una mappatura dello schema, è possibile eseguire una delle seguenti operazioni:

- Crea un flusso di lavoro corrispondente per trovare le corrispondenze tra diversi input di dati.
- Crea una fonte di namespace ID da utilizzare in un flusso di lavoro di mappatura degli ID per tradurre i dati da un'origine a una destinazione.
- Crea un flusso di lavoro di mappatura degli ID all'interno dello stesso Account AWS utilizzando la mappatura dello schema come origine.

Argomenti

Creazione di una mappatura dello schema

Questa procedura descrive il processo di creazione di una mappatura dello schema utilizzando la AWS Entity Resolution console.

Esistono tre modi per creare una mappatura dello schema:

- Importa dati di input esistenti utilizzando l' AWS Glue opzione Importa da: utilizza questo metodo di creazione per definire i campi di input a partire da colonne precompilate da una AWS Glue tabella utilizzando un flusso guidato.
- Definizione manuale dei dati di input utilizzando l'opzione Crea schema personalizzato: utilizzate questo metodo di creazione per definire manualmente i campi di input utilizzando un flusso guidato.
- Crea manualmente utilizzando l'opzione Usa JSON editor: utilizza un JSON editor per creare, utilizzare un campione o importare manualmente dati di input esistenti.

> **Note**
>
> I campi ID univoco e input non sono disponibili con questa opzione.

Import from AWS Glue

Per creare la mappatura dello schema importando dati di input esistenti da AWS Glue

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli Schema mappings.
3. Nella pagina Mappature dello schema, nell'angolo in alto a destra, scegli Crea mappatura dello schema.
4. Per il passaggio 1: specificare i dettagli dello schema, procedi come segue:
    a. Per Nome e metodo di creazione, immettere un nome di mappatura dello schema e una descrizione opzionale.
    b. Per Metodo di creazione, scegliete Importa da AWS Glue.
    c. Scegli il AWS Glue database dal menu a discesa, quindi scegli la AWS Glue tabella dal menu a discesa.

Per creare una nuova tabella, vai alla AWS Glue console. https://console.aws.amazon.com/glue/ Per ulteriori informazioni, consulta le AWS Glue tabelle nella Guida AWS Glue per l'utente.

d. Per ID univoco, specifica la colonna che fa riferimento in modo distinto a ciascuna riga dei dati.

Example

Ad esempio: **`Primary_key`**, **`Row_ID`** o **`Record_ID`**.

> **Note**
>
> La colonna ID univoco è obbligatoria. L'ID univoco deve essere un identificatore univoco all'interno di una singola tabella. Tuttavia, in tabelle diverse, l'ID univoco può avere valori duplicati. Se l'ID univoco non è specificato, non è univoco all'interno della stessa fonte o si sovrappone in termini di nomi di attributi tra le fonti, AWS Entity Resolution rifiuta il record quando viene eseguito il flusso di lavoro corrispondente. Se si utilizza questa mappatura dello schema in un flusso di lavoro di abbinamento basato su regole, l'ID univoco non deve superare i 38 caratteri.

e. Per i campi di input, scegli da 1 a 25 colonne da utilizzare per la corrispondenza e per il passaggio facoltativo.

   i. Seleziona Aggiungi colonne da esaminare se desideri specificare le colonne che non vengono utilizzate per la corrispondenza.

   ii. In Pass through (facoltativo), scegli le colonne da includere come colonne passanti.

f. (Facoltativo) Se desideri abilitare i tag per la risorsa, scegli Aggiungi nuovo tag, quindi inserisci la coppia Chiave e Valore.

g. Scegli Next (Successivo).

5. Per il passaggio 2: mappa i campi di input, definisci i campi di input che desideri utilizzare per la corrispondenza e per il passaggio facoltativo.

   a. Per i campi di input da abbinare, per ogni campo di input, specifica il tipo di input, la chiave di corrispondenza e lo stato di hashing.

Il tipo di input consente di classificare i dati. La chiave Match consente il confronto dei campi di input con il flusso di lavoro corrispondente. Lo stato Hashing indica se il valore della colonna per quel campo di input è in formato hash o non crittografato.

> **Note**
>
> Se stai creando una mappatura dello schema da utilizzare con la tecnica di abbinamento basata sui servizi del LiveRamp provider, puoi:
>
> - Specificate il tipo di input come ID. LiveRamp
> - Specificate il campo del nome come campi multipli (ad esempio**`first_name`**,**`last_name`**) o in un unico campo.
> - Specificate il campo dell'indirizzo come campi multipli (ad esempio**`address1`**,**`address2`**) o in un unico campo.
>
>   Se corrisponde a un indirizzo, è necessario un codice postale.
> - Includi email o telefono con nome e quei campi possono corrispondere all'indirizzo.

> **Note**
>
> Se stai creando una mappatura dello schema da utilizzare con il flusso di lavoro di abbinamento basato sull'apprendimento automatico, il set di dati deve contenere almeno uno dei seguenti attributi:**`phonenumber`**,,,**`emailaddress`**, **`fullname`** o. **`addresses`** **`birthdate`**
> Non specificate il tipo di input per nessuno di questi attributi come stringa personalizzata.

b. Facoltativo) Per i campi di input for pass through, aggiungi i campi di input che non verranno abbinati e lo stato di hashing corrispondente.

   Lo stato di hashing indica se il valore della colonna per quel campo di input è in formato hash o non crittografato.

c. Scegli Next (Successivo).

6. Per il passaggio 3: Raggruppa i dati, procedi come segue:

   a. Scegli i campi Nome correlati, quindi inserisci il nome del gruppo e la chiave Match.

      Example

      Ad esempio, scegli i campi di input e **`First name`** **`Middle name`** **`Last name`**, e quindi inserisci un nome di gruppo chiamato «**`Full name`**» e una chiave di corrispondenza chiamata «**`Full name`**» per abilitare il confronto.

   b. Scegli i campi relativi all'indirizzo, quindi inserisci il nome del gruppo e la chiave Match.

      Example

      Ad esempio, scegli i campi di input e **`Home street address 1`** **`Home street address 2`** **`Home city`**, e quindi inserisci un nome di gruppo chiamato «**`Shipping address`**» e una chiave Match chiamata «**`Shipping address`**» per abilitare il confronto.

   c. Scegli i campi relativi al numero di telefono, quindi inserisci il nome del gruppo e il tasto Match.

      Example

      Ad esempio, scegli i campi di immissione **`Home phone 1`** **`Home phone 2`** **`Cell phone`**, e, quindi inserisci un nome di gruppo chiamato «**`Shipping phone number`**» e una chiave di corrispondenza chiamata «**`Shipping phone number`**» per abilitare il confronto.

      Se disponi di più di un tipo di dati, puoi aggiungere altri gruppi.

   d. Scegli Next (Successivo).

7. Per il passaggio 4: revisione e creazione, procedi come segue:

   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

   b. Scegli Crea mappatura dello schema.

      > **Note**
      >
      > Non è possibile modificare una mappatura dello schema dopo averla associata a un flusso di lavoro. È possibile clonare una mappatura dello schema se si

desidera utilizzare una configurazione esistente per creare una nuova mappatura dello schema.

Dopo aver creato la mappatura dello schema, sei pronto per creare un flusso di lavoro corrispondente o creare uno spazio dei nomi ID.

Build custom schema

Per creare una mappatura dello schema utilizzando l'opzione Crea schema personalizzato

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli Schema mappings.
3. Nella pagina Mappature dello schema, nell'angolo in alto a destra, scegli Crea mappatura dello schema.
4. Per il passaggio 1: specificare i dettagli dello schema, procedi come segue:
   a. Per il nome e il metodo di creazione, immettere un nome di mappatura dello schema e una descrizione facoltativa.
   b. Per Metodo di creazione, scegli Crea schema personalizzato.
   c. Per ID univoco, inserisci un ID univoco per identificare ogni riga dei tuoi dati.

      Example

      Ad esempio: **`Primary_key`**, **`Row_ID`** o **`Record_ID`**.

      > **Note**
      >
      > La colonna ID univoco è obbligatoria. L'ID univoco deve essere un identificatore univoco all'interno di una singola tabella. Tuttavia, in tabelle diverse, l'ID univoco può avere valori duplicati. Se l'ID univoco non è specificato, non è univoco all'interno della stessa fonte o si sovrappone in termini di nomi di attributi tra le fonti, AWS Entity Resolution rifiuta il record quando viene eseguito il flusso di lavoro corrispondente. Se si utilizza questa mappatura dello schema in un flusso di lavoro di abbinamento basato su regole, l'ID univoco non deve superare i 38 caratteri.

d. (Facoltativo) Se desideri abilitare i tag per la risorsa, scegli Aggiungi nuovo tag, quindi inserisci la coppia Chiave e Valore.

e. Scegli Next (Successivo).

5. Per il passaggio 2: mappa i campi di input, definisci i campi di input che desideri utilizzare per la corrispondenza e per il passaggio facoltativo.

a. Per i campi di input da abbinare, aggiungi un campo di input e il tipo di input, la chiave di corrispondenza e lo stato di hashing corrispondenti.

Puoi aggiungere fino a 25 campi di input.

Il tipo di input consente di classificare i dati. La chiave Match consente il confronto dei campi di input con il flusso di lavoro corrispondente. Lo stato Hashing indica se il valore della colonna per quel campo di input è in formato hash o non crittografato.

> **Note**
>
> Se stai creando una mappatura dello schema da utilizzare con la tecnica di abbinamento basata sui servizi del LiveRamp provider, puoi specificare il tipo di input come ID. LiveRamp Se desideri includere PII dati nell'output, devi specificare il tipo di input come stringa personalizzata.

> **Note**
>
> Se state creando una mappatura dello schema da utilizzare con il flusso di lavoro di abbinamento basato sull'apprendimento automatico, il set di dati deve contenere almeno uno dei seguenti attributi:**`phonenumber`**,,**`emailaddress`**, **`fullname`** o. **`addresses`** **`birthdate`**
> Non specificate il tipo di input per nessuno di questi attributi come stringa personalizzata.

b. (Facoltativo) Per i campi di input for pass through, aggiungi i campi di input che non verranno abbinati e lo stato di hashing corrispondente.

c. Scegli Next (Successivo).

6. Per la fase 3: Raggruppa i dati:

a. Scegli i campi Nome correlati, quindi inserisci il nome del gruppo e la chiave Match.

   Example

   Ad esempio, scegli i campi di input e **`First name`** **`Middle name`** **`Last name`**, e quindi inserisci un nome di gruppo chiamato «**`Full name`**» e una chiave di corrispondenza chiamata «**`Full name`**» per abilitare il confronto.

b. Scegli i campi relativi all'indirizzo, quindi inserisci il nome del gruppo e la chiave Match.

   Example

   Ad esempio, scegli i campi di input e **`Home street address 1`** **`Home street address 2`** **`Home city`**, e quindi inserisci un nome di gruppo chiamato «**`Shipping address`**» e una chiave Match chiamata «**`Shipping address`**» per abilitare il confronto.

c. Scegli i campi relativi al numero di telefono, quindi inserisci il nome del gruppo e il tasto Match.

   Example

   Ad esempio, scegli i campi di immissione **`Home phone 1`** **`Home phone 2`** **`Cell phone`**, e, quindi inserisci un nome di gruppo chiamato «**`Shipping phone number`**» e una chiave di corrispondenza chiamata «**`Shipping phone number`**» per abilitare il confronto.

   Se disponi di più di un tipo di dati, puoi aggiungere altri gruppi.

d. Scegli Next (Successivo).

7. Per il passaggio 4: revisione e creazione, procedi come segue:

   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

   b. Scegli Crea mappatura dello schema.

   > **Note**
   >
   > Non è possibile modificare una mappatura dello schema dopo averla associata a un flusso di lavoro. È possibile clonare una mappatura dello schema se si

desidera utilizzare una configurazione esistente per creare una nuova mappatura dello schema.

Dopo aver creato la mappatura dello schema, sei pronto per creare un flusso di lavoro corrispondente o creare uno spazio dei nomi ID.

JSON Editor

Per creare una mappatura dello schema utilizzando l'editor JSON

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli Schema mappings.
3. Nella pagina Mappature dello schema, nell'angolo in alto a destra, scegli Crea mappatura dello schema.
4. Per il passaggio 1: specificare i dettagli dello schema, procedi come segue:
    a. Per il nome e il metodo di creazione, immettere un nome di mappatura dello schema e una descrizione facoltativa.
    b. Per Metodo di creazione, scegli Usa JSON editor.
    c. (Facoltativo) Se desideri abilitare i tag per la risorsa, scegli Aggiungi nuovo tag, quindi inserisci la coppia Chiave e Valore.
    d. Scegli Next (Successivo).
5. Per il passaggio 2: Specificare la mappatura:
    a. Inizia a creare lo schema nell'JSONeditor o scegli una delle seguenti opzioni in base al tuo obiettivo:

Il tuo obiettivo	Opzione consigliata
Inizia a creare la mappatura dello schema	Inserite il campione JSON e modificate le informazioni secondo necessità.
Usa un JSON file esistente	Importa da file

    b. Scegli Next (Successivo).

6. Per la fase 3: Rivedi e crea:

   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

   b. Scegli Crea mappatura dello schema.

> **Note**
>
> Non è possibile modificare una mappatura dello schema dopo averla associata a un flusso di lavoro. È possibile clonare una mappatura dello schema se si desidera utilizzare una configurazione esistente per creare una nuova mappatura dello schema.

Dopo aver creato la mappatura dello schema, sei pronto per creare un flusso di lavoro corrispondente o creare uno spazio dei nomi ID.

Clonazione di una mappatura dello schema

È possibile clonare una mappatura dello schema se si desidera utilizzare una configurazione esistente per creare una nuova mappatura dello schema.

Per clonare una mappatura dello schema:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli Schema mappings.
3. Scegli la mappatura dello schema.
4. Seleziona Clona.
5. Nella pagina Specificare i dettagli dello schema, apporta le modifiche necessarie, quindi scegli Avanti.
6. Nella pagina Scegli la tecnica corrispondente, apporta le modifiche necessarie, quindi scegli Avanti.
7. Nella pagina Campi di immissione della mappa, apporta le modifiche necessarie, quindi scegli Avanti.
8. Nella pagina Dati del gruppo, apporta le modifiche necessarie, quindi scegli Avanti.

9. Nella pagina Rivedi e salva, apporta le modifiche necessarie, quindi scegli Clona mappatura dello schema.

Modifica di una mappatura dello schema

È possibile modificare una mappatura dello schema solo prima di associarla a un flusso di lavoro. Dopo aver associato una mappatura dello schema a un flusso di lavoro, non è possibile modificarla. È possibile clonare una mappatura dello schema se si desidera utilizzare una configurazione esistente per creare una nuova mappatura dello schema.

Per modificare una mappatura dello schema:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli Schema mappings.
3. Scegli la mappatura dello schema.
4. Scegli Modifica.
5. Nella pagina Specificare i dettagli dello schema, apporta le modifiche necessarie, quindi scegli Avanti.
6. Nella pagina Scegli la tecnica corrispondente, apporta le modifiche necessarie, quindi scegli Avanti.
7. Nella pagina Campi di immissione della mappa, apporta le modifiche necessarie, quindi scegli Avanti.
8. Nella pagina Dati del gruppo, apporta le modifiche necessarie, quindi scegli Avanti.
9. Nella pagina Rivedi e salva, apporta le modifiche necessarie, quindi scegli Modifica mappatura dello schema.

Eliminazione di una mappatura dello schema

Non è possibile eliminare una mappatura dello schema quando è associata a un flusso di lavoro corrispondente. È innanzitutto necessario rimuovere la mappatura dello schema da tutti i flussi di lavoro corrispondenti associati prima di poterla eliminare.

Per eliminare una mappatura dello schema:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli Schema mappings.
3. Scegli la mappatura dello schema.
4. Scegli Elimina.
5. Conferma l'eliminazione, quindi scegli Elimina.

Definire i dati di input utilizzando uno spazio dei nomi ID

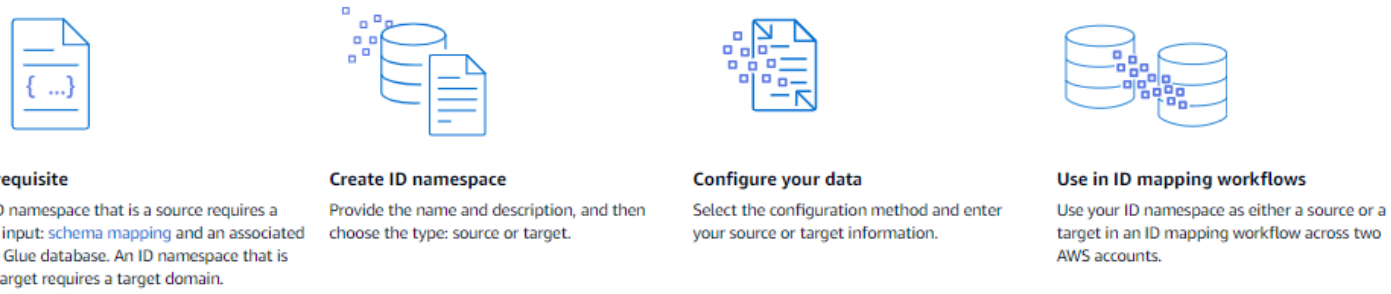
Un namespace ID è un involucro attorno alla tabella dei dati di input. Utilizzi uno spazio dei nomi ID per fornire metadati che spiegano i dati di input e le tecniche di abbinamento e come utilizzarli in un flusso di lavoro di mappatura degli ID.

Esistono due tipi di namespace ID: Source e Target.

- L'origine contiene le configurazioni per i dati di origine che vengono AWS Entity Resolution elaborati in un flusso di lavoro di mappatura degli ID.
- La destinazione contiene una configurazione dei dati di destinazione in cui si risolvono tutte le fonti.

È possibile definire i dati di input che si desidera risolvere tra due dati Account AWS in un flusso di lavoro di mappatura degli ID. Un partecipante crea un'origine dello spazio dei nomi ID e un altro partecipante crea una destinazione dello spazio dei nomi ID. Dopo che i partecipanti hanno creato l'origine e la destinazione, è possibile eseguire un flusso di lavoro di mappatura degli ID per tradurre i dati dall'origine alla destinazione.

Il diagramma seguente riassume come creare uno spazio dei nomi ID da utilizzare in un flusso di lavoro di mappatura degli ID.



Le sezioni seguenti descrivono come creare un'origine dello spazio dei nomi ID e una destinazione dello spazio dei nomi ID.

Argomenti

- Origine dello spazio dei nomi ID
- ID (destinazione dello spazio dei nomi)
- Modifica di uno spazio dei nomi ID
- Eliminazione di un namespace ID

- Aggiungere o aggiornare una politica delle risorse per un namespace ID

Origine dello spazio dei nomi ID

L'origine dello spazio dei nomi ID è l'origine dei dati in un flusso di lavoro di mappatura degli ID.

Prima di creare una fonte di namespace ID, è necessario creare una mappatura dello schema o un flusso di lavoro corrispondente, a seconda del caso d'uso. Per ulteriori informazioni, consulta Creazione di una mappatura dello schema e Abbina i dati di input utilizzando un flusso di lavoro corrispondente.

Dopo aver creato un'origine dello spazio dei nomi ID, è possibile utilizzarla insieme a una destinazione dello spazio dei nomi ID in un flusso di lavoro di mappatura degli ID. Per ulteriori informazioni, consulta Mappa i dati di input utilizzando un flusso di lavoro di mappatura degli ID.

Esistono due modi per creare un'origine dello spazio dei nomi ID nella AWS Entity Resolution console: il metodo basato su regole o il metodo dei servizi del provider.

Argomenti

- Creazione di una sorgente di namespace ID (basata su regole)
- Creazione di una sorgente di namespace ID (provider services)

Creazione di una sorgente di namespace ID (basata su regole)

Questo argomento descrive il processo di creazione di un'origine dello spazio dei nomi ID utilizzando il metodo basato su regole. Questo metodo utilizza regole di corrispondenza per tradurre i dati di prime parti da un'origine a una destinazione in un flusso di lavoro di mappatura degli ID.

> **Note**
>
> Se i dati di input sono l'origine, devono avere una mappatura dello schema e un database associato. AWS Glue

Per creare una sorgente di namespace ID (basata su regole)

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.

2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli ID namespaces.
3. Nella pagina dei namespace ID, nell'angolo in alto a destra, scegli Crea spazio dei nomi ID.
4. Per i dettagli, procedi come segue:
   a. Per il nome dello spazio dei nomi ID, immettete un nome univoco.
   b. (Facoltativo) In Descrizione, immettere una descrizione facoltativa.
   c. Per il tipo di namespace ID, scegli Sorgente.
5. Per il metodo dello spazio dei nomi ID, scegliete Basato su regole.
6. Per l'immissione dei dati, scegli il tipo di input che desideri utilizzare e quindi esegui le azioni consigliate.

Input type (Tipo input)	Azioni consigliate
Una mappatura dello schema esistente	1. Scegli la mappatura dello schema. 2. Scegli il AWS Glue database, la AWS Glue tabella e la mappatura dello schema dall'elenco a discesa. È possibile aggiungere fino a 20 input di dati.
Un flusso di lavoro corrispondente esistente	1. Scegli il flusso di lavoro Matching. 2. Scegli l'account associato allo spazio dei nomi ID: il tuo Account AWS o un altro. Account AWS 3. A seconda del tipo di account, seleziona il nome del flusso di lavoro Matching o inserisci il flusso di lavoro Matching. ARN

7. Per i parametri della regola, procedi come segue.
   a. Specificate i controlli delle regole scegliendo una delle seguenti opzioni in base al vostro obiettivo.

Il tuo obiettivo	Opzione consigliata
Consenti regole sia dall'origine che dalla destinazione	Nessuna preferenza
Scegli se un'origine, una destinazione o entrambe possono fornire regole in un flusso di lavoro di mappatura degli ID	Regole limitate

I controlli delle regole devono essere compatibili tra l'origine e la destinazione da utilizzare in un flusso di lavoro di mappatura degli ID. Ad esempio, se lo spazio dei nomi dell'ID di origine limita le regole alla destinazione ma lo spazio dei nomi dell'ID di destinazione limita le regole all'origine, viene generato un errore.

b. Specificate le regole di corrispondenza scegliendo una delle seguenti opzioni in base al tipo di input dei dati.

Tipo di input dei dati	Azione consigliata
Mappatura dello schema	Scegli Aggiungi un'altra regola per aggiunger e una regola corrispondente. Puoi applicare fino a 25 regole di abbinamen to per definire i criteri di abbinamento.
Flusso di lavoro corrispondente	Scegli Usa le regole del flusso di lavoro corrispondente o Fornisci nuove regole per definire le tue regole di abbinamento.

8. Per i parametri di confronto e abbinamento, procedi come segue.

   a. Specificate il tipo di confronto scegliendo una delle seguenti opzioni in base al vostro obiettivo.

Il tuo obiettivo	Opzione consigliata
Consenti l'utilizzo di qualsiasi tipo di confronto quando crei il flusso di lavoro di mappatura degli ID.	Nessuna preferenza
Trova qualsiasi combinazione di corrispondenze tra i dati archiviati in più campi di input, indipendentemente dal fatto che i dati si trovino nello stesso campo di input o in un campo di input diverso.	Campi di input multipli
Limita il confronto all'interno di un singolo campo di input, quando dati simili memorizzati in più campi di input non devono corrispondere.	Campo di input singolo

b. Specificate il tipo di record matching scegliendo una delle seguenti opzioni in base al vostro obiettivo.

Il tuo obiettivo	Opzione consigliata
Consenti l'utilizzo di qualsiasi tipo di confronto quando crei il flusso di lavoro di mappatura degli ID.	Nessuna preferenza
Limita il tipo di corrispondenza dei record in modo da memorizzare solo un record corrispondente nell'origine per ogni record corrispondente nella destinazione quando crei il flusso di lavoro di mappatura degli ID.	Corrispondenza limitata dei record e Una fonte per un unico obiettivo

Il tuo obiettivo	Opzione consigliata
Limita il tipo di corrispondenza dei record per memorizzare tutti i record corrispondenti nell'origine per ogni record corrispondente nella destinazione quando crei il flusso di lavoro di mappatura degli ID.	Corrispondenza limitata dei record e Molte fonti per un unico obiettivo

> **Note**
>
> È necessario specificare limitazioni compatibili per i namespace degli ID di origine e di destinazione. Ad esempio, se lo spazio dei nomi dell'ID di origine limita le regole alla destinazione ma lo spazio dei nomi dell'ID di destinazione limita le regole all'origine, viene generato un errore.

9. Specificate le autorizzazioni di accesso al servizio scegliendo il nome del ruolo di servizio esistente dall'elenco a discesa.
10. (Facoltativo) Per abilitare i tag per la risorsa, scegli Aggiungi nuovo tag, quindi inserisci la coppia Chiave e Valore.
11. Scegliete Crea spazio dei nomi ID.

Viene creata la fonte del namespace ID. Ora sei pronto per creare un target ID namespace.

Creazione di una sorgente di namespace ID (provider services)

Questo argomento descrive il processo di creazione di un'origine dello spazio dei nomi ID utilizzando il metodo Provider services. Questo metodo utilizza un servizio provider chiamato. LiveRamp LiveRamp traduce i dati codificati di terze parti da un'origine a una destinazione durante un flusso di lavoro di mappatura degli ID.

> **Note**
>
> Se i dati di input sono l'origine, devono disporre di una mappatura dello schema e di un database associato. AWS Glue

Per creare una fonte di namespace ID (provider services)

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli ID namespaces.
3. Nella pagina dei namespace ID, nell'angolo in alto a destra, scegli Crea spazio dei nomi ID.
4. Per i dettagli, procedi come segue:

   a. Per il nome dello spazio dei nomi ID, immettete un nome univoco.

   b. (Facoltativo) In Descrizione, immettere una descrizione facoltativa.

   c. Per il tipo di namespace ID, scegli Sorgente.
5. Per il metodo dello spazio dei nomi ID, scegli Provider services.

   > **Note**
   >
   > AWS Entity Resolution attualmente offre il servizio LiveRamp provider come metodo ID namespace. Se hai un abbonamento a LiveRamp, lo stato appare come Sottoscritto. Per ulteriori informazioni su come sottoscrivere un abbonamento LiveRamp, consultaFase 1: Abbonarsi a un servizio fornito da un provider su AWS Data Exchange.
6. Per l'immissione dei dati, scegli il AWS Glue database, la AWS Glue tabella e la mappatura dello schema dall'elenco a discesa.

   È possibile aggiungere fino a 20 input di dati.
7. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione e intraprendi l'azione consigliata.

Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. Il nome del ruolo di servizio predefinito è`entityresolution-id-mapping-workflow-<timestamp>` .

Opzione	Azione consigliata
	È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. Se i dati di input sono crittografati, scegli l'opzione Questi dati sono crittografati da una KMS chiave. Quindi, inserisci una AWS KMS chiave che viene utilizzata per decrittografare i dati in ingresso.
Utilizza un ruolo di servizio esistente	Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. Se disponi delle autorizzazioni per elencare i ruoli, viene visualizzato l'elenco dei ruoli. Se non disponi delle autorizzazioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibi le. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiungere le autorizzazioni necessarie.

8. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

9. Scegliete Crea spazio dei nomi ID.

Viene creata la fonte del namespace ID. Ora sei pronto per creare un target ID namespace.

ID (destinazione dello spazio dei nomi)

La destinazione dello spazio dei nomi ID è la destinazione dei dati in un flusso di lavoro di mappatura degli ID. Tutte le fonti raggiungono la destinazione.

Prima di creare un target ID namespace, è necessario creare un workflow corrispondente o sottoscrivere un abbonamento a un provider service (LiveRamp), a seconda del caso d'uso. Per ulteriori informazioni, consulta Abbina i dati di input utilizzando un flusso di lavoro corrispondente e Fase 1: Abbonarsi a un servizio fornito da un provider su AWS Data Exchange.

Dopo aver creato un target ID namespace, potete utilizzarlo insieme a un'origine dello spazio dei nomi ID in un flusso di lavoro di mappatura degli ID. Per ulteriori informazioni, consulta Mappa i dati di input utilizzando un flusso di lavoro di mappatura degli ID.

Esistono due modi per creare una destinazione dello spazio dei nomi ID nella AWS Entity Resolution console: il metodo basato su regole o il metodo dei servizi del provider.

Argomenti

- Creazione di un target di namespace ID (metodo basato su regole)
- Creazione di un target per lo spazio dei nomi ID (metodo dei servizi del fornitore)

Creazione di un target di namespace ID (metodo basato su regole)

Questo argomento descrive il processo di creazione di un target di namespace ID utilizzando il metodo basato su regole. Questo metodo utilizza regole di corrispondenza per tradurre i dati di prime parti da una sorgente a una destinazione durante un flusso di lavoro di mappatura degli ID.

Per creare un target ID namespace (basato su regole)

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli ID namespaces.
3. Nella pagina dei namespace ID, nell'angolo in alto a destra, scegli Crea spazio dei nomi ID.
4. Per i dettagli, procedi come segue:

a. Per il nome dello spazio dei nomi ID, immettete un nome univoco.

b. (Facoltativo) In Descrizione, immettere una descrizione facoltativa.

c. Per il tipo di namespace ID, scegli Target.

5. Per il metodo dello spazio dei nomi ID, scegli Basato su regole.

6. Per l'immissione dei dati, in Flusso di lavoro corrispondente, procedi come segue.

a. Scegli l'account associato allo spazio dei nomi ID: il tuo Account AWS o un altro. Account AWS

b. A seconda del tipo di account, seleziona il nome del flusso di lavoro Matching o inserisci il flusso di lavoro Matching. ARN

7. Per i parametri della regola, procedi come segue.

a. Specificate i controlli delle regole scegliendo una delle seguenti opzioni in base al vostro obiettivo.

Il tuo obiettivo	Opzione consigliata
Consenti regole sia dall'origine che dalla destinazione	Nessuna preferenza
Scegli se un'origine, una destinazione o entrambe possono fornire regole in un flusso di lavoro di mappatura degli ID	Regole limitate

I controlli delle regole devono essere compatibili tra l'origine e la destinazione da utilizzare in un flusso di lavoro di mappatura degli ID. Ad esempio, se lo spazio dei nomi dell'ID di origine limita le regole alla destinazione ma lo spazio dei nomi dell'ID di destinazione limita le regole all'origine, viene generato un errore.

b. Per le regole di abbinamento, aggiunge AWS Entity Resolution automaticamente le regole dal flusso di lavoro corrispondente.

8. Per i parametri di confronto e abbinamento, procedi come segue.

a. Specificate il tipo di confronto scegliendo una delle seguenti opzioni in base al vostro obiettivo.

Il tuo obiettivo	Opzione consigliata
Consenti l'utilizzo di qualsiasi tipo di confronto quando crei il flusso di lavoro di mappatura degli ID.	Nessuna preferenza
Trova qualsiasi combinazione di corrispondenze tra i dati archiviati in più campi di input, indipendentemente dal fatto che i dati si trovino nello stesso campo di input o in un campo di input diverso.	Campi di input multipli
Limita il confronto all'interno di un singolo campo di input, quando dati simili memorizzati in più campi di input non devono corrispondere.	Campo di input singolo

b. Specificate il tipo di record matching scegliendo una delle seguenti opzioni in base al vostro obiettivo.

Il tuo obiettivo	Opzione consigliata
Consenti l'utilizzo di qualsiasi tipo di confronto quando crei il flusso di lavoro di mappatura degli ID.	Nessuna preferenza
Limita il tipo di corrispondenza dei record in modo da memorizzare solo un record corrispondente nell'origine per ogni record corrispondente nella destinazione quando crei il flusso di lavoro di mappatura degli ID.	Corrispondenza limitata dei record e Una fonte per un unico obiettivo

Il tuo obiettivo	Opzione consigliata
Limita il tipo di corrispondenza dei record per memorizzare tutti i record corrispondenti nell'origine per ogni record corrispondente nella destinazione quando crei il flusso di lavoro di mappatura degli ID.	Corrispondenza limitata dei record e Molte fonti per un unico obiettivo

> **Note**
>
> È necessario specificare limitazioni compatibili per i namespace degli ID di origine e di destinazione. Ad esempio, se lo spazio dei nomi dell'ID di origine limita le regole alla destinazione ma lo spazio dei nomi dell'ID di destinazione limita le regole all'origine, viene generato un errore.

9. Specificate le autorizzazioni di accesso al servizio scegliendo il nome del ruolo di servizio esistente dall'elenco a discesa.
10. (Facoltativo) Per abilitare i tag per la risorsa, scegli Aggiungi nuovo tag, quindi inserisci la coppia Chiave e Valore.
11. Scegliete Crea spazio dei nomi ID.

Viene creato il target dello spazio dei nomi ID. Dopo aver creato gli spazi dei nomi ID (origine e destinazione) necessari per un flusso di lavoro di mappatura degli ID, sei pronto per creare un flusso di lavoro di mappatura degli ID.

Creazione di un target per lo spazio dei nomi ID (metodo dei servizi del fornitore)

Questo argomento descrive il processo di creazione di un target di namespace ID utilizzando il metodo Provider services. Questo metodo utilizza un servizio provider chiamato. LiveRamp LiveRamp traduce i dati codificati di terze parti da un'origine a una destinazione durante un flusso di lavoro di mappatura degli ID.

Per creare un target di namespace ID (provider services)

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli ID namespaces.
3. Nella pagina dei namespace ID, nell'angolo in alto a destra, scegli Crea spazio dei nomi ID.
4. Per i dettagli, procedi come segue:
   a. Per il nome dello spazio dei nomi ID, immettete un nome univoco.
   b. (Facoltativo) In Descrizione, immettere una descrizione facoltativa.
   c. Per il tipo di namespace ID, scegli Target.
5. Per il metodo dello spazio dei nomi ID, scegli Provider services.

> **Note**
>
> AWS Entity Resolution attualmente offre il servizio del LiveRamp provider come metodo ID namespace.
> Se hai un abbonamento a LiveRamp, lo stato appare come Sottoscritto.
> Per ulteriori informazioni su come sottoscrivere un abbonamento LiveRamp, consultaFase 1: Abbonarsi a un servizio fornito da un provider su AWS Data Exchange.

6. Per Target domain, inserisci l'identificatore LiveRamp del dominio client destinato alla transcodifica che fornisce. LiveRamp
7. (Facoltativo) Per abilitare i tag per la risorsa, scegli Aggiungi nuovo tag, quindi inserisci la coppia Chiave e Valore.
8. Scegliete Crea spazio dei nomi ID.

Viene creato il target dello spazio dei nomi ID. Dopo aver creato gli spazi dei nomi ID (origine e destinazione) necessari per un flusso di lavoro di mappatura degli ID, sei pronto per creare il flusso di lavoro di mappatura degli ID.

Modifica di uno spazio dei nomi ID

Puoi modificare uno spazio dei nomi ID solo prima di associarlo a un flusso di lavoro di mappatura degli ID. Dopo aver associato uno spazio dei nomi ID a un flusso di lavoro di mappatura degli ID, non puoi modificarlo.

Per modificare uno spazio dei nomi ID:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli ID namespaces.
3. Scegli lo spazio dei nomi ID.
4. Scegli Modifica.
5. Nella pagina Modifica spazio dei nomi ID, apporta le modifiche necessarie, quindi scegli Salva.

Eliminazione di un namespace ID

Non puoi eliminare uno spazio dei nomi ID quando è associato a un flusso di lavoro di mappatura degli ID. È necessario rimuovere la mappatura dello schema da tutti i flussi di lavoro di mappatura degli ID associati prima di poterla eliminare.

Per eliminare uno spazio dei nomi ID:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, in Preparazione dei dati, scegli ID namespaces.
3. Scegli lo spazio dei nomi ID.
4. Scegli Elimina.
5. Conferma l'eliminazione, quindi scegli Elimina.

Aggiungere o aggiornare una politica delle risorse per un namespace ID

Una politica delle risorse consente al creatore della risorsa di mappatura degli ID di accedere alla risorsa dello spazio dei nomi ID.

Per aggiungere o aggiornare una politica delle risorse

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli ID namespace.

3. Scegli lo spazio dei nomi ID.
4. Nella pagina dei dettagli dello spazio dei nomi ID, scegli la scheda Autorizzazioni.
5. Nella sezione Politica delle risorse, scegli Modifica.
6. Aggiungi o aggiorna la politica nell'JSONeditor.
7. Scegli Save changes (Salva modifiche).

Abbina i dati di input utilizzando un flusso di lavoro corrispondente

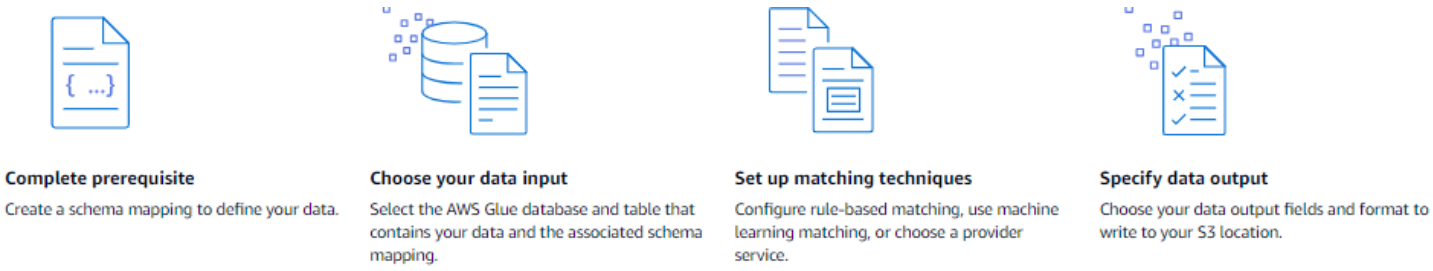
Un flusso di lavoro corrispondente è un processo di elaborazione dei dati che combina e confronta i dati provenienti da diverse fonti di input e determina quali di essi corrispondono in base a diverse tecniche di abbinamento. Produce una tabella di output dei dati.

Quando si crea un flusso di lavoro corrispondente, si specificano innanzitutto gli input di dati, le fasi di normalizzazione e quindi si scelgono le tecniche di corrispondenza e l'output dei dati desiderati. AWS Entity Resolution legge i dati dalla posizione o dalle posizioni specificate e trova una corrispondenza tra due o più record nei dati. Quindi assegna un Match ID ai record nel set di dati corrispondente. AWS Entity Resolution quindi scrive i file di output dei dati in una posizione scelta dall'utente. Se lo desideri, puoi AWS Entity Resolution utilizzarli per eseguire l'hash dei dati di output, aiutandoti a mantenere il controllo sui dati.

Un workflow corrispondente può avere più esecuzioni e i risultati (successi o errori) vengono scritti in una cartella con `jobId` il nome.

L'output dei dati contiene sia un file per le corrispondenze riuscite sia un file per gli errori. L'output dei dati può contenere più campi. I risultati positivi vengono scritti in una `success` cartella che contiene più file e ogni file contiene un sottoinsieme dei record riusciti. Analogamente, gli errori vengono scritti in una `error` cartella con più campi, ognuno dei quali contiene un sottoinsieme dei record di errore. Per ulteriori informazioni sulla risoluzione degli errori, vedereRisoluzione dei problemi relativi ai flussi di lavoro corrispondenti.

Il diagramma seguente riassume come creare un flusso di lavoro corrispondente.



Prima di creare un flusso di lavoro corrispondente, è necessario creare una mappatura dello schema. Per ulteriori informazioni, consulta Creazione di una mappatura dello schema.

Esistono tre modi per creare un flusso di lavoro corrispondente, basato su tecniche di abbinamento: basato su regole, basato sull'apprendimento automatico o basatosui servizi del provider.

Dopo aver creato ed eseguito un flusso di lavoro corrispondente, puoi effettuare le seguenti operazioni:

- Visualizza i risultati nella posizione S3 che hai specificato. I flussi di lavoro corrispondenti vengono generati IDs dopo l'indicizzazione dei dati.
- Utilizza l'output della corrispondenza basata su regole o della corrispondenza basata sull'apprendimento automatico (ML) come input per la corrispondenza basata sui servizi del provider o viceversa per soddisfare le tue esigenze aziendali.

  Example

  Ad esempio, per risparmiare sui costi di abbonamento del provider, puoi innanzitutto eseguire un abbinamento basato su regole per trovare le corrispondenze nei tuoi dati. Quindi, puoi inviare un sottoinsieme di record non corrispondenti alla corrispondenza basata sui servizi del provider.

Argomenti

Creazione di un flusso di lavoro di abbinamento basato su regole

La corrispondenza basata su regole è un insieme gerarchico di regole di corrispondenza a cascata, suggerite e basate sui dati che inserisci ed è completamente configurabile dall' AWS Entity Resolution utente. Il flusso di lavoro di abbinamento basato su regole consente di confrontare dati in chiaro o con hash per trovare corrispondenze esatte in base a criteri personalizzati.

Quando AWS Entity Resolution trova una corrispondenza tra due o più record nei dati, assegna:

- Un Match ID ai record nel set di dati corrispondente
- La regola Match che ha generato la corrispondenza.

Per creare un flusso di lavoro di abbinamento basato su regole:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Corrispondenza.
3. Nella pagina Flussi di lavoro corrispondenti, nell'angolo in alto a destra, scegli Crea flusso di lavoro corrispondente.
4. Per il passaggio 1: Specificare i dettagli del flusso di lavoro corrispondente, procedi come segue:

   a. Immettete un nome del flusso di lavoro corrispondente e una descrizione opzionale.

   b. Per l'immissione dei dati, scegli un AWS Glue database dal menu a discesa, seleziona la AWS Glue tabella e quindi la mappatura dello schema corrispondente.

      È possibile aggiungere fino a 19 input di dati.

   c. L'opzione Normalizza dati è selezionata per impostazione predefinita, in modo che gli input di dati vengano normalizzati prima della corrispondenza. Se non desiderate normalizzare i dati, deselezionate l'opzione Normalizza dati.

   d. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione e intraprendi l'azione consigliata.

Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	• AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. • Il nome del ruolo di servizio predefinito è `entityresolution-matching-workflow-<timestamp>` . • È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche.

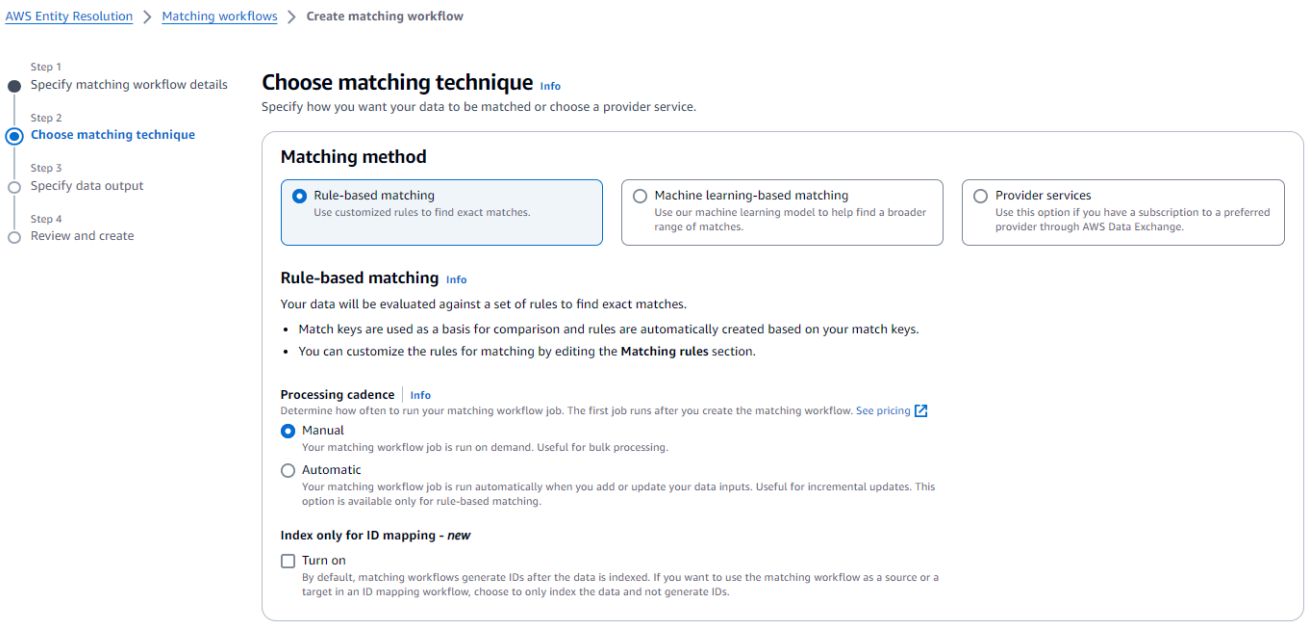
Opzione	Azione consigliata
	• Se i dati di input sono crittografati, puoi scegliere l'opzione Questi dati sono crittografati con una KMS chiave e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati in ingresso.
Utilizza un ruolo di servizio esistente	1. Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. L'elenco dei ruoli viene visualizzato se si dispone delle autorizzazioni per elencare i ruoli. Se non disponi delle autorizzazioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibile. 2. Visualizza il ruolo di servizio scegliendo il link Visualizza in IAM esterno. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiungere le autorizzazioni necessarie.

e. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

f. Scegli Next (Successivo).

5. Per la fase 2: Scegli la tecnica di abbinamento:

a. Per il metodo di abbinamento, scegli Abbinamento basato su regole.



Scegli la schermata della tecnica di abbinamento con opzioni di apprendimento automatico e basate su regole.

b. Per Processing cadence, scegli una delle seguenti opzioni in base al tuo obiettivo.

Il tuo obiettivo	Opzione consigliata
Esegui un flusso di lavoro su richiesta per un aggiornamento collettivo	Manuale
Esegui un flusso di lavoro non appena nuovi dati sono presenti nel tuo bucket S3	Automatica

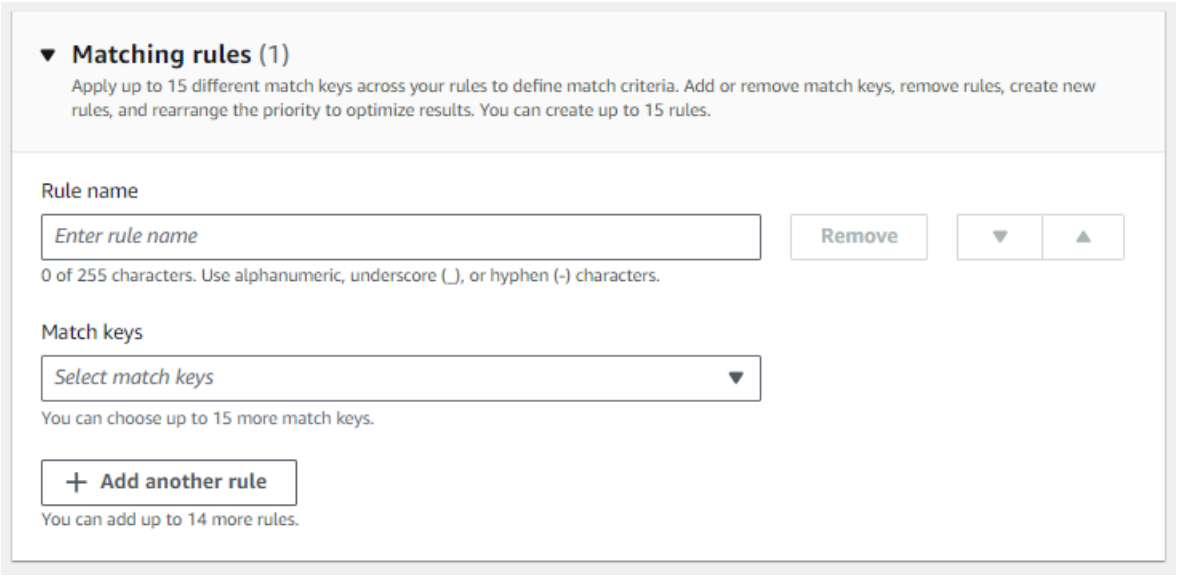
> **Note**
>
> Se scegli Automatico, assicurati di avere EventBridge le notifiche Amazon attivate per il tuo bucket S3. Per istruzioni su come abilitare Amazon EventBridge tramite la console S3, consulta Enabling Amazon EventBridge nella Amazon S3 User Guide.

c. (Facoltativo) Per Indicizza solo per la mappatura degli ID, puoi scegliere di attivare la capacità di indicizzare solo i dati e non di generarli. IDs

   Per impostazione predefinita, i flussi di lavoro corrispondenti vengono generati IDs dopo l'indicizzazione dei dati.

d. Per le regole di corrispondenza, inserisci il nome di una regola, quindi scegli i tasti di corrispondenza per quella regola.

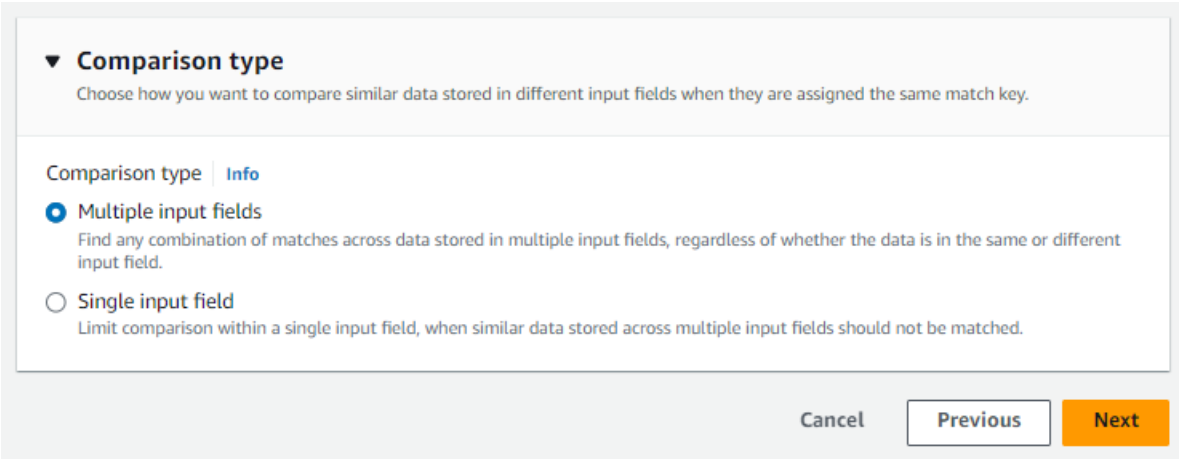
   Puoi creare fino a 15 regole e applicare fino a 15 chiavi di abbinamento diverse alle regole per definire i criteri di corrispondenza.



   Le regole di corrispondenza si interfacciano con i campi per inserire il nome della regola e selezionare le chiavi di corrispondenza.

e. Per Tipo di confronto, scegli una delle seguenti opzioni in base al tuo obiettivo.

Il tuo obiettivo	Opzione consigliata
Trova qualsiasi combinazione di corrispondenze tra i dati archiviati in più campi di input	Campi di input multipli
Limita il confronto a un singolo campo di input	Campo di input singolo



Opzion relative al tipo di confronto: campi di input multipli per trovare corrispondenze tra i dati archiviati in più campi o campo di input singolo per limitare il confronto all'interno di un campo.

f. Scegli Next (Successivo).

6. Per la fase 3: Specificare l'output e il formato dei dati:

   a. Per Destinazione e formato di output dei dati, scegli la posizione Amazon S3 per l'output dei dati e se il formato dei dati sarà Dati normalizzati o Dati originali.

   b. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave. ARN

   c. Visualizza l'output generato dal sistema.

   d. Per l'output dei dati, decidi quali campi includere, nascondere o mascherare, quindi intraprendi le azioni consigliate in base ai tuoi obiettivi.

Il tuo obiettivo	Azione consigliata
Includi campi	Mantieni lo stato di output come incluso.
Nascondi i campi (escludi dall'output)	Scegli il campo Output, quindi scegli Nascondi.
Maschera i campi	Scegli il campo Output, quindi scegli Hash output.
Ripristina le impostazioni precedenti	Scegliere Reimposta.

e. Scegli Next (Successivo).

7. Per il passaggio 4: rivedi e crea:

   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

   b. Scegli Create and run (Crea ed esegui).

      Viene visualizzato un messaggio che indica che il flusso di lavoro corrispondente è stato creato e che il processo è iniziato.

8. Nella pagina dei dettagli del flusso di lavoro corrispondente, nella scheda Metriche, visualizza quanto segue in Metriche dell'ultimo lavoro:

   - Il Job ID.
   - Lo stato del processo del flusso di lavoro corrispondente: In coda, In corso, Completato, Non riuscito
   - Il tempo di completamento del processo del flusso di lavoro.
   - Il numero di record elaborati.
   - Il numero di record non elaborati.
   - La corrispondenza unica IDs generata.
   - Il numero di record di input.

   Puoi anche visualizzare le metriche dei job per i job corrispondenti ai job del flusso di lavoro che sono stati eseguiti in precedenza nella cronologia Job.

9. Una volta completato il processo del flusso di lavoro corrispondente (lo stato è completato), puoi andare alla scheda Data output e quindi selezionare la tua sede Amazon S3 per visualizzare i risultati.
10. (Solo tipo di elaborazione manuale) Se hai creato un flusso di lavoro corrispondente basato su regole con il tipo di elaborazione manuale, puoi eseguire il flusso di lavoro corrispondente in qualsiasi momento selezionando Esegui flusso di lavoro nella pagina dei dettagli del flusso di lavoro corrispondente.

Creazione di un flusso di lavoro di abbinamento basato sull'apprendimento automatico

La corrispondenza basata sull'apprendimento automatico è un processo preimpostato che tenta di abbinare i record di tutti i dati che inserisci. Il flusso di lavoro di abbinamento basato sull'apprendimento automatico consente di confrontare i dati in chiaro per trovare un'ampia gamma di corrispondenze utilizzando un modello di apprendimento automatico.

> **Note**
>
> Il modello di apprendimento automatico non supporta il confronto di dati con hash.

Quando AWS Entity Resolution trova una corrispondenza tra due o più record nei dati, assegna:

- Un Match ID ai record nel set di dati corrispondente
- La percentuale del livello di confidenza della partita.

Puoi utilizzare l'output di un flusso di lavoro di abbinamento basato su ML come input per la corrispondenza tra fornitori di servizi di dati o viceversa per raggiungere i tuoi obiettivi specifici. Ad esempio, puoi eseguire una corrispondenza basata su ML per trovare innanzitutto le corrispondenze tra le tue fonti di dati nei tuoi record. Se un sottoinsieme non corrisponde, puoi quindi eseguire la corrispondenza basata sui servizi del provider per trovare altre corrispondenze.

Per creare un flusso di lavoro di abbinamento basato su ML:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS (se non l'hai ancora fatto).

2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Corrispondenza.
3. Nella pagina Flussi di lavoro corrispondenti, nell'angolo in alto a destra, scegli Crea flusso di lavoro corrispondente.
4. Per il passaggio 1: Specificare i dettagli del flusso di lavoro corrispondente, procedi come segue:

   a. Immettete un nome del flusso di lavoro corrispondente e una descrizione opzionale.

   b. Per l'immissione dei dati, scegli un AWS Glue database dal menu a discesa, seleziona la AWS Glue tabella e quindi la mappatura dello schema corrispondente.

      È possibile aggiungere fino a 20 input di dati.

   c. L'opzione Normalizza dati è selezionata per impostazione predefinita, in modo che gli input di dati vengano normalizzati prima della corrispondenza. Se non desiderate normalizzare i dati, deselezionate l'opzione Normalizza dati.

   d. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione e intraprendi l'azione consigliata.

Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	• AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. • Il nome del ruolo di servizio predefinito è `entityresolution-matching-workflow-<timestamp>` . • È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. • Se i dati di input sono crittografati, puoi scegliere l'opzione Questi dati sono crittografati con una KMS chiave e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati in ingresso.

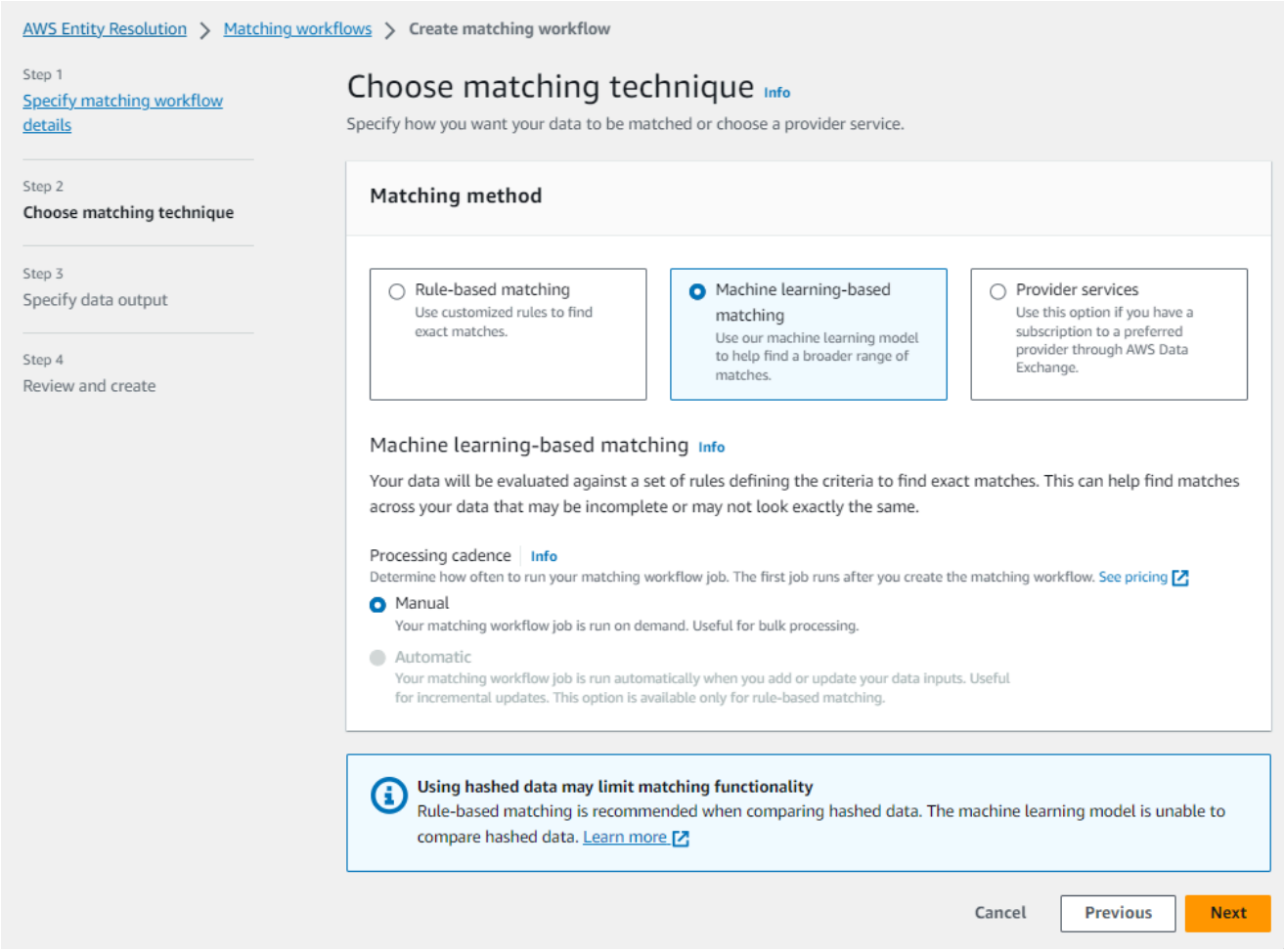
Opzione	Azione consigliata
Utilizza un ruolo di servizio esistente	1. Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. L'elenco dei ruoli viene visualizzato se si dispone delle autorizzazioni per elencare i ruoli. Se non disponi delle autorizza zioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibile. 2. Visualizza il ruolo di servizio scegliendo il link Visualizza in IAM esterno. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiunger e le autorizzazioni necessarie.

e. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

f. Scegli Next (Successivo).

5. Per la fase 2: Scegli la tecnica di abbinamento:

   a. Per il metodo di abbinamento, scegli l'abbinamento basato sull'apprendimento automatico.



AWS Entity Resolution abbinamento dell'interfaccia di creazione del flusso di lavoro con opzioni per l'abbinamento basato su regole o sull'apprendimento automatico.

b. Per Processing cadence, è selezionata l'opzione Manuale.

   Questa opzione consente di eseguire un flusso di lavoro su richiesta per un aggiornamento in blocco.

c. Scegli Next (Successivo).

6. Per la fase 3: Specificare l'output e il formato dei dati:

   a. Per Destinazione e formato di output dei dati, scegli la posizione Amazon S3 per l'output dei dati e se il formato dei dati sarà Dati normalizzati o Dati originali.

   b. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave. ARN

   c. Visualizza l'output generato dal sistema.

d. Per l'output dei dati, decidi quali campi includere, nascondere o mascherare, quindi intraprendi le azioni consigliate in base ai tuoi obiettivi.

Il tuo obiettivo	Opzione consigliata
Includi campi	Mantieni lo stato di output come incluso.
Nascondi i campi (escludi dall'output)	Scegli il campo Output, quindi scegli Nascondi.
Maschera i campi	Scegli il campo Output, quindi scegli Hash output.
Ripristina le impostazioni precedenti	Scegliere Reimposta.

e. Scegli Next (Successivo).

7. Per il passaggio 4: rivedi e crea:

   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

   b. Scegli Create and run (Crea ed esegui).

      Viene visualizzato un messaggio che indica che il flusso di lavoro corrispondente è stato creato e che il processo è iniziato.

8. Nella pagina dei dettagli del flusso di lavoro corrispondente, nella scheda Metriche, visualizza quanto segue in Metriche dell'ultimo lavoro:

   - Il Job ID.
   - Lo stato del processo del flusso di lavoro corrispondente: In coda, In corso, Completato, Non riuscito
   - Il tempo di completamento del processo del flusso di lavoro.
   - Il numero di record elaborati.
   - Il numero di record non elaborati.
   - La corrispondenza unica IDs generata.
   - Il numero di record di input.

Puoi anche visualizzare le metriche dei job per i job corrispondenti ai job del flusso di lavoro che sono stati eseguiti in precedenza nella cronologia Job.

9. Una volta completato il processo del flusso di lavoro corrispondente (lo stato è completato), puoi andare alla scheda Data output e quindi selezionare la tua sede Amazon S3 per visualizzare i risultati.
10. (Solo tipo di elaborazione manuale) Se hai creato un flusso di lavoro corrispondente basato sull'apprendimento automatico con il tipo di elaborazione manuale, puoi eseguire il flusso di lavoro corrispondente in qualsiasi momento selezionando Esegui flusso di lavoro nella pagina dei dettagli del flusso di lavoro corrispondente.

Creazione di un flusso di lavoro di abbinamento basato sui servizi del provider

La corrispondenza basata sui servizi del provider ti consente di abbinare i tuoi identificatori noti al tuo fornitore di servizi di dati preferito.

AWS Entity Resolution attualmente supporta i seguenti servizi di provider di dati:

- LiveRamp
- TransUnion
- ID unificato 2.0

Per ulteriori informazioni sui servizi del provider supportati, vederePreparazione di dati di input di terze parti.

Puoi utilizzare un abbonamento pubblico per questi provider AWS Data Exchange o negoziare un'offerta privata direttamente con il fornitore di dati. Per ulteriori informazioni sulla creazione di un nuovo abbonamento o sul riutilizzo di un abbonamento esistente a un servizio del provider, consulta. Fase 1: Abbonarsi a un servizio fornito da un provider su AWS Data Exchange

Le sezioni seguenti descrivono come creare un flusso di lavoro di abbinamento basato sul provider.

Argomenti

- Creazione di un flusso di lavoro corrispondente con LiveRamp
- Creazione di un flusso di lavoro corrispondente con TransUnion

- Creazione di un flusso di lavoro corrispondente con 2.0 UID

Creazione di un flusso di lavoro corrispondente con LiveRamp

Se hai un abbonamento al LiveRamp servizio, puoi creare un flusso di lavoro corrispondente con il LiveRamp servizio per eseguire la risoluzione delle identità.

Il LiveRamp servizio fornisce un identificatore chiamato RAMpid. Il RAMpid è una delle piattaforme più comunemente utilizzate IDs nelle piattaforme lato domanda per creare un pubblico per una campagna pubblicitaria. Utilizzando un flusso di lavoro corrispondente con LiveRamp, puoi risolvere gli indirizzi email con hash in. RAMPIDs

> **Note**
>
> AWS Entity Resolution supporta l'assegnazione PII basata su RAMpiD.

Questo flusso di lavoro richiede un bucket di data staging Amazon S3 in cui desideri che l'output del flusso di lavoro corrispondente venga scritto temporaneamente. Prima di creare un flusso di lavoro di mappatura degli ID con LiveRamp, aggiungi le seguenti autorizzazioni al bucket di data staging.

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

Sostituisci ciascuno *<user input placeholder>* con le tue informazioni.

staging-bucket	Bucket Amazon S3 che archivia temporane amente i dati durante l'esecuzione di un flusso di lavoro basato sui servizi del provider.

Per creare un flusso di lavoro corrispondente con: LiveRamp

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Corrispondenza.
3. Nella pagina Flussi di lavoro corrispondenti, nell'angolo in alto a destra, scegli Crea flusso di lavoro corrispondente.
4. Per il passaggio 1: Specificare i dettagli del flusso di lavoro corrispondente, procedi come segue:
    a. Immettete un nome del flusso di lavoro corrispondente e una descrizione opzionale.
    b. Per l'immissione dei dati, scegli un AWS Glue database dal menu a discesa, seleziona la AWS Glue tabella, quindi seleziona la mappatura dello schema corrispondente.

È possibile aggiungere fino a 20 input di dati.

c. L'opzione Normalizza dati è selezionata per impostazione predefinita, in modo che gli input di dati vengano normalizzati prima della corrispondenza.

   Se utilizzate il processo di risoluzione solo tramite e-mail, deselezionate l'opzione Normalizza i dati, poiché per i dati di input vengono utilizzate solo e-mail con hash.

d. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione e intraprendi l'azione consigliata.

Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	• AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. • Il nome del ruolo di servizio predefinito è`entityresolution-matching-workflow-<timestamp>` . • È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. • Se i dati di input sono crittografati, puoi scegliere l'opzione Questi dati sono crittografati con una KMS chiave e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati in ingresso.

Opzione	Azione consigliata
Utilizza un ruolo di servizio esistente	1. Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. L'elenco dei ruoli viene visualizzato se si dispone delle autorizzazioni per elencare i ruoli. Se non disponi delle autorizza zioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibile. 2. Visualizza il ruolo di servizio scegliendo il link Visualizza in IAM esterno. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiunger e le autorizzazioni necessarie.

e. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

f. Scegli Next (Successivo).

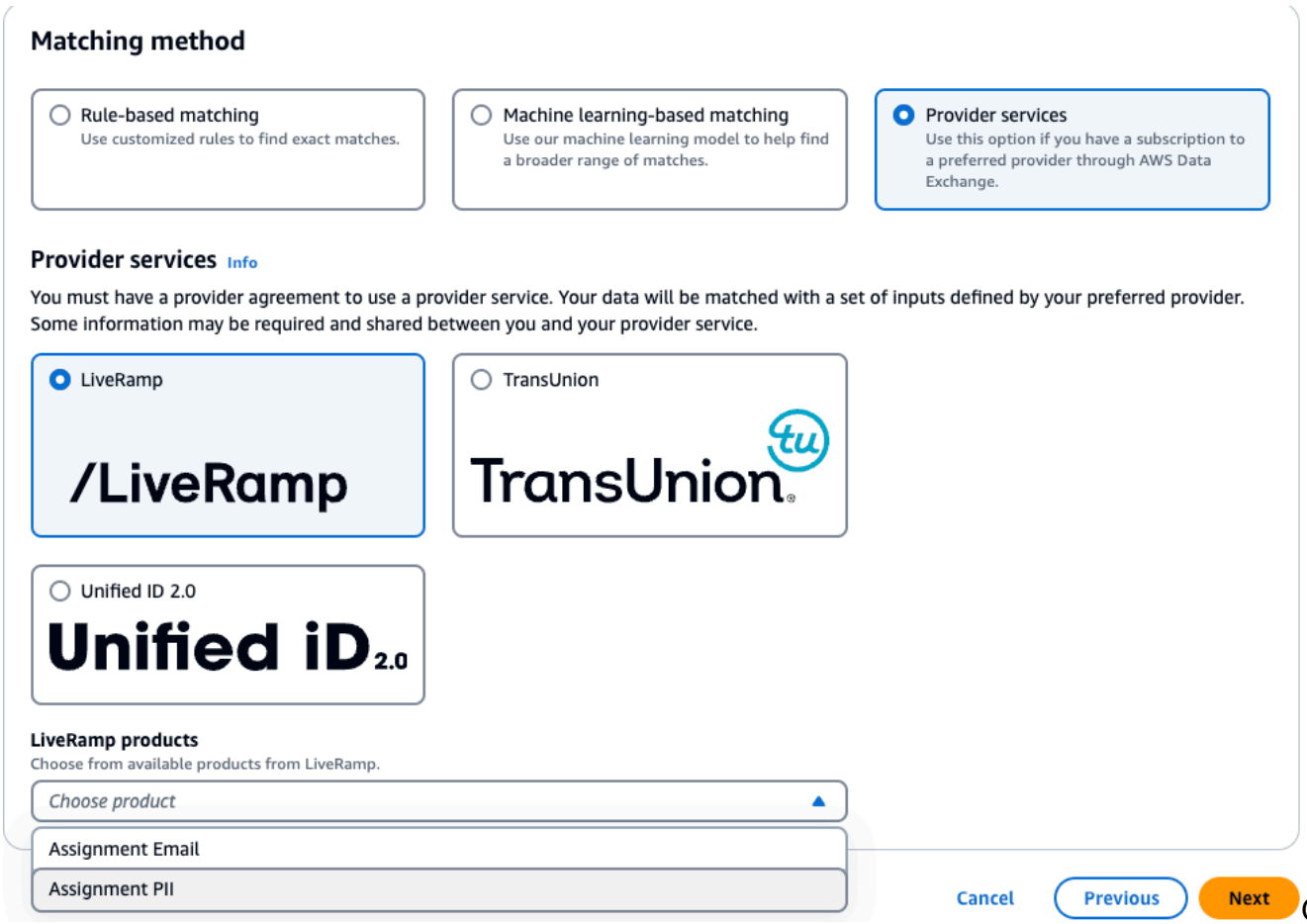
5. Per la fase 2: Scegli la tecnica di abbinamento:

   a. Per il metodo di abbinamento, scegli Provider services.

   b. Per i servizi del fornitore, scegli LiveRamp.

> **Note**
>
> Assicurati che il formato e la normalizzazione del file di input dei dati siano in linea con le linee guida del servizio del provider.
> Per ulteriori informazioni sulle linee guida per la formattazione dei file di input per il flusso di lavoro corrispondente, consulta Perform Identity Resolution Through ADX nella documentazione. LiveRamp

c. Per LiveRamp i prodotti, scegli un prodotto dall'elenco a discesa.

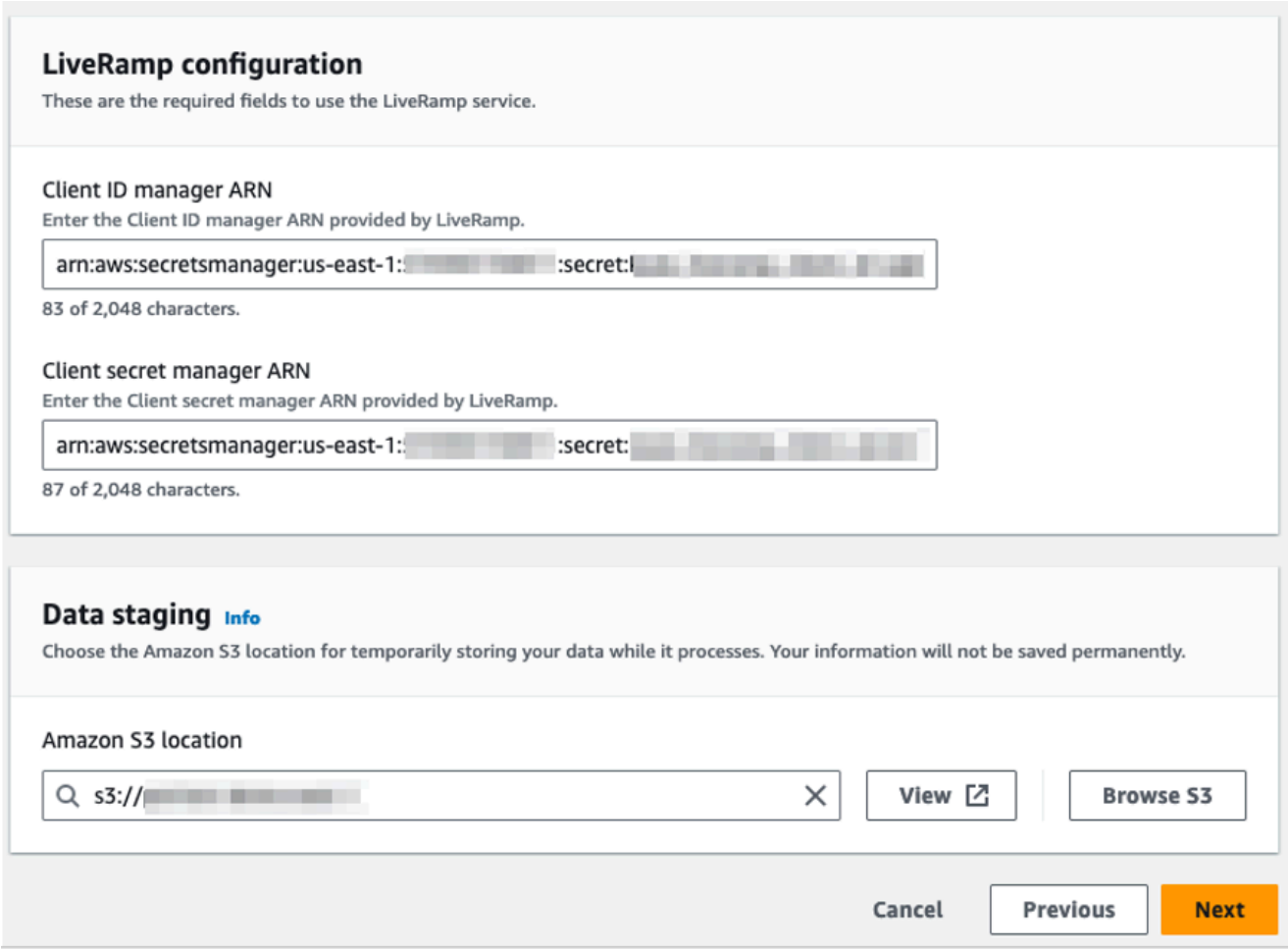


Opzion

del metodo di abbinamento: basato su regole per corrispondenze esatte, apprendimento automatico per corrispondenze più ampie, servizi forniti dai fornitori.

> **Note**
>
> Se scegli AssegnazionePII, devi fornire almeno una colonna non identificativa quando esegui la risoluzione delle entità. Ad esempio,. GENDER

d. Per la LiveRamp configurazione, inserisci un gestore di ID client ARN e un gestore segreto del client ARN.



LiveRa

modulo di configurazione con campi per Client ID manager ARN e Client secret managerARN.

e. Per il data staging, scegli la posizione Amazon S3 per l'archiviazione temporanea dei dati durante l'elaborazione.

È necessario disporre dell'autorizzazione per l'archiviazione dei dati presso la sede Amazon S3. Per ulteriori informazioni, consulta Creazione di un ruolo lavorativo nel flusso di lavoro per AWS Entity Resolution.

f. Scegli Next (Successivo).

6. Per la fase 3: Specificare l'output dei dati:

a. Per Destinazione e formato di output dei dati, scegli la posizione Amazon S3 per l'output dei dati e se il formato dei dati sarà Dati normalizzati o Dati originali.

b. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave. ARN

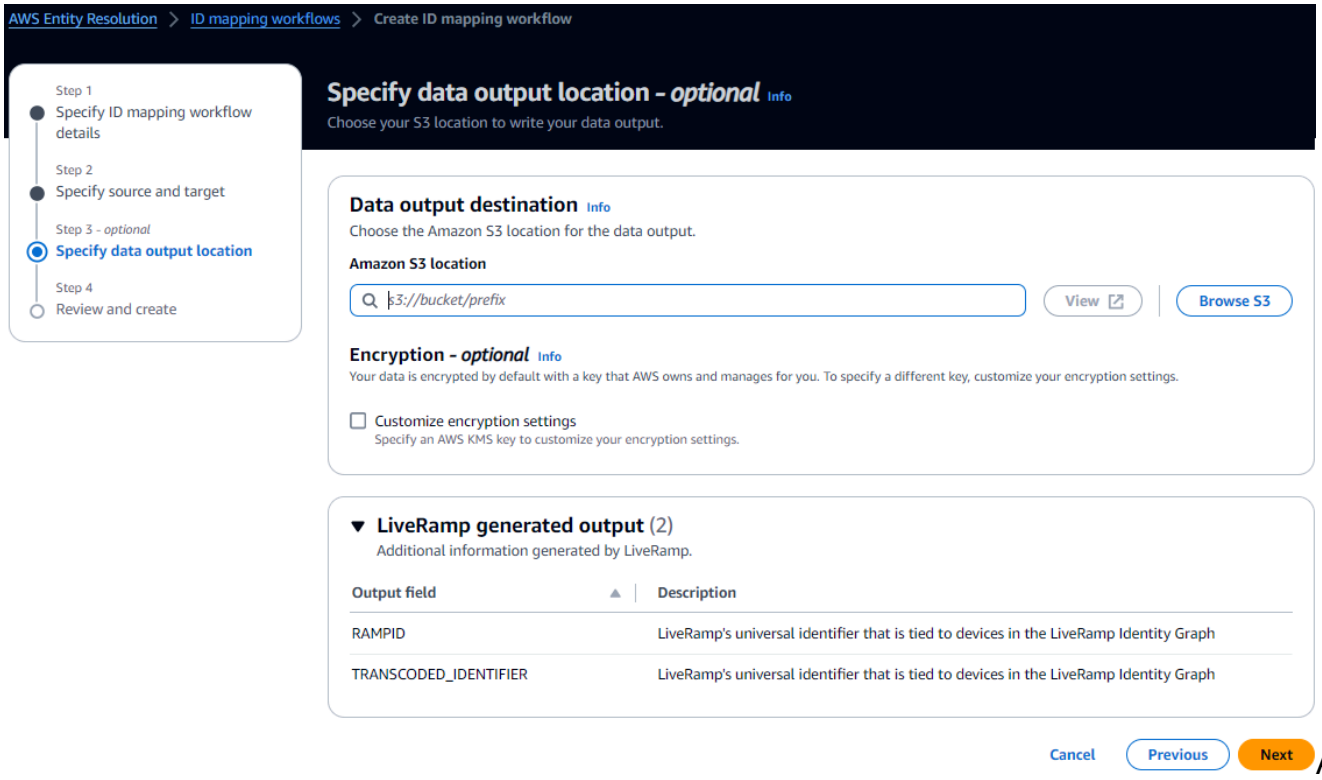
c. Visualizza l'output LiveRamp generato.

Queste sono le informazioni aggiuntive generate da LiveRamp.

d. Per l'output dei dati, decidi quali campi includere, nascondere o mascherare, quindi intraprendi le azioni consigliate in base ai tuoi obiettivi.

> **Note**
>
> Se hai scelto LiveRamp, a causa dei filtri per la LiveRamp privacy che rimuovono le informazioni di identificazione personale (PII), alcuni campi mostreranno lo stato di output non disponibile.

Il tuo obiettivo	Azione consigliata
Includi campi	Mantieni lo stato di output come incluso.
Nascondi i campi (escludi dall'output)	Scegli il campo Output, quindi scegli Nascondi.
Maschera i campi	Scegli il campo Output, quindi scegli Hash output.
Ripristina le impostazioni precedenti	Scegliere Reimposta.



AWS Entity Resolution Interfaccia per la creazione del flusso di lavoro di mappatura degli ID con opzioni per specificare la posizione di output dei dati.

e. Scegli Next (Successivo).

7. Per la fase 4: Rivedi e crea:

   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

   b. Scegli Create and run (Crea ed esegui).

      Viene visualizzato un messaggio che indica che il flusso di lavoro corrispondente è stato creato e che il processo è iniziato.

8. Nella pagina dei dettagli del flusso di lavoro corrispondente, nella scheda Metriche, visualizza quanto segue in Metriche dell'ultimo lavoro:

   - Il Job ID.
   - Lo stato del processo del flusso di lavoro corrispondente: In coda, In corso, Completato, Non riuscito
   - Il tempo di completamento del processo del flusso di lavoro.
   - Il numero di record elaborati.

- Il numero di record non elaborati.
- La corrispondenza unica IDs generata.
- Il numero di record di input.

Puoi anche visualizzare le metriche dei job per i job corrispondenti ai job del flusso di lavoro che sono stati eseguiti in precedenza nella cronologia Job.

9. Una volta completato il processo del flusso di lavoro corrispondente (lo stato è completato), puoi andare alla scheda Data output e quindi selezionare la tua sede Amazon S3 per visualizzare i risultati.

Creazione di un flusso di lavoro corrispondente con TransUnion

Se hai un abbonamento al TransUnion servizio, puoi migliorare la comprensione dei clienti collegando, abbinando e migliorando i record relativi ai clienti archiviati su diversi canali con chiavi E personali e domestiche TransUnion e oltre 200 attributi di dati.

Il TransUnion servizio fornisce identificatori noti come Individuo e Famiglia. TransUnion IDs TransUnion fornisce l'assegnazione tramite ID (nota anche come codifica) di identificatori noti come nome, indirizzo, numero di telefono e indirizzo e-mail.

Questo flusso di lavoro richiede un bucket di data staging Amazon S3 in cui desideri che l'output del flusso di lavoro corrispondente venga scritto temporaneamente. Prima di creare un flusso di lavoro corrispondente con TransUnion, aggiungi le seguenti autorizzazioni al bucket di data staging.

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

Sostituisci ciascuno *<user input placeholder>* con le tue informazioni.

staging-bucket	Bucket Amazon S3 che archivia temporane amente i dati durante l'esecuzione di un flusso di lavoro basato sui servizi del provider.

Per creare un flusso di lavoro corrispondente con: TransUnion

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Corrispondenza.
3. Nella pagina Flussi di lavoro corrispondenti, nell'angolo in alto a destra, scegli Crea flusso di lavoro corrispondente.
4. Per il passaggio 1: Specificare i dettagli del flusso di lavoro corrispondente, procedi come segue:

a. Immettete un nome del flusso di lavoro corrispondente e una descrizione opzionale.

b. Per l'immissione dei dati, scegli un AWS Glue database dal menu a discesa, seleziona la AWS Glue tabella, quindi seleziona la mappatura dello schema corrispondente.

   È possibile aggiungere fino a 20 input di dati.

c. L'opzione Normalizza dati è selezionata per impostazione predefinita, in modo che gli input di dati vengano normalizzati prima della corrispondenza. Se non desiderate normalizzare i dati, deselezionate l'opzione Normalizza dati.

d. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione e intraprendi l'azione consigliata.

Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	• AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. • Il nome del ruolo di servizio predefinito è`entityresolution-matching-workflow-<timestamp>` . • È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. • Se i dati di input sono crittografati, puoi scegliere l'opzione Questi dati sono crittografati con una KMS chiave e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati in ingresso.

Opzione	Azione consigliata
Utilizza un ruolo di servizio esistente	1. Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. L'elenco dei ruoli viene visualizzato se si dispone delle autorizzazioni per elencare i ruoli. Se non disponi delle autorizza zioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibile. 2. Visualizza il ruolo di servizio scegliendo il link Visualizza in IAM esterno. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiunger e le autorizzazioni necessarie.

e. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

f. Scegli Next (Successivo).

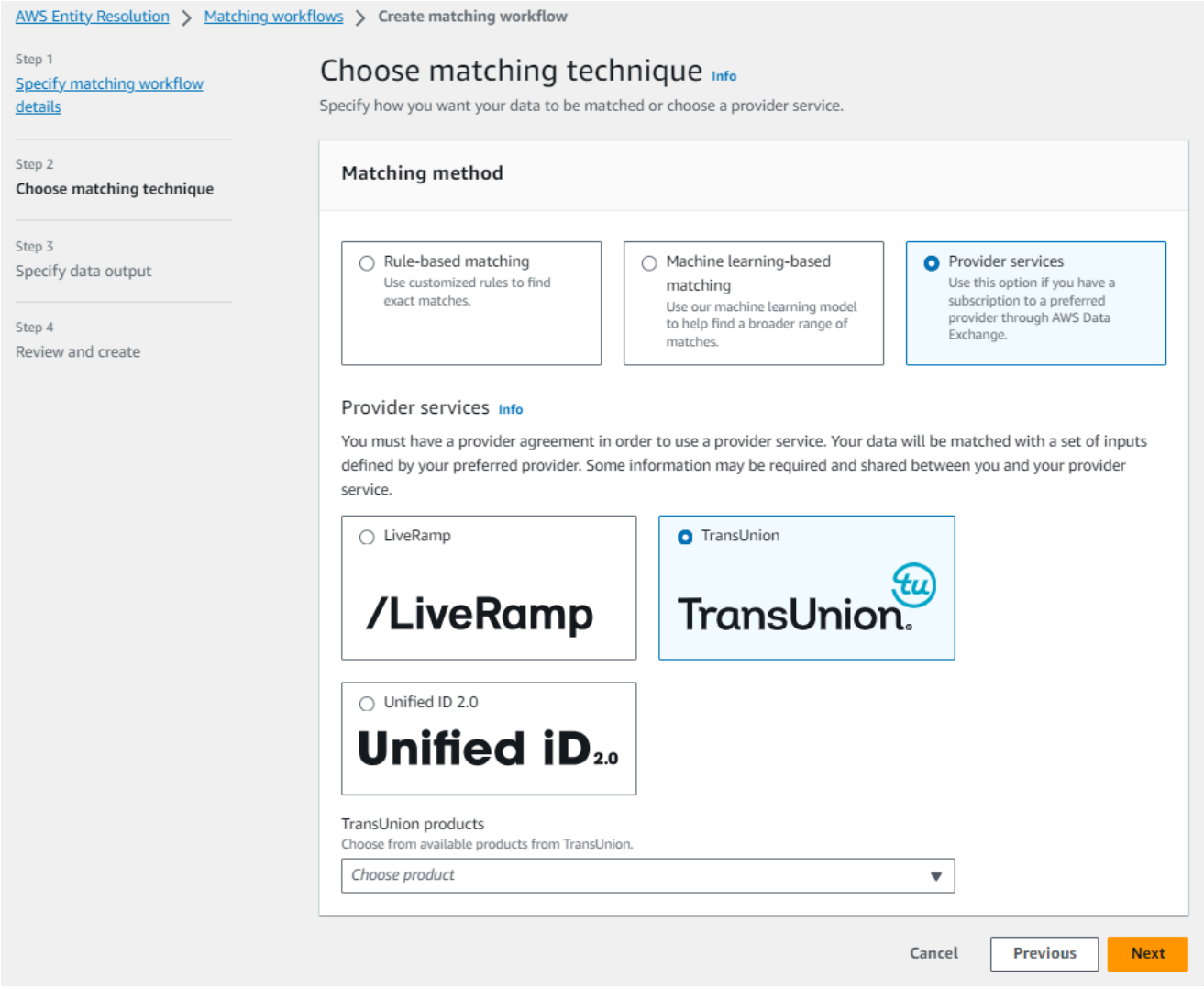
5. Per la fase 2: Scegli la tecnica di abbinamento:

a. Per il metodo di abbinamento, scegli Provider services.

b. Per i servizi del fornitore, scegli TransUnion.

> **Note**
>
> Assicurati che il formato e la normalizzazione del file di input dei dati siano in linea con le linee guida del servizio del provider.

c. Per TransUnion i prodotti, scegli un prodotto dall'elenco a discesa.



AWS Entity Resolution opzioni tecniche di abbinamento dei servizi: servizi basati su regole, basati sull'apprendimento automatico o servizi forniti dai fornitori.

d. Per il data staging, scegli la posizione Amazon S3 per l'archiviazione temporanea dei dati durante l'elaborazione.

È necessario disporre dell'autorizzazione per l'archiviazione dei dati presso la sede Amazon S3. Per ulteriori informazioni, consulta the section called “Creazione di un ruolo lavorativo nel flusso di lavoro”.

6. Scegli Next (Successivo).
7. Per la fase 3: Specificare l'output dei dati:
   a. Per Destinazione e formato di output dei dati, scegli la posizione Amazon S3 per l'output dei dati e se il formato dei dati sarà Dati normalizzati o Dati originali.
   b. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave. ARN
   c. Visualizza l'output TransUnion generato.

      Queste sono le informazioni aggiuntive generate da TransUnion.
   d. Per l'output dei dati, decidi quali campi includere, nascondere o mascherare, quindi intraprendi le azioni consigliate in base ai tuoi obiettivi.

Il tuo obiettivo	Azione consigliata
Includi campi	Mantieni lo stato di output come incluso.
Nascondi i campi (escludi dall'output)	Scegli il campo Output, quindi scegli Nascondi.
Maschera i campi	Scegli il campo Output, quindi scegli Hash output.
Ripristina le impostazioni precedenti	Scegliere Reimposta.

   e. Per l'output generato dal sistema, visualizza tutti i campi inclusi.
   f. Scegli Next (Successivo).
8. Per la fase 4: Rivedi e crea:
   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.
   b. Scegli Create and run (Crea ed esegui).

Viene visualizzato un messaggio che indica che il flusso di lavoro corrispondente è stato creato e che il processo è iniziato.

9. Nella pagina dei dettagli del flusso di lavoro corrispondente, nella scheda Metriche, visualizza quanto segue in Metriche dell'ultimo lavoro:

   - Il Job ID.
   - Lo stato del processo del flusso di lavoro corrispondente: In coda, In corso, Completato, Non riuscito
   - Il tempo di completamento del processo del flusso di lavoro.
   - Il numero di record elaborati.
   - Il numero di record non elaborati.
   - La corrispondenza unica IDs generata.
   - Il numero di record di input.

   Puoi anche visualizzare le metriche dei job per i job corrispondenti ai job del flusso di lavoro che sono stati eseguiti in precedenza nella cronologia Job.
10. Una volta completato il processo del flusso di lavoro corrispondente (lo stato è completato), puoi andare alla scheda Data output e quindi selezionare la tua sede Amazon S3 per visualizzare i risultati.

Creazione di un flusso di lavoro corrispondente con 2.0 UID

Se hai un abbonamento al servizio Unified ID 2.0, puoi attivare campagne pubblicitarie con identità deterministica e contare sull'interoperabilità con molti partecipanti UID2 abilitati all'interno dell'ecosistema pubblicitario. Per ulteriori informazioni, consulta la panoramica di Unified ID 2.0.

Il servizio Unified ID 2.0 fornisce raw UID 2, che viene utilizzato per creare campagne pubblicitarie nella piattaforma The Trade Desk. UID2.0 viene generato utilizzando un framework open source.

In un unico flusso di lavoro è possibile utilizzare uno **`Email Address`** o l'altro **`Phone number`** per la UID2 generazione non elaborata, ma non entrambi. Se entrambi sono presenti nella mappatura dello schema, il flusso di lavoro selezionerà il **`Email Address`** campo e **`Phone number`** sarà un campo passante. Per supportare entrambi, crea una nuova mappatura dello schema in cui **`Phone number`** è mappato ma non è mappato. **`Email Address`** Quindi, crea un secondo flusso di lavoro utilizzando questa nuova mappatura dello schema.

> **Note**
>
> UID2sLe materie crude si ottengono aggiungendo i sali contenuti nei secchi di sale, che vengono fatti ruotare all'incirca una volta all'anno, facendo UID2 ruotare anche il prodotto crudo. Pertanto, si consiglia di rinfrescare il crudo ogni giorno. UID2s Per ulteriori informazioni, consulta https://unifiedid.com/docs/how-often-should-uidgetting-started/gs-faqs# 2 -incremental-updates. s-be-refreshed-for

Per creare un flusso di lavoro corrispondente alla versione UID 2.0:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Corrispondenza.
3. Nella pagina Flussi di lavoro corrispondenti, nell'angolo in alto a destra, scegli Crea flusso di lavoro corrispondente.
4. Per il passaggio 1: Specificare i dettagli del flusso di lavoro corrispondente, procedi come segue:

   a. Immettete un nome del flusso di lavoro corrispondente e una descrizione opzionale.

   b. Per l'immissione dei dati, scegli un AWS Glue database dal menu a discesa, seleziona la AWS Glue tabella, quindi seleziona la mappatura dello schema corrispondente.

      È possibile aggiungere fino a 20 input di dati.

   c. Lascia selezionata l'opzione Normalizza dati, in modo che gli input di dati (**`Email Address`**o**`Phone number`**) vengano normalizzati prima della corrispondenza.

      Per ulteriori informazioni sulla **`Email Address`** normalizzazione, consulta Normalizzazione degli indirizzi e-mail nella documentazione 2.0. UID

      Per ulteriori informazioni sulla **`Phone number`** normalizzazione, vedere Normalizzazione dei numeri di telefono nella documentazione 2.0. UID

   d. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione e intraprendi l'azione consigliata.

Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	• AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. • Il nome del ruolo di servizio predefinito è`entityresolution-matching-workflow-<timestamp>` . • È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. • Se i dati di input sono crittografati, puoi scegliere l'opzione Questi dati sono crittografati con una KMS chiave e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati in ingresso.

Opzione	Azione consigliata
Utilizza un ruolo di servizio esistente	1. Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. L'elenco dei ruoli viene visualizzato se si dispone delle autorizzazioni per elencare i ruoli. Se non disponi delle autorizza zioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibile. 2. Visualizza il ruolo di servizio scegliendo il link Visualizza in IAM esterno. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiunger e le autorizzazioni necessarie.

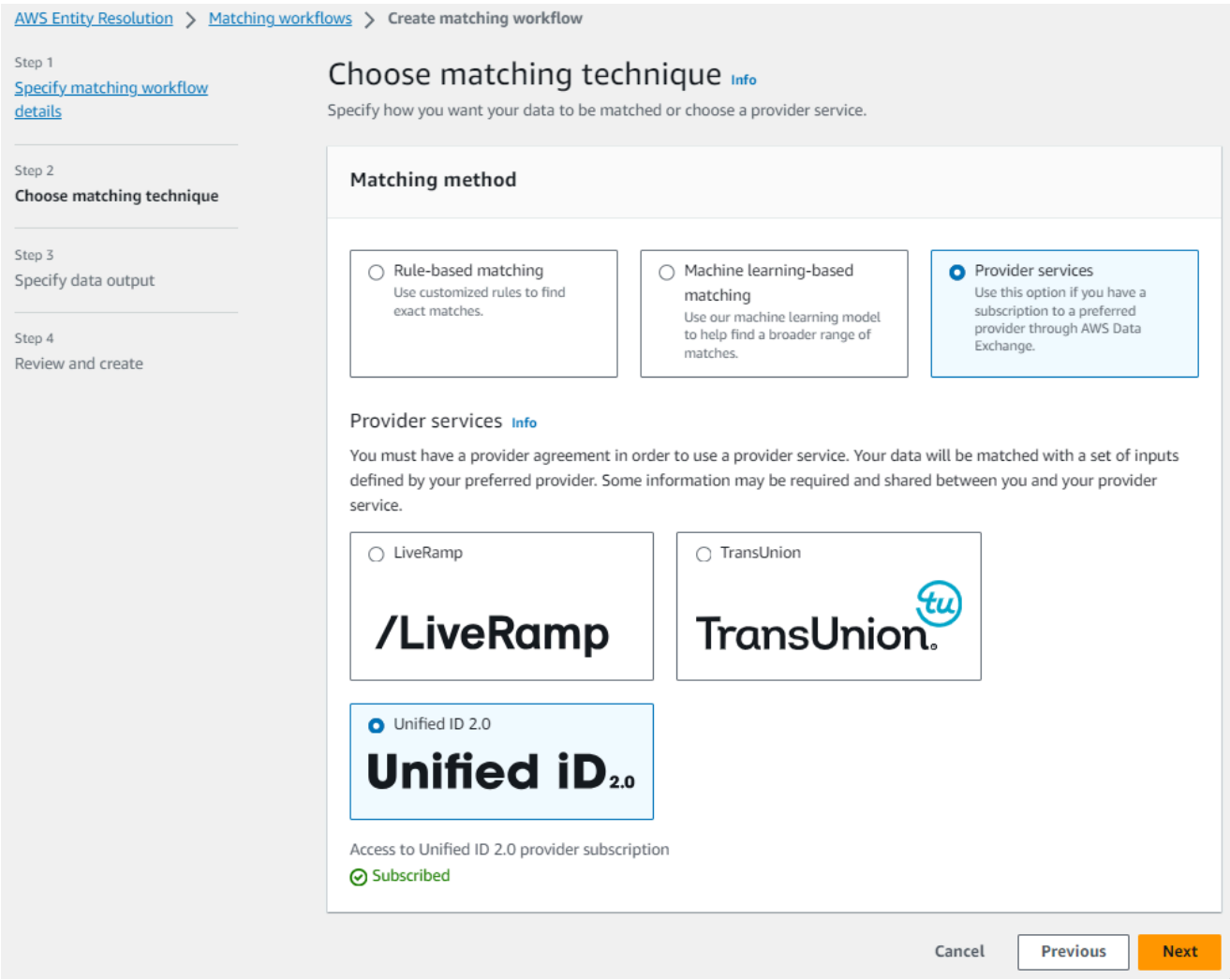
e. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

f. Scegli Next (Successivo).

5. Per la fase 2: Scegli la tecnica di abbinamento:

   a. Per il metodo di abbinamento, scegli Provider services.

   b. Per i servizi Provider, scegli Unified ID 2.0.



AWS Entity Resolution opzioni tecniche di abbinamento dei servizi: servizi basati su regole, basati sull'apprendimento automatico o servizi forniti dai fornitori.

c. Scegli Next (Successivo).

6. Per la fase 3: Specificare l'output dei dati:

a. Per Destinazione e formato di output dei dati, scegli la posizione Amazon S3 per l'output dei dati e se il formato dei dati sarà Dati normalizzati o Dati originali.

b. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave. ARN

c. Visualizza l'output generato da Unified ID 2.0.

Questo è un elenco di tutte le informazioni aggiuntive generate da 2.0 UID

d. Per l'output dei dati, decidi quali campi includere, nascondere o mascherare, quindi intraprendi le azioni consigliate in base ai tuoi obiettivi.

Il tuo obiettivo	Azione consigliata
Includi campi	Mantieni lo stato di output come incluso.
Nascondi i campi (escludi dall'output)	Scegli il campo Output, quindi scegli Nascondi.
Maschera i campi	Scegli il campo Output, quindi scegli Hash output.
Ripristina le impostazioni precedenti	Scegliere Reimposta.

e. Per l'output generato dal sistema, visualizza tutti i campi inclusi.

f. Scegli Next (Successivo).

7. Per la fase 4: Rivedi e crea:

   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

   b. Scegli Create and run (Crea ed esegui).

      Viene visualizzato un messaggio che indica che il flusso di lavoro corrispondente è stato creato e che il processo è iniziato.

8. Nella pagina dei dettagli del flusso di lavoro corrispondente, nella scheda Metriche, visualizza quanto segue in Metriche dell'ultimo lavoro:

   - Il Job ID.
   - Lo stato del processo del flusso di lavoro corrispondente: In coda, In corso, Completato, Non riuscito
   - Il tempo di completamento del processo del flusso di lavoro.
   - Il numero di record elaborati.
   - Il numero di record non elaborati.
   - La corrispondenza unica IDs generata.
   - Il numero di record di input.

Puoi anche visualizzare le metriche dei job per i job corrispondenti ai job del flusso di lavoro che sono stati eseguiti in precedenza nella cronologia Job.

9. Una volta completato il processo del flusso di lavoro corrispondente (lo stato è completato), puoi andare alla scheda Data output e quindi selezionare la tua sede Amazon S3 per visualizzare i risultati.

Modifica di un flusso di lavoro corrispondente

Per modificare un flusso di lavoro corrispondente:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Corrispondenza.
3. Scegli il flusso di lavoro corrispondente.
4. Nella pagina dei dettagli del flusso di lavoro corrispondente, nell'angolo in alto a destra, scegli Modifica.
5. Nella pagina Specificare i dettagli del flusso di lavoro corrispondente, apporta le modifiche necessarie, quindi scegli Avanti.
6. Nella pagina Scegli la tecnica corrispondente, apporta le modifiche necessarie, quindi scegli Avanti.
7. Nella pagina Specificare l'output dei dati, apporta le modifiche necessarie, quindi scegli Avanti.
8. Nella pagina Rivedi e salva, apporta le modifiche necessarie, quindi scegli Salva.

Eliminazione di un flusso di lavoro corrispondente

Per eliminare un flusso di lavoro corrispondente:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Corrispondenza.
3. Scegli il flusso di lavoro corrispondente.
4. Nella pagina dei dettagli del flusso di lavoro corrispondente, nell'angolo in alto a destra, scegli Elimina.

5. Conferma l'eliminazione, quindi scegli Elimina.

Ricerca di un Match ID per un flusso di lavoro di abbinamento basato su regole

Dopo aver eseguito un flusso di lavoro di abbinamento basato su regole, puoi trovare il Match ID corrispondente e la regola associata per i record elaborati.

Per trovare un Match ID per un flusso di lavoro di abbinamento basato su regole:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Corrispondenza.
3. Scegli il flusso di lavoro corrispondente basato su regole che è stato elaborato (lo stato del Job è Completato).
4. Nella pagina dei dettagli del flusso di lavoro corrispondente, scegli la scheda Trova ID corrispondente.
5. Esegui una di queste operazioni:

Se...	Allora...
Esiste solo una mappatura dello schema associata a questo flusso di lavoro.	Visualizza la mappatura dello schema selezionata per impostazione predefinita.
Esiste più di una mappatura dello schema associata a questo flusso di lavoro.	Scegli la mappatura dello schema dall'elenco a discesa.

6. Espandi le regole di abbinamento.
7. Inserisci un valore per ogni chiave Match.

   L'opzione Normalizza dati è selezionata per impostazione predefinita, in modo che gli input di dati vengano normalizzati prima della corrispondenza. Se non desiderate normalizzare i dati, deselezionate l'opzione Normalizza dati.

> **Tip**
>
> Inserisci quanti più valori puoi per aiutarti a trovare il Match ID.

8. Scegliere Look up (Cerca).
9. Visualizza il Match ID corrispondente e la regola associata utilizzata per la corrispondenza.

Eliminazione di record da un flusso di lavoro di abbinamento basato su regole o ML

Se devi rispettare le normative sulla gestione dei dati, puoi eliminare i record da un flusso di lavoro di abbinamento basato su regole o basato su ML.

Per eliminare i record da un flusso di lavoro di abbinamento basato su regole o ML

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Corrispondenza.
3. Scegli il flusso di lavoro di abbinamento basato su regole o basato su ML.
4. Nella pagina dei dettagli del flusso di lavoro corrispondente, scegli Elimina univoco IDs dall'elenco a discesa Azioni.
5. Inserisci l'ID univoco che desideri eliminare nella IDs sezione Univoco.

   Puoi inserire fino a 10 univociIDs.
6. Specificare la sorgente di input da cui eliminare l'univocoIDs.

   Se esiste una sola fonte di input per il flusso di lavoro, la fonte di input è elencata per impostazione predefinita.

   Se si specifica una sola fonte di input, l'univoca IDs delle altre fonti di input non ne risentirà.
7. Scegli Elimina univoco IDs.

Risoluzione dei problemi relativi ai flussi di lavoro corrispondenti

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare durante l'esecuzione di flussi di lavoro corrispondenti.

Ho ricevuto un file di errore dopo aver eseguito un flusso di lavoro corrispondente

Causa comune

Un workflow corrispondente può avere più esecuzioni e i risultati (successi o errori) vengono scritti in una cartella con `jobId` il nome.

I risultati positivi di un workflow corrispondente vengono scritti in una `success` cartella che contiene più file e ogni file contiene un sottoinsieme dei record riusciti.

Gli errori relativi a un flusso di lavoro corrispondente vengono scritti in una `error` cartella con più campi, ognuno dei quali contiene un sottoinsieme dei record di errore.

Il file di errore può essere creato per i seguenti motivi:

- L'ID univoco è:
  - null
  - mancante in una riga di dati
  - mancante in un record nella tabella dati
  - ripetuto in un'altra riga di dati nella tabella dati
  - non specificata
  - non univoco all'interno della stessa fonte
  - non univoco tra più fonti
  - si sovrappone tra le fonti
  - supera i 38 caratteri (solo flusso di lavoro di abbinamento basato su regole)
- Uno dei campi nella mappatura dello schema include un nome riservato:
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - MatchID

- HashingProtocol
- ConfidenceLevel
- Origine

> **Note**
>
> Se il record nel file di errore viene creato per i motivi elencati in precedenza, all'utente viene addebitato un costo, in quanto comporta il costo di elaborazione del servizio. Se il record nel file di errore è dovuto a un errore interno del server, non ti viene addebitato alcun costo.

Risoluzione

Per risolvere questo problema

1. Verifica se l'ID univoco è valido.

   Se l'ID univoco non è valido, aggiorna l'ID univoco nella tabella di dati, salva la nuova tabella di dati, crea una nuova mappatura dello schema ed esegui nuovamente il flusso di lavoro corrispondente.
2. Controlla se uno dei campi nella mappatura dello schema include un nome riservato.

   Se uno dei campi include un nome riservato, crea una nuova mappatura dello schema con un nuovo nome ed esegui nuovamente il flusso di lavoro corrispondente.

Mappa i dati di input utilizzando un flusso di lavoro di mappatura degli ID

Un flusso di lavoro di mappatura degli ID è un processo di elaborazione dei dati che mappa i dati da una fonte di dati di input a una destinazione di dati di input in base al metodo di mappatura ID specificato. Produce una tabella di mappatura degli ID.

Un flusso di lavoro di mappatura degli ID richiede un'origine dati di input e una destinazione di dati di input. L'origine e la destinazione di input dei dati dipendono dal tipo di mappatura degli ID che si desidera eseguire. Esistono due modi per eseguire la mappatura degli ID: servizi basati su regole o servizi forniti dal fornitore:

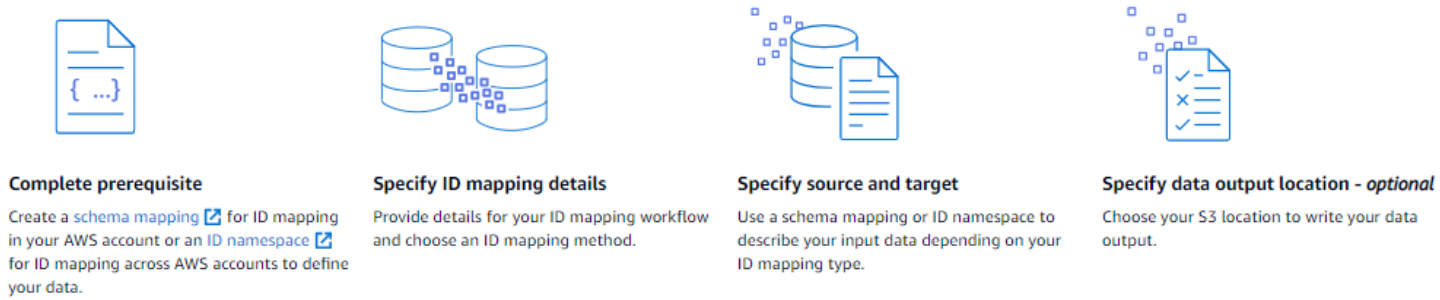
- Mappatura degli ID basata su regole: si utilizzano regole di corrispondenza per tradurre i dati di prime parti da un'origine a una destinazione.
- Mappatura degli ID dei servizi del fornitore: si utilizza il servizio del LiveRamp provider per tradurre i dati di terze parti da un'origine a una destinazione.

> **Note**
>
> Il flusso di lavoro di mappatura degli ID dei servizi del provider in AWS Entity Resolution è attualmente integrato con. LiveRamp Se hai un abbonamento al LiveRamp servizio, puoi creare un flusso di lavoro di mappatura degli ID con cui LiveRamp eseguire la transcodifica. Con la LiveRamp transcodifica, puoi tradurre un set di sorgenti R ampIDs in qualsiasi destinazione di destinazione RAMpiD. Utilizzando RAMpid come token per rappresentare i vostri clienti, potete evitare di condividere i dati dei clienti direttamente con le piattaforme pubblicitarie.
> Per ulteriori informazioni, consulta Perform Translation Through ADX sul sito Web della LiveRamp documentazione.

È possibile eseguire la mappatura degli ID tra due set di dati in uno dei seguenti scenari:

- All'interno del tuo Account AWS
- Tra due diversi Account AWS

Il diagramma seguente riassume come impostare un flusso di lavoro di mappatura degli ID.



Argomenti

- Flusso di lavoro di mappatura degli ID per uno Account AWS
- Flusso di lavoro di mappatura degli ID su due Account AWS
- Esecuzione di un workflow di mappatura degli ID
- Esecuzione di un flusso di lavoro di mappatura degli ID con una nuova destinazione di output
- Modifica di un flusso di lavoro di mappatura degli ID
- Eliminazione di un flusso di lavoro di mappatura degli ID
- Aggiungere o aggiornare una politica delle risorse per un flusso di lavoro di mappatura degli ID

Flusso di lavoro di mappatura degli ID per uno Account AWS

Un flusso di lavoro di mappatura degli ID, per esempio, Account AWS consente di eseguire autonomamente la mappatura degli ID tra due set di dati. Account AWS

Prima di creare autonomamente un flusso di lavoro di mappatura degli ID Account AWS, è necessario completare i prerequisiti.

Dopo aver creato ed eseguito un flusso di lavoro di mappatura degli ID, è possibile visualizzare l'output (la tabella di mappatura degli ID) e utilizzarlo per l'analisi.

I seguenti argomenti guidano l'utente attraverso una serie di passaggi per creare un flusso di lavoro di mappatura degli ID nello stesso. Account AWS

Argomenti

- Prerequisiti
- Creazione di un flusso di lavoro di mappatura degli ID (basato su regole)
- Creazione di un flusso di lavoro di mappatura degli ID (servizi del fornitore)

Prerequisiti

Prima di creare un flusso di lavoro di mappatura degli ID per una persona Account AWS utilizzando il metodo di mappatura degli ID basato su regole o il metodo di mappatura degli ID di Provider services, devi prima effettuare le seguenti operazioni:

- Completa le attività in Configurazione della risoluzione delle entità. AWS
- Crea una mappatura dello schema o Crea un flusso di lavoro corrispondente.
- (Solo mappatura degli ID dei servizi del provider) Prima di creare un flusso di lavoro di mappatura degli ID con LiveRamp, devi scegliere un bucket di data staging di Amazon Simple Storage Service (Amazon S3) in cui scrivere temporaneamente l'output del flusso di lavoro di mappatura degli ID.

  Se utilizzi il servizio del LiveRamp provider per tradurre dati di terze parti, aggiungi la seguente politica di autorizzazione, che ti consente di accedere al data staging bucket.

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

Nella precedente politica di autorizzazione, sostituisci ciascuna *<user input placeholder>* con le tue informazioni.

staging-bucket	Il bucket Amazon S3 che archivia temporane amente i dati durante l'esecuzione di un flusso di lavoro basato sui servizi del provider.

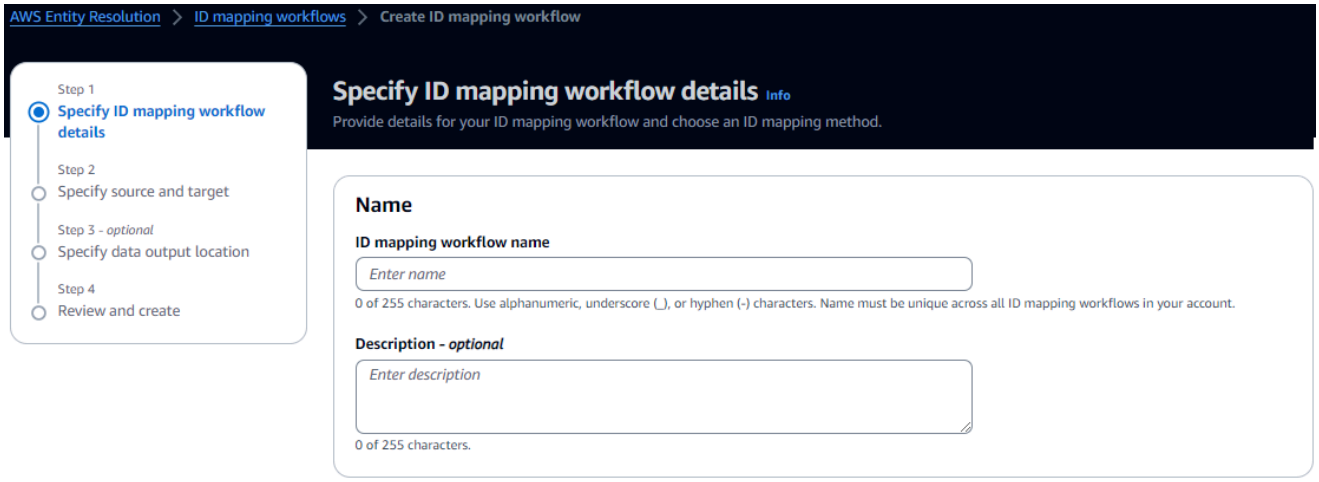
Creazione di un flusso di lavoro di mappatura degli ID (basato su regole)

Questo argomento descrive il processo di creazione di un flusso di lavoro di mappatura degli ID per uno Account AWS che utilizza regole di corrispondenza per tradurre dati di prime parti da un'origine a una destinazione.

Per creare un flusso di lavoro di mappatura degli ID basato su regole per una persona Account AWS

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Nella pagina Flussi di lavoro di mappatura degli ID, nell'angolo in alto a destra, scegli Crea flusso di lavoro di mappatura degli ID.
4. Per il passaggio 1: Specificare i dettagli del flusso di lavoro di mappatura degli ID, procedi come segue.

    a. Immettere il nome del flusso di lavoro di mappatura degli ID e una descrizione opzionale.



b. Per il metodo di mappatura degli ID, scegli Basato su regole.

c. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

d. Scegli Next (Successivo).

5. Per il passaggio 2: Specificate l'origine e la destinazione, effettuate le seguenti operazioni.

a. Per Origine, scegli lo scenario che ti riguarda e quindi esegui l'azione consigliata.

Scenario	Azione consigliata
Usa il tuo database AWS Glue, la tabella AWS Glue e la mappatura dello schema nel flusso di lavoro di mappatura degli ID.	1. Scegli Schema mapping. 2. Seleziona un AWS Gluedatabase dal menu a discesa, seleziona la AWS Glue tabella, quindi seleziona la mappatura dello schema corrispondente. È possibile aggiungere fino a 19 input di dati.
Utilizza un flusso di lavoro di abbinamento esistente che punti ai dati dei record che desideri utilizzare nel flusso di lavoro di mappatura degli ID.	1. Scegli il flusso di lavoro Matching. 2. Seleziona un flusso di lavoro Matching esistente dall'elenco a discesa.

b. Per Target, seleziona un flusso di lavoro Matching esistente dall'elenco a discesa.

c. Per i parametri delle regole, procedi come segue.

i. Specificate i controlli delle regole scegliendo una delle seguenti opzioni in base al tipo di origine.

Tipo di origine	Azione consigliata
Flusso di lavoro corrispondente	Specificate i controlli delle regole scegliendo se Source, Target o entrambi possono fornire regole in un flusso di lavoro di mappatura degli ID. I controlli delle regole devono essere compatibili tra l'origine e la destinazione da utilizzare in un flusso di lavoro di mappatura degli ID. Ad esempio, se lo spazio dei nomi dell'ID di origine limita le regole alla destinazione ma lo spazio dei nomi dell'ID di destinazione limita le regole all'origine, viene generato un errore.
Mappatura dello schema	Salta questo passaggio.

ii. Per i parametri di confronto e abbinamento, il tipo di confronto viene impostato automaticamente su Più campi di input.

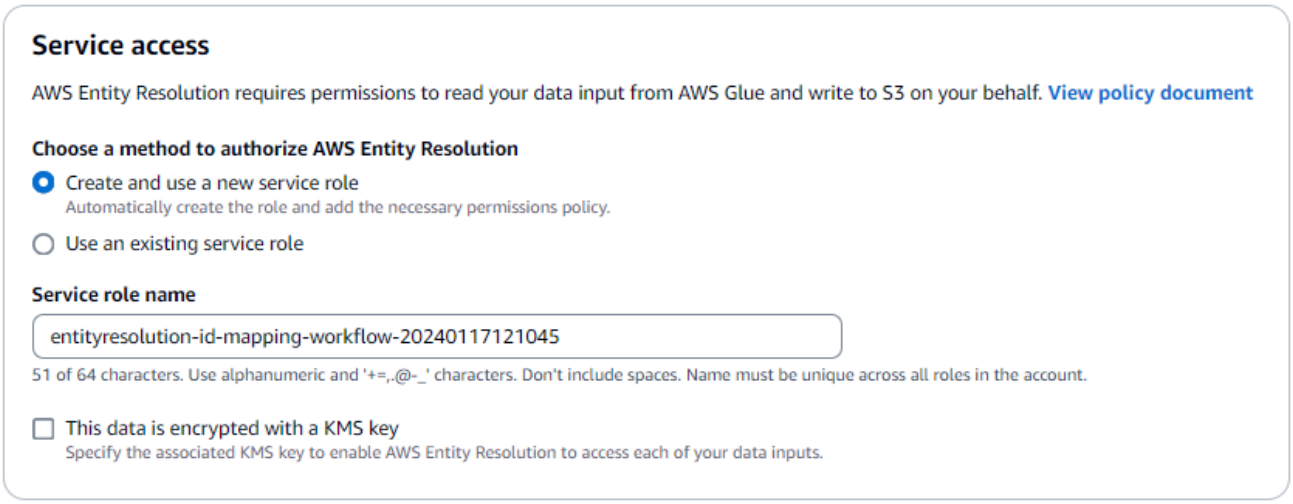
Questo perché entrambi i partecipanti avevano selezionato questa opzione in precedenza.

d. Specificate il tipo di record matching scegliendo una delle seguenti opzioni in base al vostro obiettivo.

Il tuo obiettivo	Opzione consigliata
Limita il tipo di corrispondenza dei record in modo da memorizzare solo un record corrispondente nell'origine per ogni record corrispondente nella destinazione quando crei il flusso di lavoro di mappatura degli ID.	Una fonte per una destinazione
Limita il tipo di corrispondenza dei record per memorizzare tutti i record corrispondenti nell'origine per ogni record corrispondente nella destinazione quando crei il flusso di lavoro di mappatura degli ID.	Molte fonti per un unico obiettivo

> **Note**
>
> È necessario specificare limitazioni compatibili per i namespace degli ID di origine e di destinazione.

e. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione ed esegui l'azione consigliata.



Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. Il nome del ruolo di servizio predefinito è`entityresolution-id-mapping-workflow-<timestamp>` . È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. Se i dati di input sono crittografati, scegli l'opzione Questi dati sono crittografati da una KMS chiave. Quindi, inserisci una AWS KMS chiave che viene utilizzata per decrittografare i dati in ingresso.

Opzione	Azione consigliata
Utilizza un ruolo di servizio esistente	Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. Se disponi delle autorizzazioni per elencare i ruoli, viene visualizzato l'elenco dei ruoli. Se non disponi delle autorizzazioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti , l'opzione Usa un ruolo di servizio esistente non è disponibile. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornar e la politica esistente sui ruoli per aggiungere le autorizzazioni necessarie.

6. Scegli Next (Successivo).
7. Per il passaggio 3: Specificare la posizione di output dei dati. Facoltativo, procedi come segue.
    a. Per Destinazione di output dei dati, procedi come segue:
        i. Scegli la posizione Amazon S3 per l'output dei dati.
        ii. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave ARN o scegli Crea una AWS KMS chiave.
    b. Scegli Next (Successivo).
8. Per il passaggio 4: revisione e creazione, procedi come segue.
    a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.
    b. Scegli Create (Crea) .

    Viene visualizzato un messaggio che indica che il flusso di lavoro di mappatura degli ID è stato creato.

Dopo aver creato il flusso di lavoro di mappatura degli ID, sei pronto per eseguire un flusso di lavoro di mappatura degli ID.

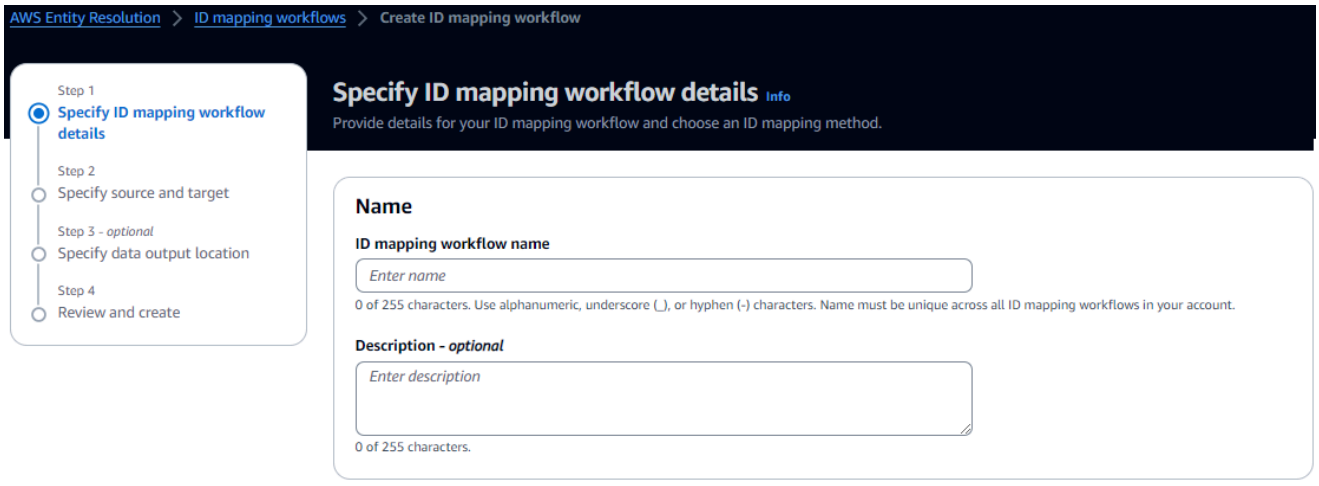
Creazione di un flusso di lavoro di mappatura degli ID (servizi del fornitore)

Questo argomento descrive il processo di creazione di un flusso di lavoro di mappatura degli ID per un utente che Account AWS utilizza un servizio di provider chiamato. LiveRamp LiveRamp traduce un set di sorgenti R ampIDs in un altro set usando R mantenuto o derivato. ampIDs

Per creare un flusso di lavoro di mappatura degli ID basato sui servizi del provider per uno Account AWS

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Nella pagina Flussi di lavoro di mappatura degli ID, nell'angolo in alto a destra, scegli Crea flusso di lavoro di mappatura degli ID.
4. Per il passaggio 1: Specificare i dettagli del flusso di lavoro di mappatura degli ID, procedi come segue.

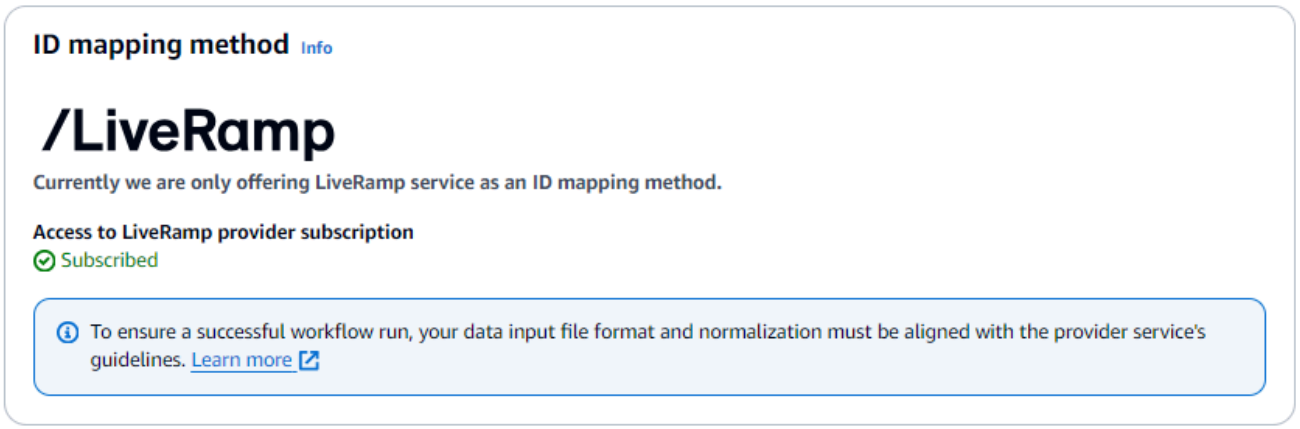
    a. Immettere il nome del flusso di lavoro di mappatura degli ID e una descrizione opzionale.



    b. Per il metodo di mappatura degli ID, scegli Provider services.

        AWS Entity Resolution attualmente offre il servizio del LiveRamp provider come metodo di mappatura degli ID. Se hai un abbonamento a LiveRamp, lo stato appare come Sottoscritto.

Per ulteriori informazioni su come abbonarsi LiveRamp, consultaFase 1: Abbonarsi a un servizio fornito da un provider su AWS Data Exchange.



> **Note**
>
> Assicurati che il formato del file di input dei dati sia conforme alle linee guida del servizio del provider. Per ulteriori informazioni sulle linee guida per LiveRamp la formattazione dei file di input, consulta Perform Translation Through nel ADX sito Web della LiveRamp documentazione.

c. Per la LiveRamp configurazione, inserisci i seguenti valori che LiveRamp forniscono:

- Gestione degli ID client ARN
- Responsabile segreto del cliente ARN

d. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

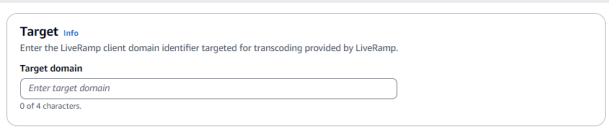
e. Scegli Next (Successivo).

5. Per il passaggio 2: Specificate l'origine e la destinazione, effettuate le seguenti operazioni.

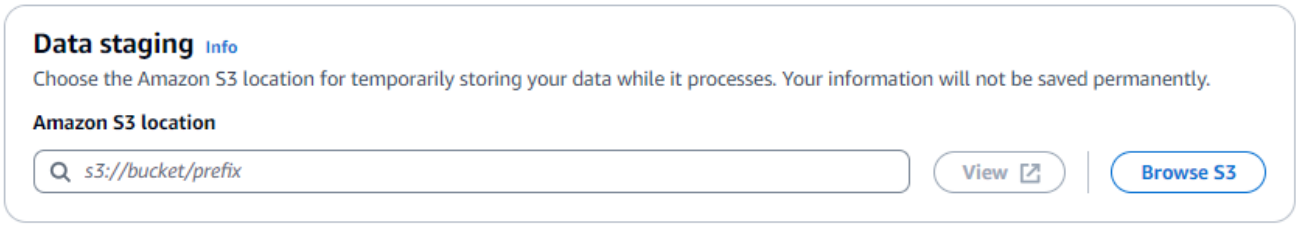
   a. Per Origine, scegli lo scenario che ti riguarda e quindi esegui l'azione consigliata.

Scenario	Azione consigliata
Usa il tuo database AWS Glue, la tabella AWS Glue e la mappatura dello schema nel flusso di lavoro di mappatura degli ID.	1. Scegli Schema mapping. 2. Seleziona un AWS Gluedatabase dal menu a discesa, seleziona la AWS Glue tabella, quindi seleziona la mappatura dello schema corrispondente. È possibile aggiungere fino a 19 input di dati.
Utilizza un flusso di lavoro di abbinamento esistente che punti ai dati dei record che desideri utilizzare nel flusso di lavoro di mappatura degli ID.	1. Scegli il flusso di lavoro Matching. 2. Seleziona un flusso di lavoro Matching esistente dall'elenco a discesa.

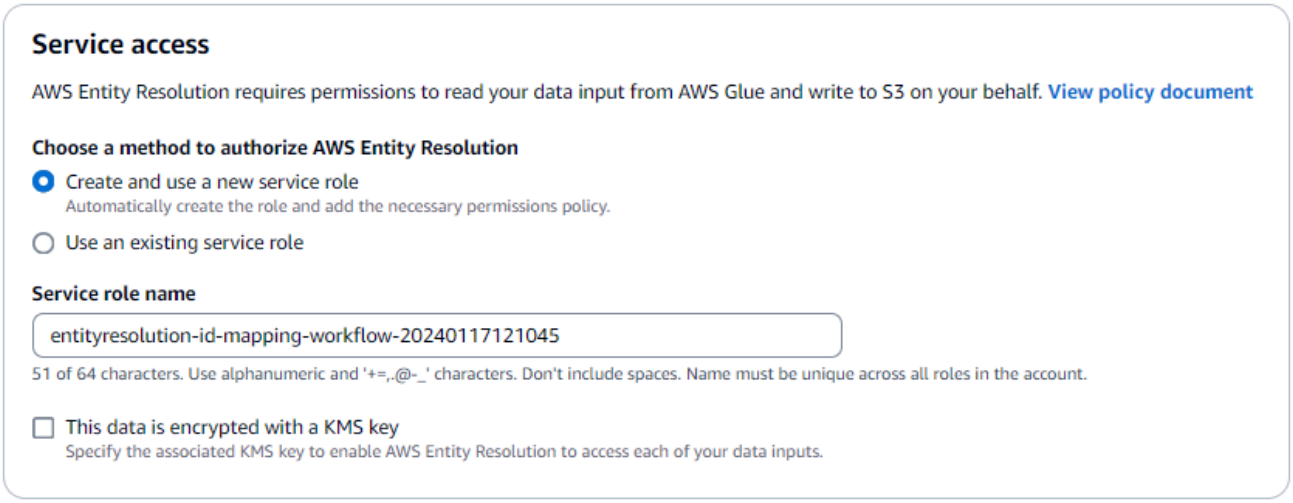
   b. Per Target, esegui una delle seguenti azioni in base al metodo di mappatura degli ID scelto.

Metodo di mappatura degli ID	Azione consigliata
Basato su regole	Seleziona un flusso di lavoro Matching esistente dall'elenco a discesa.
Servizi del fornitore	Inserisci l'identificatore LiveRamp del dominio client destinato alla transcodifica LiveRamp fornito nel dominio Target. 

c. Per lo staging dei dati, scegli la posizione Amazon S3 in cui desideri scrivere temporaneamente l'output del flusso di lavoro di mappatura degli ID.



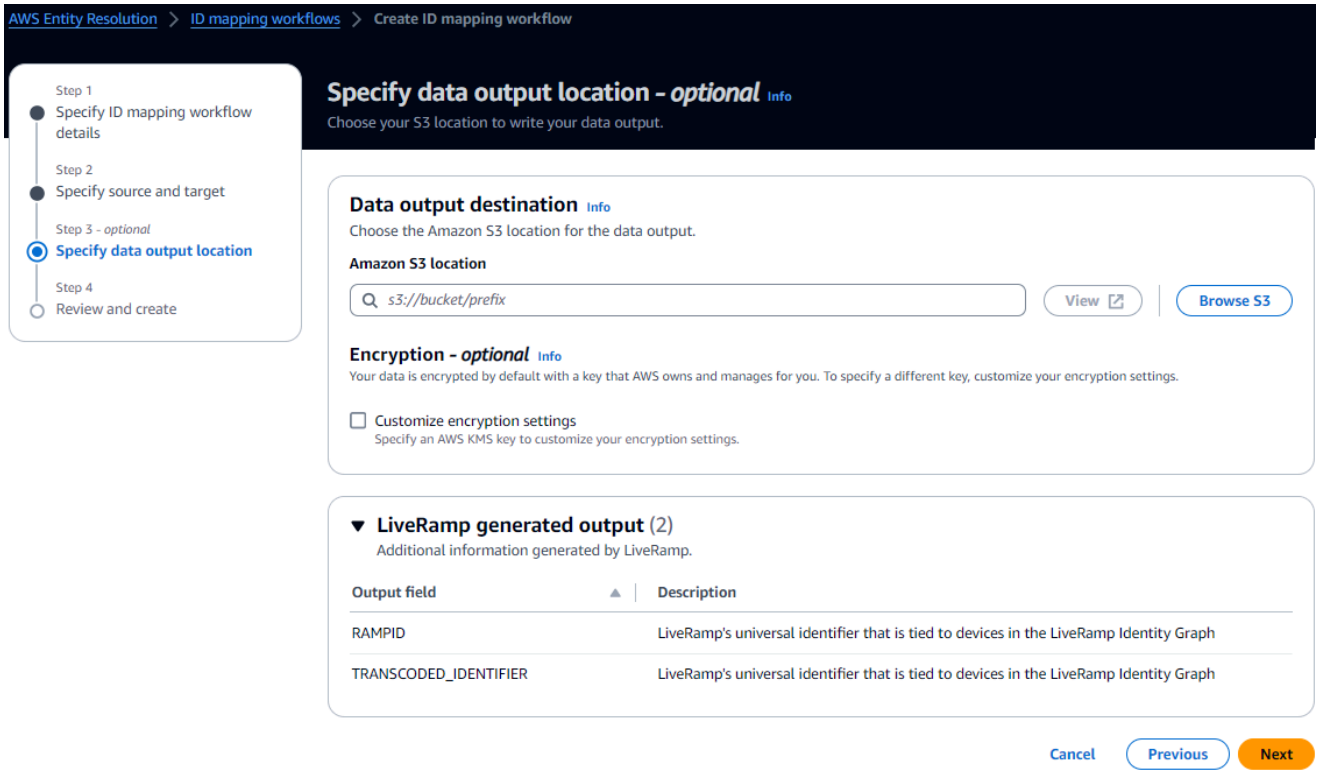
d. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione e intraprendi l'azione consigliata.



Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. Il nome del ruolo di servizio predefinito è`entityresolution-id-mapping-workflow-<timestamp>` . È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. Se i dati di input sono crittografati, scegli l'opzione Questi dati sono crittografati da una KMS chiave. Quindi, inserisci una AWS KMS chiave che viene utilizzata per decrittografare i dati in ingresso.

Opzione	Azione consigliata
Utilizza un ruolo di servizio esistente	Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. Se disponi delle autorizzazioni per elencare i ruoli, viene visualizzato l'elenco dei ruoli. Se non disponi delle autorizzazioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibi le. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiungere le autorizzazioni necessarie.

6. Scegli Next (Successivo).
7. Per il passaggio 3: Specificare la posizione di output dei dati. Facoltativo, procedi come segue.
   a. Per Destinazione di output dei dati, procedi come segue:
      i. Scegli la posizione Amazon S3 per l'output dei dati.
      ii. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave ARN o scegli Crea una AWS KMS chiave.
   b. Visualizza l'output LiveRamp generato.
   c. Scegli Next (Successivo).



8. Per il passaggio 4: revisione e creazione, procedi come segue.

   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

   b. Scegli Create (Crea) .

      Viene visualizzato un messaggio che indica che il flusso di lavoro di mappatura degli ID è stato creato.

9. Dopo aver creato il flusso di lavoro di mappatura degli ID, sei pronto per eseguire un flusso di lavoro di mappatura degli ID.

Flusso di lavoro di mappatura degli ID su due Account AWS

Un flusso di lavoro di mappatura degli ID su due Account AWS consente di eseguire la mappatura degli ID tra due set di dati su due. Account AWS Questa operazione viene in genere eseguita tra il proprio Account AWS e l'altro. Account AWS

Ad esempio, un publisher può creare un flusso di lavoro di mappatura degli ID utilizzando il proprio spazio dei nomi degli ID di destinazione (nel proprio Account AWS) e lo spazio dei nomi degli ID di origine di un inserzionista (in un altro). Account AWS

Prima di creare un flusso di lavoro di mappatura degli ID su due Account AWS, devi prima completare i prerequisiti.

Dopo aver creato un flusso di lavoro di mappatura degli ID, è possibile visualizzare l'output (la tabella di mappatura degli ID) e utilizzarlo per l'analisi.

I seguenti argomenti guidano l'utente attraverso una serie di passaggi per creare un flusso di lavoro di mappatura degli ID tra due: Account AWS

Argomenti

Prerequisiti

Prima di creare un flusso di lavoro di mappatura degli ID su due Account AWS, devi prima effettuare le seguenti operazioni:

- Completare le operazioni descritte in Configurare AWS Entity Resolution.
- Crea una fonte di namespace ID.
- Crea un target ID namespace.
- Acquisisci lo spazio dei nomi ID ARN se utilizzi un'origine dello spazio dei nomi ID da un'altra. Account AWS
- (Solo servizi per provider) La creazione di un flusso di lavoro di mappatura degli ID su due piattaforme Account AWS richiede l'autorizzazione per accedere LiveRamp al bucket S3 e alla () chiave gestita dal cliente. AWS Key Management Service AWS KMS

  Prima di creare un flusso di lavoro di mappatura degli ID su due Account AWS con LiveRamp, aggiungi la seguente politica di autorizzazione, che consente di accedere LiveRamp al bucket S3 e alla chiave gestita dal 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"
            }
        }
    }]
}
```

Nella precedente politica di autorizzazione, sostituisci ciascuna *<user input placeholder>* con le tue informazioni.

<KMSKeyARN>	ARNDi una chiave gestita dal AWS KMS cliente.

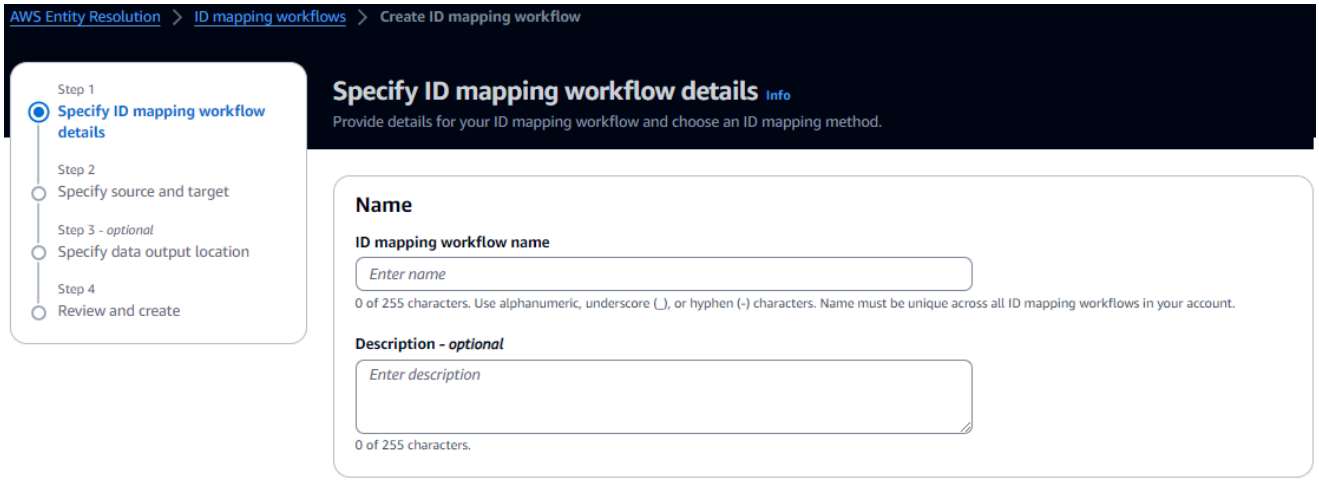
Creazione di un flusso di lavoro di mappatura degli ID (basato su regole)

Dopo aver completato i prerequisiti, puoi creare uno o più flussi di lavoro di mappatura degli ID per utilizzare le regole di corrispondenza per tradurre i dati di prime parti da una fonte a una destinazione.

Per creare un flusso di lavoro di mappatura degli ID basato su regole su due Account AWS

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Nella pagina Flussi di lavoro di mappatura degli ID, nell'angolo in alto a destra, scegli Crea flusso di lavoro di mappatura degli ID.
4. Per il passaggio 1: Specificare i dettagli del flusso di lavoro di mappatura degli ID, procedi come segue.

    a. Immettere il nome del flusso di lavoro di mappatura degli ID e una descrizione opzionale.



b. Per il metodo di mappatura degli ID, scegli Basato su regole.

c. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

d. Scegli Next (Successivo).

5. Per il passaggio 2: Specificate l'origine e la destinazione, effettuate le seguenti operazioni.

a. Attiva le opzioni avanzate.

b. Per Origine, scegli Flusso di lavoro corrispondente, quindi seleziona il flusso di lavoro Matching esistente dall'elenco a discesa.

c. Per Target, scegli Flusso di lavoro corrispondente, quindi seleziona il flusso di lavoro Matching esistente dall'elenco a discesa.

d. Per i parametri delle regole, specifica i controlli delle regole scegliendo se una sorgente o una destinazione possono fornire regole in un flusso di lavoro di mappatura degli ID.

   I controlli delle regole devono essere compatibili tra l'origine e la destinazione da utilizzare in un flusso di lavoro di mappatura degli ID. Ad esempio, se lo spazio dei nomi dell'ID di origine limita le regole alla destinazione ma lo spazio dei nomi dell'ID di destinazione limita le regole all'origine, viene generato un errore.

e. Per i parametri di confronto e abbinamento, procedi come segue.

   i. Specificate il tipo di confronto scegliendo un'opzione in base al vostro obiettivo.

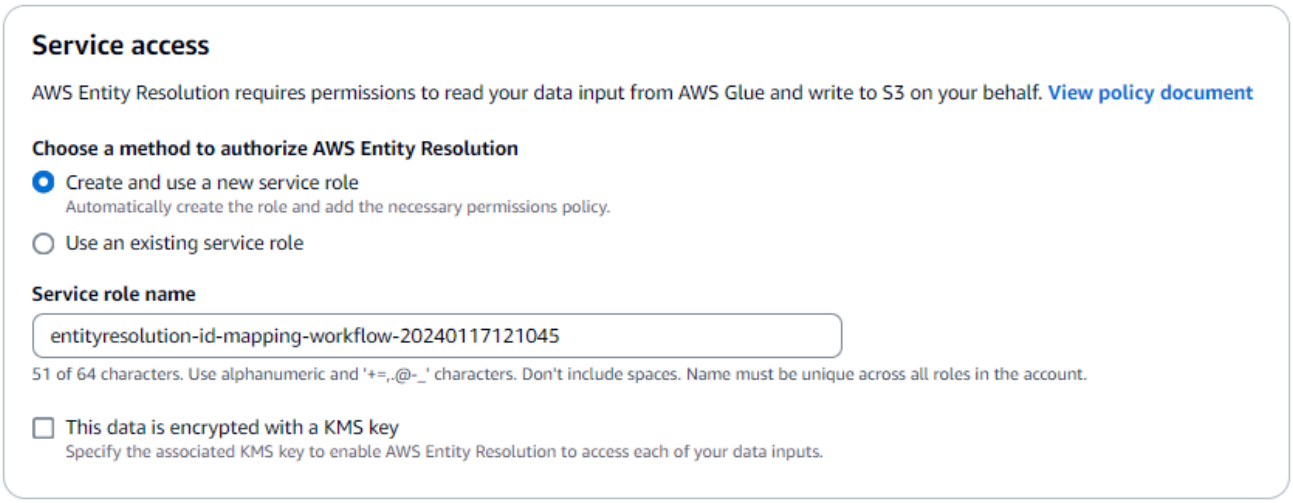
Il tuo obiettivo	Opzione consigliata
Trova qualsiasi combinazione di corrispondenze tra i dati archiviati in più campi di input, indipendentemente dal fatto che i dati si trovino nello stesso campo di input o in un campo di input diverso.	Campi di input multipli
Limita il confronto all'interno di un singolo campo di input, quando dati simili memorizzati in più campi di input non devono corrispondere.	Campo di input singolo

ii. Specificate il tipo di record matching scegliendo un'opzione in base al vostro obiettivo.

Il tuo obiettivo	Opzione consigliata
Limita il tipo di corrispondenza dei record in modo da memorizzare solo un record corrispondente nell'origine per ogni record corrispondente nella destinazione quando crei il flusso di lavoro di mappatura degli ID.	Una fonte per una destinazione
Limita il tipo di corrispondenza dei record per memorizzare tutti i record corrispondenti nell'origine per ogni record corrispondente nella destinazi one quando crei il flusso di lavoro di mappatura degli ID.	Molte fonti per un unico obiettivo

> **Note**
>
> È necessario specificare limitazioni compatibili per i namespace degli ID di origine e di destinazione.

f. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione ed esegui l'azione consigliata.



Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. Il nome del ruolo di servizio predefinito è`entityresolution-id-mapping-workflow-<timestamp>` . È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. Se i dati di input sono crittografati, scegli l'opzione Questi dati sono crittografati da una KMS chiave. Quindi, inserisci una AWS KMS chiave che viene utilizzata per decrittografare i dati in ingresso.

Opzione	Azione consigliata
Utilizza un ruolo di servizio esistente	Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. Se disponi delle autorizzazioni per elencare i ruoli, viene visualizzato l'elenco dei ruoli. Se non disponi delle autorizzazioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibi le. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiungere le autorizzazioni necessarie.

6. Scegli Next (Successivo).
7. Per il passaggio 3: Specificare la posizione di output dei dati. Facoltativo, procedi come segue.
    a. Per Destinazione di output dei dati, procedi come segue.
        i. Scegli la posizione Amazon S3 per l'output dei dati.
        ii. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave ARN o scegli Crea una AWS KMS chiave.
    b. Visualizza l'output LiveRamp generato.
    c. Scegli Next (Successivo).
8. Per il passaggio 4: revisione e creazione, procedi come segue.

a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

b. Scegli Create (Crea) .

   Viene visualizzato un messaggio che indica che il flusso di lavoro di mappatura degli ID è stato creato.

Dopo aver creato il flusso di lavoro di mappatura degli ID, sei pronto per eseguire un flusso di lavoro di mappatura degli ID.

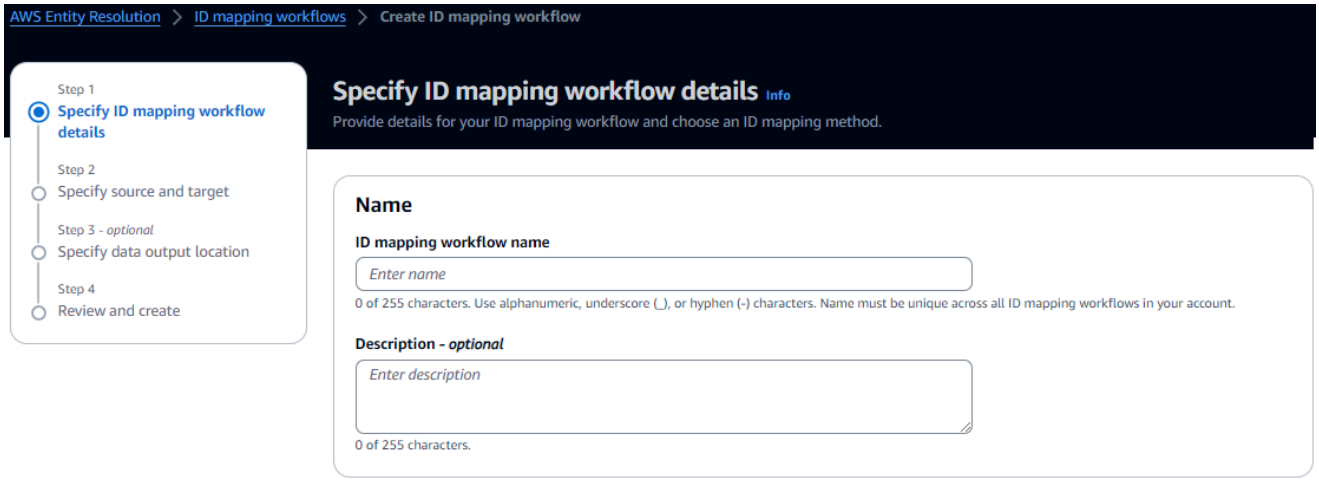
Creazione di un flusso di lavoro di mappatura degli ID (servizi del fornitore)

Dopo aver completato i prerequisiti, puoi creare uno o più flussi di lavoro di mappatura degli ID utilizzando il servizio del provider. LiveRamp LiveRamp traduce un set di sorgenti R ampIDs in un altro set usando R mantenuto o derivato. ampIDs

Per creare un flusso di lavoro di mappatura degli ID utilizzando il servizio del provider

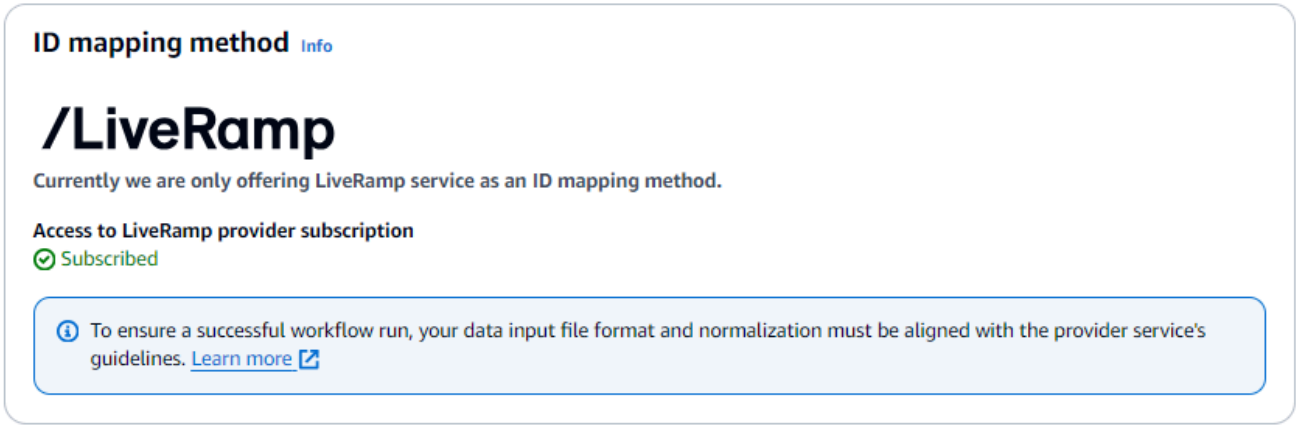
1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Nella pagina Flussi di lavoro di mappatura degli ID, nell'angolo in alto a destra, scegli Crea flusso di lavoro di mappatura degli ID.
4. Per il passaggio 1: Specificare i dettagli del flusso di lavoro di mappatura degli ID, procedi come segue.

   a. Immettere il nome del flusso di lavoro di mappatura degli ID e una descrizione opzionale.



b. Per il metodo di mappatura degli ID, scegli Provider services.

AWS Entity Resolution attualmente offre il servizio del LiveRamp provider come metodo di mappatura degli ID. Se hai un abbonamento a LiveRamp, lo stato appare come Sottoscritto. Per ulteriori informazioni su come abbonarsi LiveRamp, consultaFase 1: Abbonarsi a un servizio fornito da un provider su AWS Data Exchange.



> **Note**
>
> Assicurati che il formato del file di input dei dati sia conforme alle linee guida del servizio del provider. Per ulteriori informazioni sulle linee guida per LiveRamp la formattazione dei file di input, consulta Perform Translation Through nel ADX sito Web della LiveRamp documentazione.

c. Per la LiveRamp configurazione, inserisci i seguenti valori che LiveRamp forniscono:

- Gestione degli ID client ARN
- Responsabile segreto del cliente ARN

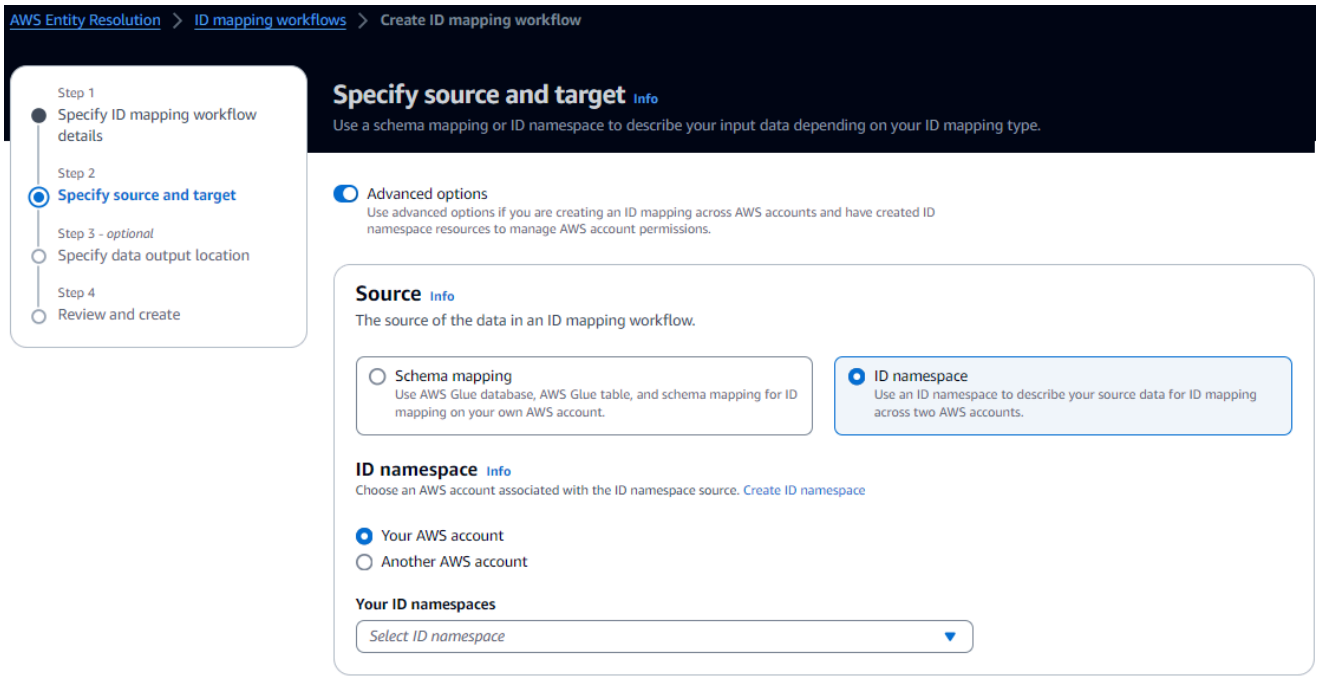
d. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

e. Scegli Next (Successivo).

5. Per il passaggio 2: Specificate l'origine e la destinazione, effettuate le seguenti operazioni.

a. Attiva le opzioni avanzate.

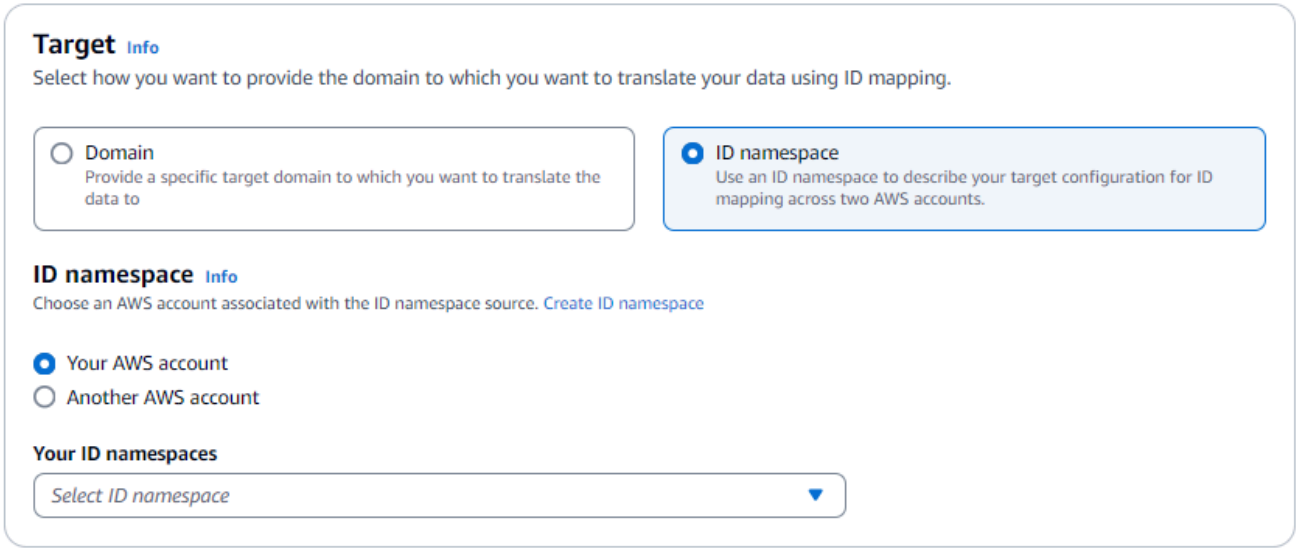
b. Per Source, scegli ID namespace.



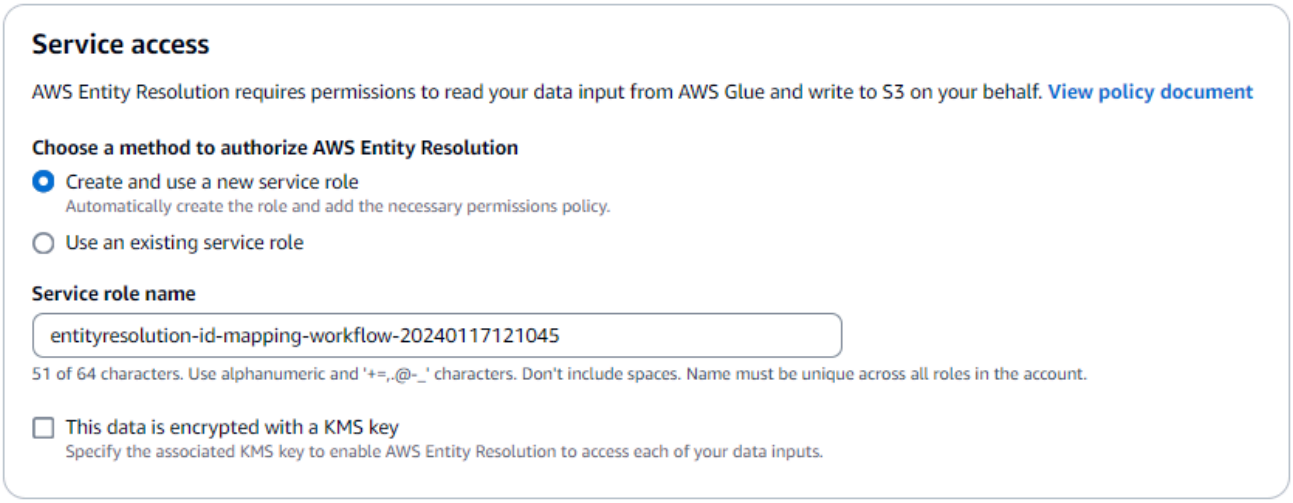
c. Per lo spazio dei nomi ID, identifica dove si trova lo spazio dei nomi ID, quindi esegui l'azione consigliata.

Ubicazione dello spazio dei nomi ID	Azione consigliata
La tua Account AWS	1. Scegli il tuo Account AWS. 2. Seleziona lo spazio dei nomi ID dall'elenco a discesa I tuoi spazi dei nomi ID.
Di qualcun altro Account AWS	1. Scegli un altro Account AWS. 2. Inserisci lo spazio dei nomi ARN ID.

d. Per Target, scegli lo spazio dei nomi ID.



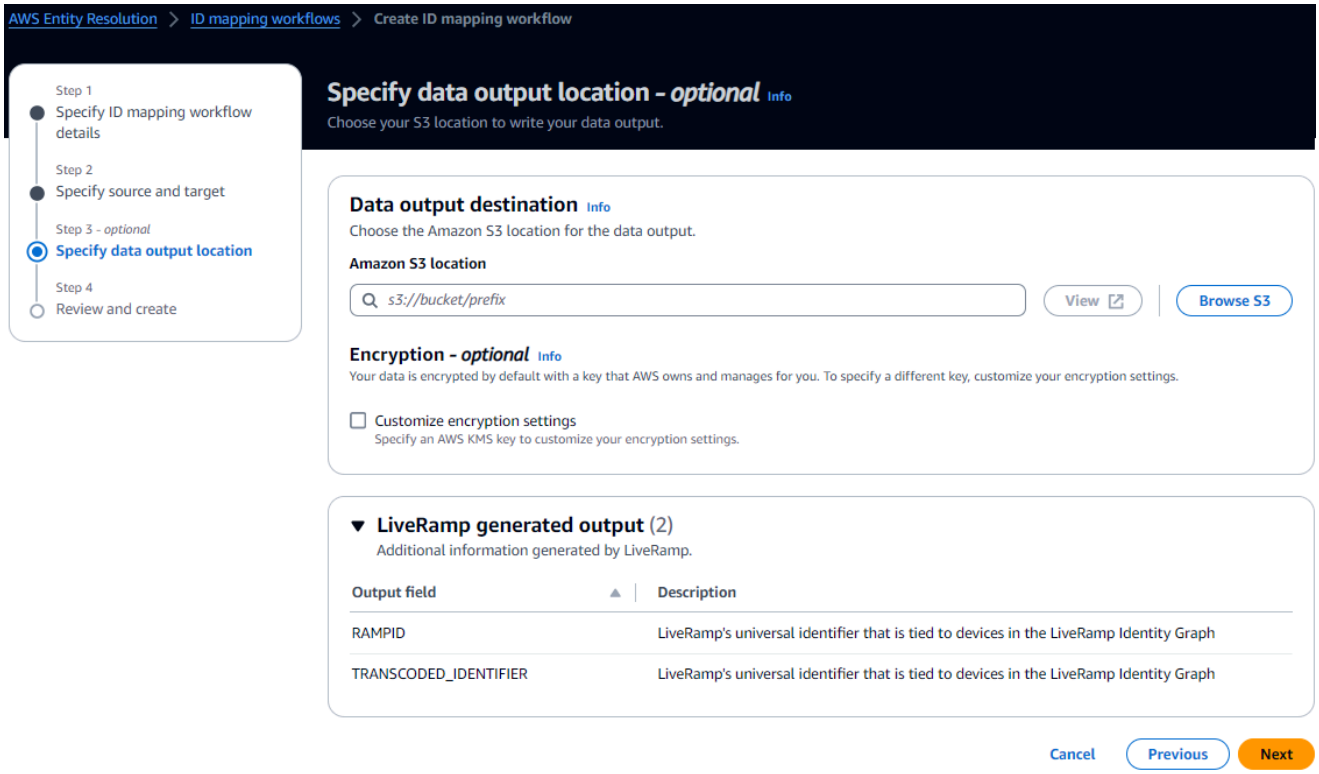
e. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione e intraprendi l'azione consigliata.



Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. Il nome del ruolo di servizio predefinito è`entityresolution-id-mapping-workflow-<timestamp>` . È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. Se i dati di input sono crittografati, scegli l'opzione Questi dati sono crittografati da una KMS chiave. Quindi, inserisci una AWS KMS chiave che viene utilizzata per decrittografare i dati in ingresso.

Opzione	Azione consigliata
Utilizza un ruolo di servizio esistente	Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. Se disponi delle autorizzazioni per elencare i ruoli, viene visualizzato l'elenco dei ruoli. Se non disponi delle autorizzazioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibi le. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiungere le autorizzazioni necessarie.

6. Scegli Next (Successivo).
7. Per il passaggio 3: Specificare la posizione di output dei dati. Facoltativo, procedi come segue.
   a. Per Destinazione di output dei dati, procedi come segue.
      i. Scegli la posizione Amazon S3 per l'output dei dati.
      ii. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave ARN o scegli Crea una AWS KMS chiave.
   b. Visualizza l'output LiveRamp generato.
   c. Scegli Next (Successivo).



8. Per il passaggio 4: revisione e creazione, procedi come segue.

   a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

   b. Scegli Create (Crea) .

      Viene visualizzato un messaggio che indica che il flusso di lavoro di mappatura degli ID è stato creato.

Dopo aver creato il flusso di lavoro di mappatura degli ID, sei pronto per eseguire un flusso di lavoro di mappatura degli ID.

Esecuzione di un workflow di mappatura degli ID

Dopo aver creato un flusso di lavoro di mappatura degli ID per uno Account AWS o creato un flusso di lavoro di mappatura degli ID tra due Account AWS, puoi eseguire il flusso di lavoro di mappatura degli ID. Il flusso di lavoro di mappatura degli ID genera un file. CSV

Per eseguire un flusso di lavoro di mappatura degli ID

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Scegli il flusso di lavoro di mappatura degli ID.
4. Nella pagina dei dettagli del flusso di lavoro di mappatura degli ID, nell'angolo in alto a destra, scegli Esegui.
5. Nella pagina dei dettagli del flusso di lavoro corrispondente, nella scheda Metriche, visualizza quanto segue in Metriche dell'ultimo lavoro:

   - Il Job ID
   - L'ora di completamento del processo del flusso di lavoro
   - Lo stato del processo del flusso di lavoro corrispondente: In coda, In corso, Completato, Non riuscito
   - Il numero di record elaborati
   - Il numero di record non elaborati
   - Il numero di record di input

   In Cronologia lavori, puoi anche visualizzare le metriche dei lavori del flusso di lavoro di mappatura degli ID eseguiti in precedenza.
6. Una volta completato il processo di mappatura degli ID (lo stato è Completato), scegli Data output, quindi scegli la tua posizione Amazon S3 per visualizzare i risultati.

   Dopo aver ricevuto il CSV file, puoi unirti a. `RAMPID` `TRANSCODED_ID`

Esecuzione di un flusso di lavoro di mappatura degli ID con una nuova destinazione di output

Dopo aver creato un flusso di lavoro di mappatura degli ID per uno Account AWS o creato un flusso di lavoro di mappatura degli ID tra due Account AWS, puoi scegliere una posizione S3 diversa per scrivere l'output dei dati.

Per eseguire un flusso di lavoro di mappatura degli ID con una nuova destinazione di output

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Scegli il flusso di lavoro di mappatura degli ID.
4. Nella pagina dei dettagli del flusso di lavoro di mappatura degli ID, nell'angolo in alto a destra, scegli Esegui con nuova destinazione di output dall'elenco a discesa Esegui flusso di lavoro.
5. Per Destinazione di output dei dati, procedi come segue.
   a. Scegli la posizione Amazon S3 per l'output dei dati.
   b. Per la crittografia, se scegli di personalizzare le impostazioni di crittografia, inserisci la AWS KMS chiave ARN o scegli Crea una AWS KMS chiave.
6. Per specificare le autorizzazioni di accesso al servizio, scegli un'opzione e intraprendi l'azione consigliata.

Opzione	Azione consigliata
Crea e utilizza un nuovo ruolo di servizio	AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella. Il nome del ruolo di servizio predefinito è`entityresolution-id-mapping-workflow-<timestamp>` . È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. Se i dati di input sono crittografati, scegli l'opzione Questi dati sono crittografati da una KMS chiave. Quindi, inserisci una AWS KMS

Opzione	Azione consigliata
	chiave che viene utilizzata per decrittografare i dati in ingresso.
Utilizza un ruolo di servizio esistente	Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. Se disponi delle autorizzazioni per elencare i ruoli, viene visualizzato l'elenco dei ruoli. Se non disponi delle autorizzazioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibi le. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiungere le autorizzazioni necessarie.

7. Seleziona Esegui.
8. Nella pagina dei dettagli del flusso di lavoro corrispondente, nella scheda Metriche, visualizza quanto segue in Metriche dell'ultimo lavoro:

   - Il Job ID
   - L'ora di completamento del processo del flusso di lavoro
   - Lo stato del processo del flusso di lavoro corrispondente: In coda, In corso, Completato, Non riuscito
   - Il numero di record elaborati

- Il numero di record non elaborati
- Il numero di record di input

In Cronologia lavori, puoi anche visualizzare le metriche dei lavori del flusso di lavoro di mappatura degli ID eseguiti in precedenza.

9. Una volta completato il processo di mappatura degli ID (lo stato è Completato), scegli Data output, quindi scegli la tua posizione Amazon S3 per visualizzare i risultati.

   Dopo aver ricevuto il CSV file, puoi unirti a. `RAMPID TRANSCODED_ID`

Modifica di un flusso di lavoro di mappatura degli ID

Per modificare un flusso di lavoro di mappatura degli ID:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Scegli il flusso di lavoro di mappatura degli ID.
4. Nella pagina dei dettagli del flusso di lavoro di mappatura degli ID, nell'angolo in alto a destra, scegli Modifica.
5. Nella pagina dei dettagli del flusso di lavoro Specificare la mappatura degli ID, apporta le modifiche necessarie, quindi scegli Avanti.
6. Nella pagina Specificare l'output dei dati, apporta le modifiche necessarie, quindi scegli Avanti.
7. Nella pagina Rivedi e salva, apporta le modifiche necessarie, quindi scegli Salva.

Eliminazione di un flusso di lavoro di mappatura degli ID

Per eliminare un flusso di lavoro di mappatura degli ID:

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Scegli il flusso di lavoro di mappatura degli ID.

4. Nella pagina dei dettagli del flusso di lavoro di mappatura degli ID, nell'angolo in alto a destra, scegli Elimina.
5. Conferma l'eliminazione, quindi scegli Elimina.

Aggiungere o aggiornare una politica delle risorse per un flusso di lavoro di mappatura degli ID

Una politica delle risorse consente al creatore della risorsa di mappatura degli ID di accedere alla risorsa del flusso di lavoro di mappatura degli ID.

Per aggiungere o aggiornare una politica delle risorse

1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Scegli il flusso di lavoro di mappatura degli ID.
4. Nella pagina dei dettagli del flusso di lavoro di mappatura degli ID, scegli la scheda Autorizzazioni.
5. Nella sezione Politica delle risorse, scegli Modifica.
6. Aggiungi o aggiorna la politica nell'JSONeditor.
7. Scegli Save changes (Salva modifiche).

Integrazione con AWS Entity Resolution come provider

AWS Entity Resolution le integrazioni con fornitori terzi aiutano i clienti a proteggere la privacy dei consumatori e a mantenere la conformità alle leggi sulla sovranità dei dati. I fornitori terzi, come LiveRamp and TransUnion, traducono gli identificativi dei consumatori in pubblicitàIDs, come Ramp e Fabrick. IDs IDs Questi identificatori pubblicitari sono comunemente utilizzati negli strumenti pubblicitari e di marketing, per impedire che i dati dei consumatori vengano esportati su sistemi non gestiti.AWS Questa sezione fornisce ai fornitori indicazioni su come integrarsi per codificare o AWS Entity Resolution transcodificare gli identificativi dei consumatori in pubblicità da utilizzare in un flusso di lavoro di IDs abbinamento basato sui servizi del fornitore.

Per ulteriori informazioni sui servizi del provider con cui sono attualmente integrati, vedere. AWS Entity ResolutionCreazione di un flusso di lavoro di abbinamento basato sui servizi del provider

Argomenti

Requisiti

Prima di effettuare l'integrazione come provider di servizi con AWS Entity Resolution, completa i seguenti requisiti.

Argomenti

Elenca un servizio fornito da un provider su AWS Data Exchange

In qualità di fornitore terzo, devi inserire il tuo prodotto nel catalogo prodotti AWSData Exchange (ADX). Dopo che il prodotto è stato inserito nel catalogo AWS Data Exchange prodotti, gli abbonati possono abbonarsi al prodotto tramite un'offerta pubblica o privata.

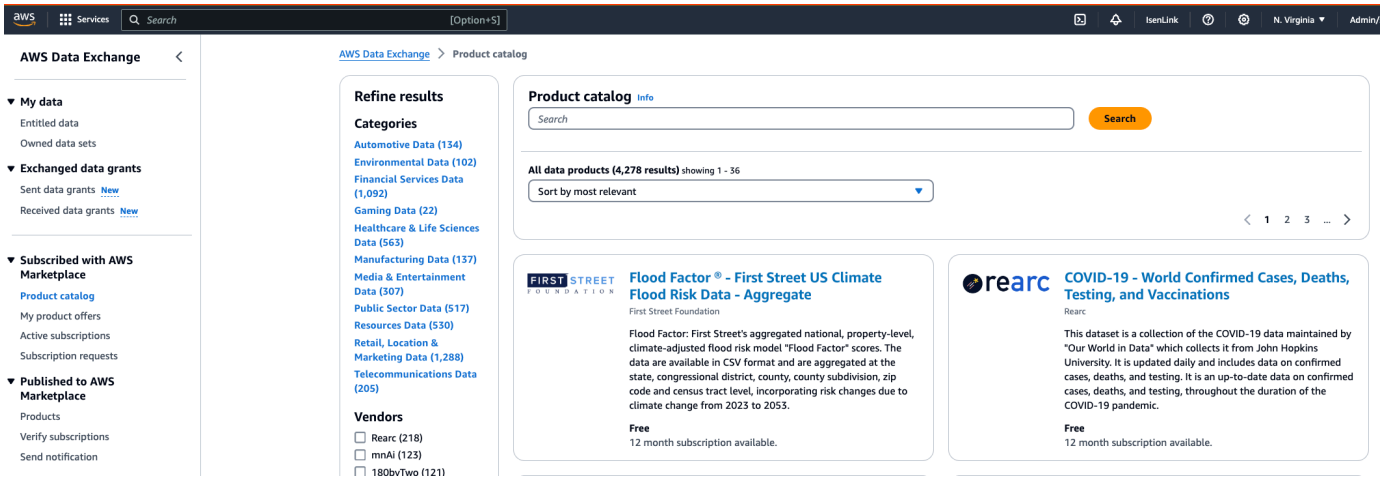
Per inserire un fornitore di servizi su AWS Data Exchange

1. Se sei un nuovo fornitore di prodotti di dati AWS Data Exchange, completa i passaggi nella sezione intitolata Guida introduttiva come fornitore nella Guida per l'AWS Data Exchange utente.
2. Crea un set di REST API dati e pubblica un nuovo prodotto contenente APIs on AWS Data Exchange seguendo i passaggi indicati nella sezione intitolata Come pubblicare un prodotto contenuto APIs nella Guida per l'AWS Data Exchange utente. È possibile completare il processo utilizzando la AWS Data Exchange console o il AWS Command Line Interface.

   Se hai impostato la visibilità del prodotto Pubblica, l'offerta pubblica è disponibile per tutti gli abbonati.

   Se hai impostato la visibilità del prodotto Privata, completa i passaggi nella sezione intitolata Crea offerte personalizzate nella Guida per l'AWS Data Exchange utente, a seconda del tuo caso d'uso.

   L'immagine seguente mostra un esempio di prodotto disponibile nel Catalogo AWS Data Exchange prodotti.



3. Dopo che il prodotto è disponibile nel Catalogo AWS Data Exchange prodotti, l'abbonato può abbonarsi al prodotto nei seguenti modi.

   - Abbonati al prodotto pubblico.
   - Utilizza un'offerta privata (offerta personalizzata) emessa dal servizio del fornitore.
   - Utilizza un'offerta Bring Your Own Subscription (BYOS).

Per ulteriori informazioni, consulta Abbonarsi e accedere a un prodotto contenuto APIs nella Guida AWS Data Exchange per l'utente.

Identifica i tuoi attributi

Gli attributi dei dati di input sono le definizioni dei tipi delle entità da risolvere in un flusso di lavoro. Alcuni esempi di attributi sono `FirstNameLastName`,`Email`, o`Custom String`.

Quando identificate gli attributi, dovreste prendere nota di eventuali requisiti o linee guida.

Example Esempio

Di seguito è riportato un esempio di convalida per l'identificazione degli attributi del fornitore.

- L'`LastName`attributo `FirstName` or è obbligatorio.
- Se l'`Email`attributo è presente, deve essere sottoposto a hash.

In qualità di provider, è necessario identificare gli attributi del prodotto di servizio fornito dal provider e quindi comunicarli al team di sviluppo AWS Entity Resolution aziendale all'indirizzo `<aws-entity-resolution-bd@amazon .com>` per un'ulteriore convalida prima di procedere.

Richiedi la specifica Open AWS Entity Resolution API

AWS Entity Resolution dispone di una API specifica Open che il provider può utilizzare come handshake che contiene gli elementi APIs coinvolti nell'integrazione. Per ulteriori informazioni, consulta Utilizzo della API specifica AWS Entity Resolution Open.

Per richiedere la API definizione Open, contatta il team di AWS Entity Resolution Business Development all'indirizzo `<aws-entity-resolution-bd@amazon .com>`.

Utilizzo della API specifica AWS Entity Resolution Open

La API specifica Open definisce tutti i protocolli associati a AWS Entity Resolution. Questa specifica è necessaria per implementare l'integrazione.

La API definizione aperta contiene le seguenti API operazioni:

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

Per richiedere la API specifica Open, contattate il team di sviluppo AWS Entity Resolution aziendale all'indirizzo `<aws-entity-resolution-bd@amazon .com>`.

La API specifica Open supporta due tipi di integrazioni per la codifica e la transcodifica degli identificativi di consumo, l'elaborazione in batch e l'elaborazione sincrona. Dopo aver ottenuto la API specifica Open, implementate il tipo di integrazione di elaborazione adatto al vostro caso d'uso.

Argomenti

Integrazione dell'elaborazione in batch

L'integrazione dell'elaborazione in batch segue uno schema di progettazione asincrono. Dopo l'avvio AWS Data Exchange, un flusso di lavoro invia un lavoro tramite un endpoint di integrazione del provider e quindi attende il completamento del processo controllando periodicamente lo stato del lavoro. Questa soluzione è più indicata per le esecuzioni dei lavori che possono richiedere più tempo e hanno un throughput inferiore da parte del provider. Il provider utilizzerà la posizione del set di dati come collegamento Amazon S3, che potrà elaborare da parte sua e scrivere i risultati in una posizione S3 di output predeterminata.

L'integrazione dell'elaborazione in batch è abilitata utilizzando tre definizioni. API AWS Entity Resolution chiamerà l'endpoint del provider che è disponibile AWS Data Exchange nel seguente ordine:

1. `POST CreateJob`: Questa API operazione invia le informazioni sulla mansione al provider per l'elaborazione. Queste informazioni riguardano il tipo di lavoro, la codifica o la transcodifica, le posizioni S3, lo schema fornito dal cliente ed eventuali proprietà del lavoro aggiuntive richieste.

Questo API restituisce un`JobId`, e lo Status del Job sarà uno dei seguenti: `PENDINGREADY`,`IN_PROGRESS`,`COMPLETE`, o`FAILED`.

Esempio di richiesta di codifica

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

Risposta di esempio

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

2. `POST StartJob`: Ciò API consente al provider di sapere come avviare il lavoro in base a quanto `JobId` fornito. Ciò consente al provider di eseguire tutte le convalide necessarie dal `CreateJob` `StartJob`

   Ciò API restituisce a`JobId`, the `Status` for the Job`statusMessage`, e`statusCode`.

Esempio di richiesta di codifica

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

Risposta di esempio

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

3. `GET GetJob`: API Indica AWS Entity Resolution se il lavoro è stato completato o se è in corso un altro stato.

   Ciò API restituisce a`JobId`, the `Status` for the Job`statusMessage`, `estatusCode`.

   Esempio di richiesta di codifica

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

   Risposta di esempio

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

La definizione completa di questi APIs elementi è fornita nella API specifica AWS Entity Resolution Open.

Integrazione dell'elaborazione sincrona

La soluzione di elaborazione sincrona è più desiderabile per i provider che hanno un tempo di risposta quasi in tempo reale con tempi di risposta in tempo reale con un throughput più elevato e superiore. TPS Questo AWS Entity Resolution flusso di lavoro partiziona il set di dati ed effettua più API richieste in parallelo. Il AWS Entity Resolution flusso di lavoro gestisce quindi la scrittura dei risultati nella posizione di output desiderata.

Questo processo è abilitato utilizzando una delle API definizioni. AWS Entity Resolution chiama l'endpoint del provider che è disponibile tramite AWS Data Exchange:

`POST AssignIdentities`: Questo API invia i dati al provider utilizzando un `source_id` identificatore e `recordFields` associato a quel record.

Questo API restituisce il. `assignedRecords`

Esempio di richiesta di codifica

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

Risposta di esempio

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

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

La definizione completa di questi APIs elementi è fornita nella API specifica AWS Entity Resolution Open.

A seconda dell'approccio scelto dal provider, il provider AWS Entity Resolution creerà una configurazione specifica che verrà utilizzata per avviare la codifica o la transcodifica. Inoltre, queste configurazioni sono disponibili per i clienti che utilizzano il servizio fornito da. APIs AWS Entity Resolution

Questa configurazione è accessibile utilizzando un Amazon Resource Name (ARN), che deriva dal luogo in cui AWS Data Exchange è ospitata l'offerta del servizio del provider e dal tipo di servizio del provider. AWS Entity Resolution si riferisce a questo ARN come`providerServiceARN`.

Test dell'integrazione di un provider

Sebbene AWS Entity Resolution offra servizi di abbinamento dei dati, l'integrazione di un provider è un componente di terze parti fondamentale per il flusso di lavoro di end-to-end abbinamento. Sono stati definiti diversi test per i provider che aggiungono una protezione in caso di errore dell'integrazione. AWS Entity Resolution Questo approccio offre ai provider l'opportunità di monitorare lo stato dei propri servizi in base a questi casi end-to-end di test.

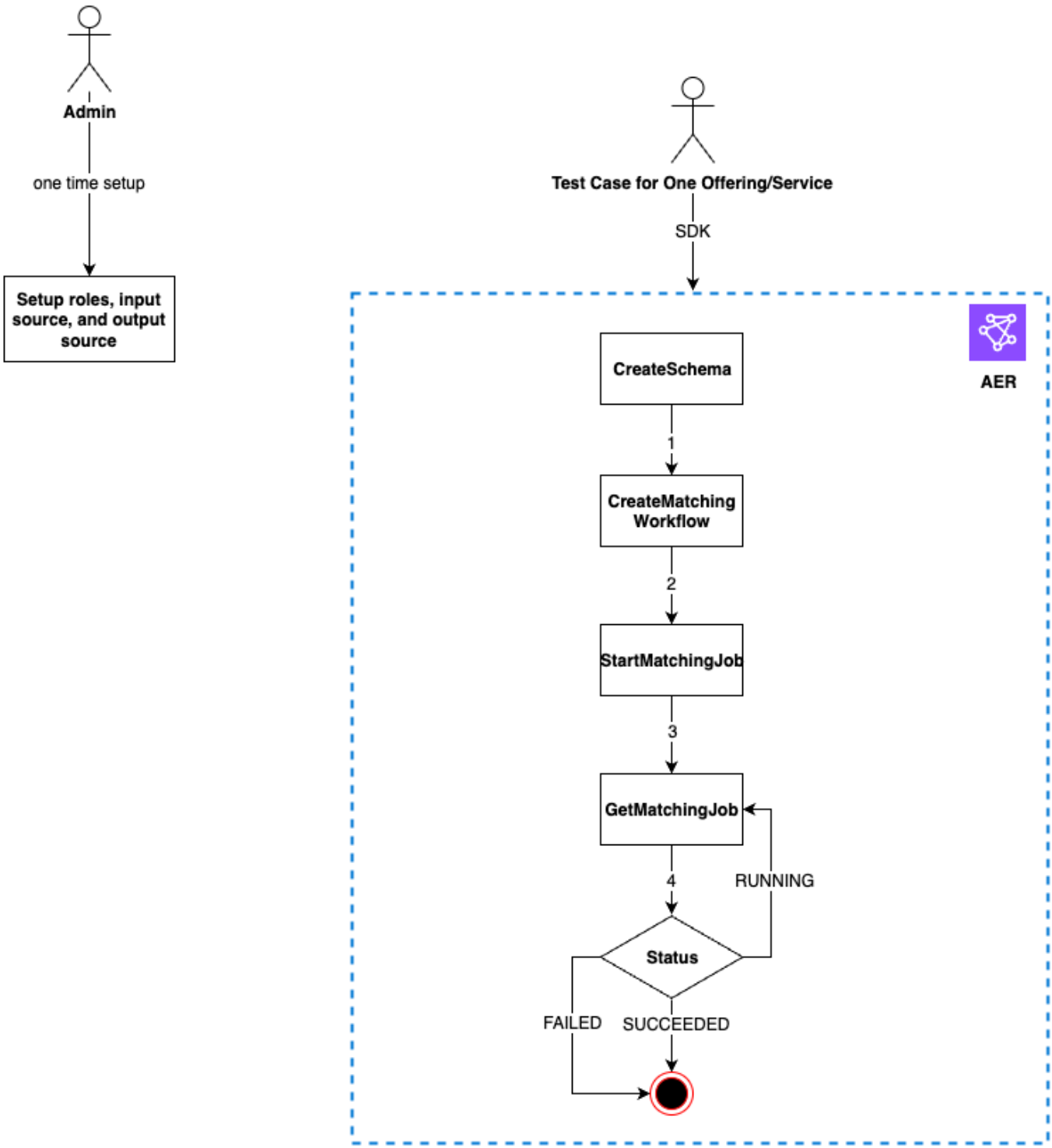
I provider possono utilizzare i propri account di test e i propri dati per eseguire questi casi di end-to-end test utilizzando il AWS Entity Resolution Software Development Kit (SDK). In caso di problemi con i provider, AWS Entity Resolution utilizza il percorso di escalation preferito per segnalare il problema. Inoltre, i fornitori devono implementare il proprio monitoraggio sui risultati dei test. I provider devono condividere con loro Account AWS IDs i dati utilizzati per eseguire questi test AWS Entity Resolution.

Un'esecuzione riuscita significa che un provider può configurare i propri dati, utilizzare il proprio servizio e lo stato del lavoro viene restituito Completato senza errori. AWS Entity Resolution Questa operazione può essere eseguita a livello di codice utilizzando il APIs comando fornito da. AWS Entity Resolution

Ad esempio, i provider possono configurare il bucket S3, la fonte di input, i ruoli, lo schema e i flussi di lavoro in base ai propri servizi. Una volta completate queste configurazioni, i provider possono eseguire questi flussi di lavoro una volta al giorno con 200 record per testare il proprio servizio. In questo approccio, i provider utilizzano la propria scelta SDK ed eseguono un end-to-end test dei servizi offerti tramite l' AWS Data Exchange utilizzo dei propri account di prova. I fornitori sono tenuti a eseguire questi test per ciascuna delle loro offerte o servizi.

> **Note**
>
> I provider devono fornire AWS Entity Resolution l' Account AWS ID (`accountId`)che utilizzano) per eseguire questi flussi di lavoro a scopo di test. Inoltre, i provider devono monitorare questi test e assicurarsi che vengano superati, il che significa che devono abilitare la notifica in caso di errori e risolvere il problema di conseguenza.

Il diagramma seguente mostra un tipico caso di test end-to-end del flusso di lavoro.



Per testare l'integrazione di un provider

1. (Configurazione una tantum) Configura le risorse per AWS Entity Resolution seguendo le procedure riportate in[Configurare AWS Entity Resolution](#).

Dopo aver completato le procedure di configurazione una tantum, dovresti avere i ruoli, i dati e la fonte di dati pronti. Ora sei pronto per testare l'integrazione del provider utilizzando la AWS Entity Resolution console oAPIs.

2. Verifica l'integrazione del provider utilizzando la console AWS Entity Resolution APIs o.

API

Per testare l'integrazione di un provider utilizzando il AWS Entity Resolution APIs

1. Creare una mappatura dello schema utilizzando. CreateSchemaMapping API Per un elenco completo dei linguaggi di programmazione supportati, vedere la sezione Vedere anche di CreateSchemaMapping API.

   La mappatura dello schema è il processo mediante il quale si spiega AWS Entity Resolution come interpretare i dati per la corrispondenza. Si definisce lo schema della tabella dei dati di input che si desidera che AWS Entity Resolution legga in un flusso di lavoro corrispondente.

   Quando si crea una mappatura dello schema, è necessario designare e assegnare un identificatore univoco a ciascuna riga di dati di input letta da AWS Entity Resolution. Ad esempio, `Primary_key`, `Row_ID`, `Record_ID`.

   Example Esempio

   Di seguito è riportato un esempio di mappatura dello schema per un'origine dati che contiene e: `id` `email`

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

Example Esempio

Di seguito è riportato un esempio di mappatura dello schema per un'origine dati che contiene `id` e `email` utilizza Java: SDK

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

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

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

)
```

2. Crea un flusso di lavoro corrispondente utilizzando. CreateMatchingWorkflow API Per un elenco completo dei linguaggi di programmazione supportati, vedere la sezione Vedere anche di CreateMatchingWorkflow API.

   Example Esempio

   Di seguito è riportato un esempio di flusso di lavoro corrispondente che utilizza JavaSDK:

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

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

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

 .resolutionTechniques(ResolutionTechniques.builder()

   .resolutionType(PROVIDER)
```

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

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

)
```

Dopo aver impostato il flusso di lavoro corrispondente, è possibile eseguire un flusso di lavoro.

3. Esegui un flusso di lavoro corrispondente utilizzando StartMatchingJob API. Per eseguire un flusso di lavoro corrispondente, è necessario aver creato un flusso di lavoro corrispondente utilizzando l'`CreateMatchingWorkflow`endpoint.

   Per un elenco completo dei linguaggi di programmazione supportati, vedere la sezione Vedere anche di StartMatchingJob API.

   Example Esempio

   Di seguito è riportato un esempio di flusso di lavoro corrispondente in esecuzione utilizzando JavaSDK:

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

4. Monitora lo stato di un flusso di lavoro utilizzando GetMatchingJob API.

   Ciò API restituisce lo stato, le metriche e gli errori (se presenti) associati a un lavoro.

Example Esempio

Di seguito è riportato un esempio di monitoraggio di un processo di workflow corrispondente utilizzando JavaSDK:

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

Il end-to-end test è completo se il flusso di lavoro è stato completato correttamente.

Console

Per testare l'integrazione di un provider utilizzando la AWS Entity Resolution console

1. Crea una mappatura dello schema seguendo i passaggi riportati di seguito. Creazione di una mappatura dello schema

   La mappatura dello schema è il processo mediante il quale spieghi AWS Entity Resolution come interpretare i dati per la corrispondenza. Definisci lo schema della tabella dei dati di input che desideri AWS Entity Resolution leggere in un flusso di lavoro corrispondente.

   Quando si crea una mappatura dello schema, è necessario designare e assegnare un identificatore univoco a ciascuna riga di dati di input che AWS Entity Resolution viene letta. Ad esempio, `Primary_key`, `Row_ID`, `Record_ID`.

   Example Esempio

   Di seguito è riportato un esempio di mappatura dello schema per un'origine dati che contiene e: `id` `email`

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

```
    "type": "EMAIL_ADDRESS"
  }
]
```

2. Crea ed esegui il flusso di lavoro corrispondente seguendo i passaggi indicati in[Creazione di un flusso di lavoro di abbinamento basato sui servizi del provider](#).

   La creazione di un flusso di lavoro corrispondente è il processo impostato per specificare i dati di input da abbinare e il modo in cui deve essere eseguita la corrispondenza. Nel flusso di lavoro basato sul provider, se un account ha un abbonamento a un provider di servizi tramite AWS Data Exchange, puoi abbinare gli identificatori noti al tuo provider preferito. A seconda del provider e del servizio che utilizzi per eseguire un test end-to-end, puoi configurare di conseguenza il flusso di lavoro corrispondente.

   La AWS Entity Resolution console combina le azioni di creazione ed esecuzione in un unico pulsante. Dopo aver selezionato Crea ed esegui, viene visualizzato un messaggio che indica che il flusso di lavoro corrispondente è stato creato e che il processo è iniziato.
3. Monitora lo stato del flusso di lavoro nella pagina Corrispondenza dei flussi di lavoro.

   Il end-to-end test è completo se il flusso di lavoro è stato completato correttamente (lo stato del Job è Completato).

   Nella scheda Metriche della pagina di dettaglio del flusso di lavoro corrispondente, puoi visualizzare quanto segue in Metriche dell'ultimo lavoro:

   - Il Job ID.
   - Lo stato del processo del flusso di lavoro corrispondente: In coda, In corso, Completato, Non riuscito
   - Il tempo di completamento del processo del flusso di lavoro.
   - Il numero di record elaborati.
   - Il numero di record non elaborati.
   - La corrispondenza unica IDs generata.
   - Il numero di record di input.

   Puoi anche visualizzare le metriche dei job per i job corrispondenti ai job del flusso di lavoro che sono stati eseguiti in precedenza nella cronologia Job.

Sicurezza in AWS Entity Resolution

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWS e l'utente. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue AWS servizi nel Cloud AWS. AWS fornisce, inoltre, servizi utilizzabili in modo sicuro. I revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per informazioni sui programmi di conformità applicabili a AWS Entity Resolution, consulta Servizi AWS coperti dal programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che viene utilizzato. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda, le leggi e le normative applicabili.

Questa documentazione facilitaconsenteladicomprensionecomprenderedell'applicazionecomedelapplicare il modello di responsabilità condivisa quando utilizzisi usaAWS Entity Resolution. I seguenti argomenti illustrano come configurare AWS Entity Resolution per soddisfare gli obiettivi di sicurezza e conformità. Scoprirai anche come utilizzare altri AWS servizi per monitorare e proteggere le risorse AWS Entity Resolution.

Argomenti

- Protezione dei dati in AWS Entity Resolution
- Gestione delle identità e degli accessi per AWS Entity Resolution
- Convalida della conformità per AWS Entity Resolution
- Resilienza in AWS Entity Resolution

Protezione dei dati in AWS Entity Resolution

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS Entity Resolution. Come descritto in questo modello, AWS è responsabile della protezione

dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i AWS servizi utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta il Modello di responsabilitàAWS condivisa e GDPR il post sul blog sulla AWS sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o unAPI, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard () 140-3. FIPS

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori AWS Entity Resolution o AWS servizi utilizzi in altro modo la console, API AWS CLI, o. AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Se fornisci un messaggio URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

Crittografia dei dati a riposo per AWS Entity Resolution

AWS Entity Resolution fornisce la crittografia di default per proteggere i dati sensibili dei clienti archiviati utilizzando chiavi AWS di crittografia proprietarie.

AWSchiavi di proprietà: AWS Entity Resolution utilizza queste chiavi per impostazione predefinita per crittografare automaticamente i dati di identificazione personale. Non è possibile visualizzare, gestire o utilizzare chiavi AWS di proprietà o controllarne l'utilizzo. Tuttavia, non è necessario intraprendere alcuna azione per proteggere le chiavi che crittografano i dati. Per ulteriori informazioni, consulta le chiavi AWS possedute nella Guida per gli AWS Key Management Service sviluppatori.

La crittografia predefinita dei dati a riposo aiuta a ridurre il sovraccarico operativo e la complessità associati alla protezione dei dati sensibili. Allo stesso tempo, puoi utilizzarlo per creare applicazioni sicure che soddisfino i rigorosi requisiti normativi e di conformità alla crittografia.

In alternativa, puoi anche fornire una KMS chiave di crittografia gestita dal cliente quando crei la risorsa di flusso di lavoro corrispondente.

Chiavi gestite dal cliente: AWS Entity Resolution supporta l'uso di una KMS chiave simmetrica gestita dal cliente che potete creare, possedere e gestire per consentire la crittografia dei dati sensibili. Avendo il pieno controllo di questo livello di crittografia, è possibile eseguire operazioni quali:

- Stabilire e mantenere le policy delle chiavi
- Stabilire e mantenere IAM politiche e sovvenzioni
- Abilitare e disabilitare le policy delle chiavi
- Ruotare i materiali crittografici delle chiavi
- Aggiungere tag
- Creare alias delle chiavi
- Pianificare l’eliminazione delle chiavi

Per ulteriori informazioni, consulta Customer Managed Key nella Guida per gli AWS Key Management Service sviluppatori.

Per ulteriori informazioni su AWS KMS, consulta Cos'è il servizio di gestione delle AWS chiavi?

Gestione delle chiavi

Come AWS Entity Resolution utilizza le sovvenzioni in AWS KMS

AWS Entity Resolution richiede una concessione per utilizzare la chiave gestita dal cliente. Quando crei un flusso di lavoro corrispondente crittografato con una chiave gestita dal cliente, AWS Entity Resolution crea una concessione per tuo conto inviando una CreateGrantrichiesta a AWS KMS. Le sovvenzioni AWS KMS vengono utilizzate per AWS Entity Resolution consentire l'accesso a una

KMS chiave in un account cliente. AWS Entity Resolution richiede la concessione dell'utilizzo della chiave gestita dal cliente per le seguenti operazioni interne:

- Invia GenerateDataKeyrichieste per AWS KMS generare chiavi dati crittografate dalla tua chiave gestita dal cliente.
- Invia le richieste Decrypt a per AWS KMS decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per crittografare i dati.

Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. In tal caso, AWS Entity Resolution non sarà in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, il che influirà sulle operazioni che dipendono da tali dati. Ad esempio, se rimuovi l'accesso al servizio alla tua chiave tramite la concessione e tenti di avviare un processo per un flusso di lavoro corrispondente crittografato con una chiave cliente, l'operazione restituirà un `AccessDeniedException` errore.

Creazione di una chiave gestita dal cliente

È possibile creare una chiave simmetrica gestita dal cliente utilizzando AWS Management Console, o il. AWS KMS APIs

Per creare una chiave simmetrica gestita dal cliente

AWS Entity Resolution supporta la crittografia utilizzando chiavi di crittografia simmetriche. KMS Segui la procedura riportata in Creazione di una chiave simmetrica gestita dal cliente nella Guida per gli sviluppatori di AWS Key Management Service .

Dichiarazione politica chiave

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy della chiave. Per ulteriori informazioni, consulta Gestire l'accesso alle chiavi gestite dal cliente nella Guida per gli AWS Key Management Service sviluppatori.

Per utilizzare la chiave gestita dal cliente con AWS Entity Resolution le tue risorse, nella politica chiave devono essere consentite le seguenti API operazioni:

- `kms:DescribeKey`— Fornisce informazioni quali la chiaveARN, la data di creazione (e la data di eliminazione, se applicabile), lo stato della chiave e la data di origine e scadenza (se presente) del materiale chiave. Include campi che`KeySpec`, ad esempio, aiutano a distinguere diversi tipi di KMS

chiavi. Visualizza anche l'utilizzo della chiave (crittografia, firma o generazione e verificaMACs) e gli algoritmi supportati dalla KMS chiave. AWS Entity Resolution conferma che lo è e lo `KeySpec` è`SYMMETRIC_DEFAULT`. `KeyUsage` `ENCRYPT_DECRYPT`

- `kms:CreateGrant`: aggiunge una concessione a una chiave gestita dal cliente. Concede il controllo dell'accesso a una KMS chiave specificata, che consente l'accesso alle operazioni AWS Entity Resolution di concessione richieste. Per ulteriori informazioni sull'utilizzo di Grants, consulta la Guida per gli AWS Key Management Service sviluppatori.

Ciò consente di AWS Entity Resolution effettuare le seguenti operazioni:

- Chiama `GenerateDataKey` per generare una chiave dati crittografata e archiviarla, poiché la chiave dati non viene utilizzata immediatamente per crittografare.
- Chiama `Decrypt` per utilizzare la chiave dati crittografata memorizzata per accedere ai dati crittografati.
- Imposta un preside in pensione per consentire al servizio di farlo`RetireGrant`.

Di seguito sono riportati alcuni esempi di dichiarazioni politiche che è possibile aggiungere per 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"
        }
      }
}
```

Autorizzazioni per gli utenti

Quando si configura una KMS chiave come chiave predefinita per la crittografia, la politica di KMS chiave predefinita consente a qualsiasi utente con accesso alle KMS azioni richieste di utilizzare

questa KMS chiave per crittografare o decrittografare le risorse. È necessario concedere agli utenti l'autorizzazione a eseguire le seguenti azioni per utilizzare la crittografia a chiave gestita KMS dal cliente:

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

Durante una `CreateMatchingWorkflow`richiesta, AWS Entity Resolution invierà una CreateGrantrichiesta DescribeKeye una a per tuo AWS KMS conto. Ciò richiederà che l'IAMentità che effettua la `CreateMatchingWorkflow` richiesta con una KMS chiave gestita dal cliente disponga delle `kms:DescribeKey` autorizzazioni relative alla politica delle KMS chiavi.

Durante una `StartIdMappingJob`richiesta `CreateIdMappingWorkflow`e, AWS Entity Resolution invierà una CreateGrantrichiesta DescribeKeye una a per tuo AWS KMS conto. Ciò richiederà che l'IAMentità che effettua la `StartIdMappingJob` richiesta `CreateIdMappingWorkflow` e con una KMS chiave gestita dal cliente disponga delle `kms:DescribeKey` autorizzazioni relative alla politica delle KMS chiavi. I provider saranno in grado di accedere alla chiave gestita dal cliente per decrittografare i dati nel bucket Amazon AWS Entity Resolution S3.

Di seguito sono riportati alcuni esempi di policy che è possibile aggiungere ai provider per decrittografare i dati nel bucket Amazon AWS Entity Resolution S3:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::715724997226:root"
        },
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "<KMSKeyARN>",
        "Condition": {
            "StringEquals": {
                "kms:ViaService": "s3.amazonaws.com"
            }
```

```
        }
    }]
}
```

Sostituisci ciascuno *<user input placeholder>* con le tue informazioni.

<KMSKeyARN>	AWS KMS Nome della risorsa Amazon.

Analogamente, l'IAMentità che richiama il `StartMatchingJobAPI`must have `kms:Decrypt` e `kms:GenerateDataKey` le autorizzazioni sulla KMS chiave gestita dal cliente fornite nel flusso di lavoro corrispondente.

Per ulteriori informazioni sulla specificazione delle autorizzazioni in una politica, consulta la Guida per gli sviluppatori.AWS Key Management Service

Per ulteriori informazioni sulla risoluzione dei problemi di accesso tramite chiave, consulta la Guida per gli AWS Key Management Service sviluppatori.

Specificazione di una chiave gestita dal cliente per AWS Entity Resolution

È possibile specificare una chiave gestita dal cliente come crittografia di secondo livello per le seguenti risorse:

Flusso di lavoro corrispondente: quando si crea una risorsa di flusso di lavoro corrispondente, è possibile specificare la chiave dati inserendo un KMSArn, che viene AWS Entity Resolution utilizzato per crittografare i dati personali identificabili archiviati dalla risorsa.

KMSArn— Immettere una chiaveARN, che è un identificatore chiave per una chiave gestita AWS KMS dal cliente.

È possibile specificare una chiave gestita dal cliente come crittografia di secondo livello per le seguenti risorse se si sta creando o eseguendo un flusso di lavoro di mappatura degli ID su due: Account AWS

Flusso di lavoro di mappatura degli ID o flusso di lavoro di mappatura degli ID: quando si crea una risorsa del flusso di lavoro di mappatura degli ID o si avvia un processo di flusso di lavoro di mappatura degli ID, è possibile specificare la chiave dati inserendo un KMSArn, che viene AWS Entity Resolution utilizzato per crittografare i dati personali identificabili archiviati dalla risorsa.

KMSArn— Immettere una chiaveARN, che è un identificatore chiave per una chiave gestita dal cliente. AWS KMS

Monitoraggio delle chiavi di crittografia per Service AWS Entity Resolution

Quando utilizzi una chiave gestita AWS KMS dal cliente con le tue risorse di AWS Entity Resolution servizio, puoi utilizzare AWS CloudTrailAmazon CloudWatch Logs per tenere traccia delle richieste AWS Entity Resolution inviate a AWS KMS.

Gli esempi seguenti sono AWS CloudTrail eventi per`CreateGrant`, `GenerateDataKeyDecrypt`, e per `DescribeKey` monitorare AWS KMS le operazioni richieste per accedere AWS Entity Resolution ai dati crittografati dalla chiave gestita dal cliente:

Argomenti

- CreateGrant
- DescribeKey
- GenerateDataKey
- Decrypt

CreateGrant

Quando utilizzi una chiave gestita AWS KMS dal cliente per crittografare la risorsa del flusso di lavoro corrispondente, AWS Entity Resolution invia una `CreateGrant` richiesta per tuo conto per accedere alla KMS chiave contenuta nel tuo Account AWS. La concessione che AWS Entity Resolution viene creata è specifica per la risorsa associata alla chiave gestita dal AWS KMS cliente. Inoltre, AWS Entity Resolution utilizza l'`RetireGrant`operazione per rimuovere una concessione quando si elimina una risorsa.

L'evento di esempio seguente registra l'operazione `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 utilizza l'`DescribeKey`operazione per verificare se la chiave gestita AWS KMS dal cliente associata alla risorsa corrispondente esiste nell'account e nella regione.

L'evento di esempio seguente registra l'`DescribeKey`operazione.

```
{
    "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 abiliti una chiave gestita AWS KMS dal cliente per la risorsa del flusso di lavoro corrispondente, AWS Entity Resolution invia una `GenerateDataKey` richiesta tramite Amazon Simple Storage Service (Amazon S3) AWS KMS a cui specifica AWS KMS la chiave gestita dal cliente per la risorsa.

L'evento di esempio seguente registra l'`GenerateDataKey`operazione.

```
{
    "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 abiliti una chiave gestita AWS KMS dal cliente per la risorsa del flusso di lavoro corrispondente, AWS Entity Resolution invia una `Decrypt` richiesta tramite Amazon Simple Storage Service (Amazon S3) AWS KMS a cui specifica AWS KMS la chiave gestita dal cliente per la risorsa.

L'evento di esempio seguente registra l'`Decrypt`operazione.

```
{
    "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"
}
```

Considerazioni

AWS Entity Resolution non supporta l'aggiornamento di un flusso di lavoro corrispondente con una nuova KMS chiave gestita dal cliente. In questi casi, puoi creare un nuovo flusso di lavoro con la KMS chiave gestita dal cliente.

Ulteriori informazioni

Le seguenti risorse forniscono ulteriori informazioni sulla crittografia dei dati a riposo.

Per ulteriori informazioni sui concetti di base del servizio di gestione delle AWS chiavi, consulta la Guida per gli AWS Key Management Service sviluppatori.

Per ulteriori informazioni sulle best practice di sicurezza per il servizio di gestione delle AWS chiavi, consulta la Guida per gli AWS Key Management Service sviluppatori.

Accesso AWS Entity Resolution tramite un endpoint di interfaccia ()AWS PrivateLink

Puoi usarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e. AWS Entity Resolution Puoi accedere AWS Entity Resolution come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze del tuo VPC non necessitano di indirizzi IP pubblici per accedervi. AWS Entity Resolution

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Queste sono interfacce di rete gestite dal richiedente che fungono da punto di ingresso per il traffico destinato a AWS Entity Resolution.

Per ulteriori informazioni, consulta Access AWS servizi through AWS PrivateLink nella AWS PrivateLink Guida.

Considerazioni per AWS Entity Resolution

Prima di configurare un endpoint di interfaccia per AWS Entity Resolution, consulta le considerazioni nella Guida.AWS PrivateLink

AWS Entity Resolution supporta l'effettuazione di chiamate a tutte le sue azioni API tramite l'endpoint dell'interfaccia.

Le policy degli endpoint VPC non sono supportate per. AWS Entity Resolution Per impostazione predefinita, l'accesso completo a AWS Entity Resolution è consentito tramite l'endpoint dell'interfaccia. In alternativa, è possibile associare un gruppo di sicurezza alle interfacce di rete dell'endpoint per controllare il traffico che AWS Entity Resolution attraversa l'endpoint dell'interfaccia.

Crea un endpoint di interfaccia per AWS Entity Resolution

Puoi creare un endpoint di interfaccia per AWS Entity Resolution utilizzare la console Amazon VPC o AWS Command Line Interface ().AWS CLI Per ulteriori informazioni, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di AWS PrivateLink .

Crea un endpoint di interfaccia per AWS Entity Resolution utilizzare il seguente nome di servizio:

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

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API AWS Entity Resolution utilizzando il nome DNS regionale predefinito. Ad esempio, `entityresolution.us-east-1.amazonaws.com`.

Creazione di una policy dell' endpoint per l'endpoint dell'interfaccia

Una policy dell'endpoint è una risorsa IAM che è possibile allegare all'endpoint dell'interfaccia. La policy predefinita per gli endpoint consente l'accesso completo AWS Entity Resolution tramite l'endpoint dell'interfaccia. Per controllare l'accesso consentito AWS Entity Resolution dal tuo VPC, collega una policy endpoint personalizzata all'endpoint di interfaccia.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali che possono eseguire azioni (Account AWS, utenti IAM e ruoli IAM).
- Le azioni che possono essere eseguite.
- Le risorse in cui è possibile eseguire le operazioni.

Per ulteriori informazioni, consulta la sezione Controllo dell'accesso ai servizi con policy di endpoint nella Guida di AWS PrivateLink .

Esempio: policy degli endpoint VPC per le azioni AWS Entity Resolution

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando alleghi questa policy all'endpoint dell'interfaccia, concede l'accesso alle AWS Entity Resolution azioni elencate per tutti i principali su tutte le risorse.

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

Gestione delle identità e degli accessi per AWS Entity Resolution

AWS Identity and Access Management (IAM) è un dispositivo AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Entity Resolution IAMè un dispositivo AWS servizio che puoi utilizzare senza costi aggiuntivi.

> **Note**
>
> AWS Entity Resolution supporta le politiche relative a più account. Per ulteriori informazioni, consulta la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi. AWS Entity Resolution

Utente del servizio: se utilizzi il AWS Entity Resolution servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS Entity Resolution funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS Entity Resolution, consulta Risoluzione dei problemi AWS Entity Resolution di identità e accesso.

Amministratore del servizio: se sei responsabile delle AWS Entity Resolution risorse della tua azienda, probabilmente hai pieno accesso a AWS Entity Resolution. È tuo compito determinare a quali AWS Entity Resolution funzionalità e risorse devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con AWS Entity Resolution, consultaCome AWS Entity Resolution funziona con IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche a cui gestire l'accesso AWS Entity Resolution. Per visualizzare esempi di policy AWS Entity Resolution basate sull'identità che puoi utilizzare inIAM, consulta. Esempi di policy basate su identità per AWS Entity Resolution

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Firmare AWS API le richieste nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione

a più fattori nella Guida per l'AWS IAM Identity Center utente e Utilizzo dell'autenticazione a più fattori (MFA) AWS nella Guida per l'IAMutente.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte AWS servizi le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere AWS servizi utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le AWS servizi credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

IAMruoli

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console cambiando ruolo. È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

IAMi ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per

conoscere la differenza tra i ruoli e le politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Cross Account Resource Access IAM nella Guida per l'utente. IAM

- Accesso tra servizi: alcuni AWS servizi utilizzano funzionalità in altri. AWS servizi Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta di effettuare richieste AWS servizio ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o richiedono AWS API. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite contenute IAM in una policy basata sulle risorse.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM
- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations

AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

Come AWS Entity Resolution funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Entity Resolution, scopri con quali IAM funzionalità è disponibile l'uso AWS Entity Resolution.

IAMfunzionalità che puoi usare con AWS Entity Resolution

IAMcaratteristica	AWS Entity Resolution supporto
Policy basate su identità	Sì
Policy basate su risorse	Sì
Azioni di policy	Sì
Risorse relative alle policy	Sì

IAMcaratteristica	AWS Entity Resolution supporto
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC(tag nelle politiche)	Parziale
Credenziali temporanee	Sì
Sessioni di accesso diretto (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	No

Per avere una panoramica generale del funzionamento AWS Entity Resolution e degli altri AWS servizi con la maggior parte delle IAM funzionalità, consulta AWS i servizi che funzionano con la maggior parte delle funzionalità IAM nella Guida per l'IAMutente.

Politiche basate sull'identità per AWS Entity Resolution

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

Esempi di policy basate sull'identità per AWS Entity Resolution

Per visualizzare esempi di politiche basate sull' AWS Entity Resolution identità, vedere. Esempi di policy basate su identità per AWS Entity Resolution

Politiche basate sulle risorse all'interno AWS Entity Resolution

Supporta politiche basate sulle risorse: Sì

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Azioni politiche per AWS Entity Resolution

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AWS Entity Resolution azioni, vedere Azioni definite da AWS Entity Resolution nel Service Authorization Reference.

Le azioni politiche in AWS Entity Resolution uso utilizzano il seguente prefisso prima dell'azione:

```
entityresolution
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

Per visualizzare esempi di politiche AWS Entity Resolution basate sull'identità, vedere. Esempi di policy basate su identità per AWS Entity Resolution

Risorse politiche per AWS Entity Resolution

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di AWS Entity Resolution risorse e relativiARNs, consulta Resources Defined by AWS Entity Resolution nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare le caratteristiche ARN di ciascuna risorsa, consulta Azioni definite da AWS Entity Resolution.

Per visualizzare esempi di politiche AWS Entity Resolution basate sull'identità, vedere. Esempi di policy basate su identità per AWS Entity Resolution

Chiavi relative alle condizioni delle politiche per AWS Entity Resolution

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica`OR`. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

Per visualizzare un elenco di chiavi di AWS Entity Resolution condizione, consulta Condition Keys for AWS Entity Resolution nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS Entity Resolution.

Per visualizzare esempi di politiche AWS Entity Resolution basate sull'identità, vedere. Esempi di policy basate su identità per AWS Entity Resolution

ACLsin AWS Entity Resolution

SupportiACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

ABACcon AWS Entity Resolution

Supporti ABAC (tag nelle politiche): Parziale

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni suABAC, vedere Cos'è? ABAC nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Utilizzo di credenziali temporanee con AWS Entity Resolution

Supporta le credenziali temporanee: sì

Alcuni AWS servizi non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che AWS servizi funzionano con credenziali temporanee, consulta la sezione AWS servizi relativa alla funzionalità IAM nella Guida per l'IAMutente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla

console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Sessioni di accesso diretto per AWS Entity Resolution

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta AWS servizio per effettuare richieste ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio per AWS Entity Resolution

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. AWS Entity Resolution Modifica i ruoli di servizio solo quando viene AWS Entity Resolution fornita una guida in tal senso.

Ruoli collegati ai servizi per AWS Entity Resolution

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con. IAM Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate su identità per AWS Entity Resolution

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS Entity Resolution . Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o. AWS API Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta Creazione di IAM politiche nella Guida per l'IAMutente.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS Entity Resolution, incluso il formato di ARNs per ogni tipo di risorsa, vedere Actions, Resources and Condition Keys AWS Entity Resolution nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console di AWS Entity Resolution
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS Entity Resolution risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative nella Guida per l'IAMutente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico AWS servizio, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.

Utilizzo della console di AWS Entity Resolution

Per accedere alla AWS Entity Resolution console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle

AWS Entity Resolution risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso il AWS CLI o il. AWS API Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la AWS Entity Resolution console, allega anche la policy AWS Entity Resolution *`ConsoleAccess`* o la policy *`ReadOnly`* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiungere autorizzazioni a un utente nella Guida per l'IAMutente.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI AWS API

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

```
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiche gestite per AWS Entity Resolution

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne AWS servizio viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AWSEntityResolutionConsoleFullAccess

È possibile allegare la policy `AWSEntityResolutionConsoleFullAccess`alle identità IAM.

Questa politica garantisce l'accesso completo agli AWS Entity Resolution endpoint e alle risorse.

Questa policy consente inoltre un certo accesso in lettura ad applicazioni correlate AWS servizi come S3 e Tagging e AWS KMS consente alla console di visualizzare le scelte e utilizzare quelle

selezionate per eseguire azioni di risoluzione delle entità. AWS Glue Alcune risorse sono limitate per contenere il nome del servizio. `entityresolution`

Poiché AWS Entity Resolution si basa su un ruolo passato per eseguire azioni sulle AWS risorse correlate, questa politica concede anche le autorizzazioni per selezionare e assegnare il ruolo desiderato.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `EntityResolutionAccess`— Consente ai responsabili l'accesso completo agli endpoint e alle risorse AWS Entity Resolution .
- `GlueSourcesConsoleDisplay`— Concede l'accesso alle AWS Glue tabelle degli elenchi come opzioni di origine dati e importa lo schema della tabella di una fonte di dati per l'esperienza utente.
- `S3BucketsConsoleDisplay`— Concede l'accesso per elencare tutti i bucket S3 come opzioni di origine dati.
- `S3SourcesConsoleDisplay`— Concede l'accesso alla visualizzazione dei bucket S3 come opzioni di origine dati.
- `TaggingConsoleDisplay`— Garantisce l'accesso alle chiavi e ai valori di read tagging.
- `KMSConsoleDisplay`— Concede l'accesso per descrivere le chiavi ed elencare gli alias per decrittografare e AWS Key Management Service crittografare le fonti di dati.
- `ListRolesToPickForPassing`— Concede l'accesso all'elenco di tutti i ruoli in modo che l'utente possa scegliere il ruolo da assegnare.
- `PassRoleToEntityResolutionService`— Concede l'accesso per trasferire un ruolo ristretto al servizio. AWS Entity Resolution
- `ManageEventBridgeRules`— Concede l'accesso per creare, aggiornare ed eliminare la EventBridge regola Amazon per ricevere notifiche S3.
- `ADXReadAccess`— Concede l'accesso per AWS Data Exchange verificare se il cliente ha un diritto o un abbonamento.

```
{
    "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 politica gestita: AWSEntityResolutionConsoleReadOnlyAccess

È possibile allegare `AWSEntityResolutionConsoleReadOnlyAccess` alle entità IAM.

Questa policy garantisce l'accesso in sola lettura agli AWS Entity Resolution endpoint e alle risorse.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `EntityResolutionRead`— Consente ai principali l'accesso in sola lettura agli endpoint e alle risorse. AWS Entity Resolution

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

```
        },
    ]
}
```

AWS Entity Resolution aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Entity Resolution da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS Entity Resolution documenti.

Modifica	Descrizione	Data
`AWSEntityResolutionConsoleFullAccess` : aggiornamento a policy esistente	È stata aggiunta `ADXReadAccess` e `ManageEventBridgeRules` abilitata l'opzione dei servizi del fornitore nel flusso di lavoro corrispondente.	16 ottobre 2023
AWS Entity Resolution ha iniziato a tenere traccia delle modifiche	AWS Entity Resolution ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	18 agosto 2023

Risoluzione dei problemi AWS Entity Resolution di identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con e. AWS Entity Resolution IAM

Argomenti

- Non sono autorizzato a eseguire alcuna azione in AWS Entity Resolution
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Entity Resolution risorse

Non sono autorizzato a eseguire alcuna azione in AWS Entity Resolution

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'errore di esempio seguente si verifica quando l'`mateojackson`IAMutente tenta di utilizzare la console per visualizzare i dettagli su una *`my-example-widget`* risorsa fittizia ma non dispone delle autorizzazioni fittizie`entityresolution:`*`GetWidget`*.

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

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *`my-example-widget`* utilizzando l'azione `entityresolution:`*`GetWidget`*.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS Entity Resolution.

Alcuni AWS servizi consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in. AWS Entity Resolution Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di assistenza, contatta AWS l'amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Entity Resolution risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Entity Resolution supporta queste funzionalità, consulta. Come AWS Entity Resolution funziona con IAM
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a persone Account AWS di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM IAM

Convalida della conformità per AWS Entity Resolution

Per sapere se un AWS servizio programma rientra nell'ambito di specifici programmi di conformità, consulta AWS servizi la sezione Scope by Compliance Program AWS servizi e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo AWS servizi è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

  > **Note**
  >
  > Non tutte sono idonee. AWS servizi HIPAA Per ulteriori informazioni, consulta la Guida ai servizi HIPAA idonei.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione AWS servizi e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization ()). ISO
- Evaluating Resources with Rules nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Ciò AWS servizio fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: AWS servizio rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, ad esempio PCI DSS soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò AWS servizio consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

AWS Entity Resolution migliori pratiche di conformità

Questa sezione fornisce le migliori pratiche e consigli per la conformità durante l'uso AWS Entity Resolution.

Standard di sicurezza dei dati del settore delle carte di pagamento (PCIDSS)

AWS Entity Resolution supporta l'elaborazione, l'archiviazione e la trasmissione dei dati delle carte di credito da parte di un commerciante o di un fornitore di servizi ed è stato convalidato come conforme al Payment Card Industry (PCI) Data Security Standard (). DSS Per ulteriori informazioni PCIDSS, incluso come richiedere una copia del AWS PCI Compliance Package, vedere PCIDSSLevel 1.

Controlli di sistema e organizzazione (SOC)

AWS Entity Resolution è conforme alle misure System and Organization Controls (SOC), incluse SOC 1, SOC 2 e SOC 3. SOCi report sono rapporti di esame indipendenti di terze parti che dimostrano come AWS raggiungere i controlli e gli obiettivi chiave di conformità. Questi audit assicurano che vengano attuate le adeguate procedure e tutele per proteggersi dai rischi che possono minare sicurezza, riservatezza e disponibilità dei dati di clienti e aziende. I risultati di questi audit di terze parti sono disponibili sul sito Web sulla AWS SOC conformità, dove è possibile visualizzare i report pubblicati per ottenere maggiori informazioni sui controlli a supporto AWS delle operazioni e della conformità.

Resilienza in AWS Entity Resolution

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Oltre all'infrastruttura AWS globale, AWS Entity Resolution offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati.

Monitoraggio AWS Entity Resolution

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Entity Resolution altre AWS soluzioni esistenti. AWS fornisce i seguenti strumenti di monitoraggio per osservare AWS Entity Resolution, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto tuo Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Argomenti

Registrazione delle chiamate AWS Entity Resolution API utilizzando AWS CloudTrail

AWS Entity Resolution è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS Entity Resolution. CloudTrail acquisisce tutte le chiamate API AWS Entity Resolution come eventi. Le chiamate acquisite includono chiamate dalla AWS Entity Resolution console e chiamate di codice alle operazioni AWS Entity Resolution API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Entity Resolution Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AWS Entity Resolution, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

AWS Entity Resolution informazioni in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in AWS Entity Resolution, tale attività viene registrata in un CloudTrail evento

insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo Account AWS, inclusi gli eventi di AWS Entity Resolution, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte AWS Entity Resolution le azioni vengono registrate CloudTrail e documentate nell'AWS Entity Resolution API Reference.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Comprendere le AWS Entity Resolution voci dei file di registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni

sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Crea risorse per la risoluzione delle AWS entità con AWS CloudFormation

AWSEntity Resolution è integrato con AWS CloudFormation un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (ad esempio AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e AWS::EntityResolution::PolicyStatement) e fornisce AWS CloudFormation e configura tali risorse per te.

Quando lo utilizzi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse di AWS Entity Resolution in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse più e più volte in più Account AWS regioni.

AWSRisoluzione e AWS CloudFormation modelli delle entità

Per fornire e configurare le risorse per AWS Entity Resolution e i servizi correlati, è necessario conoscere AWS CloudFormation i modelli. I modelli sono file di testo formattati in JSON oYAML. Questi modelli descrivono le risorse che desideri inserire nei tuoi AWS CloudFormation stack. Se non conosci JSON oYAML, puoi usare AWS CloudFormation Designer per iniziare a usare i AWS CloudFormation modelli. Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation .

AWSEntity Resolution supporta la creazione AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e l' AWS::EntityResolution::PolicyStatement inserimento AWS CloudFormation. Per ulteriori informazioni, inclusi esempi JSON e YAML modelli per AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e AWS::EntityResolution::PolicyStatement, consultate il riferimento al tipo di risorsa AWS Entity Resolution nella Guida per l'AWS CloudFormation utente.

Sono disponibili i seguenti modelli:

- Flusso di lavoro corrispondente

Crea un `MatchingWorkflow` oggetto, che memorizza la configurazione del processo di elaborazione dati da eseguire.

Per ulteriori informazioni, consulta i seguenti argomenti:

AWS::EntityResolution::MatchingWorkflow nella Guida per l'utente di AWS CloudFormation

CreateMatchingWorkflownel AWS Entity Resolution APIriferimento

- Mappatura dello schema

  Crea una mappatura dello schema, che definisce lo schema della tabella dei record dei clienti di input.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  AWS::EntityResolution::SchemaMapping nella Guida per l'utente di AWS CloudFormation

  CreateSchemaMappingnel riferimento AWS Entity Resolution API

- Workflow di mappatura degli ID

  Crea un `IdMappingWorkflow` oggetto, che memorizza la configurazione del processo di elaborazione dati da eseguire.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  AWS::EntityResolution::IdMappingWorkflow nella Guida per l'utente di AWS CloudFormation

  CreateIdMappingWorkflownel AWS Entity Resolution APIriferimento

- Namespace ID

  Crea un `IdNamespace` oggetto, che memorizza i metadati che spiegano il set di dati e come usarlo.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  AWS::EntityResolution::IdNamespace nella Guida per l'utente di AWS CloudFormation

  CreateIdNamespacenel riferimento AWS Entity Resolution API

- PolicyStatement

Crea un oggetto `PolicyStatement`.

Per ulteriori informazioni, consulta i seguenti argomenti:

AWS::EntityResolution::PolicyStatement nella Guida per l'utente di AWS CloudFormation

AddPolicyStatementnel AWS Entity Resolution APIriferimento

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- AWS CloudFormation APIRiferimento
- AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando

Quote per AWS Entity Resolution

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuno di essi. AWS servizio Salvo diversa indicazione, ogni quota si applica a una regione specifica. Puoi richiedere aumenti per alcune quote, ma altre quote non possono essere aumentate.

Per visualizzare le quote per AWS Entity Resolution, apri la console Service Quotas. Nel riquadro di navigazione, scegli Servizi AWS e seleziona AWS Entity Resolution.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo di aumento del limite.

La tua Account AWS ha le seguenti quote relative a. AWS Entity Resolution

Nome	Predefinita	Adattabile	Descrizione
Lavori simultanei di mappatura degli ID	1	No	Il numero massimo di processi di mappatura degli ID che possono essere elaborati contemporaneamente nella versione corrente. Regione AWS
Lavori di abbinamento simultanei	1	No	Il numero massimo di lavori corrispon denti che possono essere elaborati contemporaneamente nella versione corrente. Regione AWS
Lavori di abbinamento dei servizi del fornitore simultaneo	1	No	Il numero massimo di lavori di abbinamento dei servizi del provider che possono essere elaborati contemporaneamente nella versione corrente. Regione AWS
Input dei dati	20	No	Questo è l'elenco delle tabelle di input che si desidera utilizzare in un flusso di lavoro corrispondente. Ogni input corrisponde a una colonna nella tabella dei dati AWS Glue di input,

Nome	Predefinita	Adattabile	Descrizione
			che contiene il nome della colonna e informazioni aggiuntive AWS Entity Resolution utilizzate per scopi di corrispondenza. Gli input devono contenere un ID univoco più almeno un campo di input aggiuntivo.
Uscita dati	750	No	Questo è un elenco di `OutputAttribute` oggetti, ognuno dei quali ha i campi Name e Hashed. Ciascuno di questi oggetti rappresenta una colonna da includere nella tabella di AWS Glue output e indica se si desidera che i valori nella colonna vengano sottoposti a hash.
Schema dei dati	25	No	Il numero massimo di campi di input dello schema di dati.
Flussi di lavoro di mappatura degli ID	10	Sì	Il numero massimo di flussi di lavoro di mappatura degli ID che è possibile creare in questo Account AWS campo è quello corrente. Regione AWS
Namespace ID	10	Sì	Il numero massimo di namespace ID che è possibile creare in questo campo è quello corrente. Account AWS Regione AWS
Identifica gli ID	500	No	Il numero massimo di record che possono essere consolidati in un MatchID per carico di lavoro.

Nome	Predefinita	Adattabile	Descrizione
Regola della partita	15	No	Per la corrispondenza basata su regole, questo è il numero della regola applicata che ha generato un set di record corrispondente. Questo fa parte della corrispondenza dei metadati del flusso di lavoro che verranno inclusi nell'output.
Flussi di lavoro corrispondenti	10	Sì	Il numero massimo di flussi di lavoro corrispondenti.
Numero di regole per flusso di lavoro	15	No	Il numero massimo di regole per flusso di lavoro corrispondente.
Frequenza delle richieste API `GetMatchId`	50	Sì	Il numero massimo di richieste `GetCustomerID` API al secondo.
Mappature dello schema	50	Sì	Il numero massimo di mappature dello schema che è possibile creare in questo account nella regione corrente. AWS
Chiavi di abbinamento uniche per set di regole	15	No	Il numero massimo di chiavi di abbinamento univoche per set di regole. Una chiave di confronto indica AWS Entity Resolution quali campi di input devono essere considera ti come dati simili e quali devono essere considerati come dati diversi. Questo aiuta a configurare AWS Entity Resolution automaticamente le regole di corrispondenza basate su regole e a confrontare dati simili memorizzati in campi di input diversi.

Quote di limitazione per le API

Risorsa	Predefinito	Descrizione
Frequenza delle richieste `GetMatchId`	50 TPS	Numero massimo di chiamate `GetMatchId` API al secondo.

Cronologia dei documenti per la Guida per AWS Entity Resolution l'utente

La tabella seguente descrive le versioni della documentazione per AWS Entity Resolution.

Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi iscriverti al RSS feed. Per iscriverti agli RSS aggiornamenti, devi avere un RSS plug-in abilitato per il browser che stai utilizzando.

Modifica	Descrizione	Data
Integrazione con il provider	Aggiornamento solo della documentazione. I clienti possono imparare a integrars i come provider di servizi con. AWS Entity Resolution	8 agosto 2024
Flusso di lavoro di mappatura degli ID: aggiornamento	I clienti possono ora utilizzar e le regole di corrispondenza per tradurre i dati di prime parti in un flusso di lavoro di mappatura degli ID.	23 luglio 2024
Flusso di lavoro corrispon dente: aggiornamento	I clienti possono ora eliminare i record da un flusso di lavoro di abbinamento basato su regole o basato su ML per contribuire alla conformità alle normative sulla gestione dei dati.	8 aprile 2024
Flusso di lavoro di mappatura degli ID: aggiornamento	I clienti possono ora utilizzar e un flusso di lavoro di mappatura degli ID su più piattaforme. Account AWS	2 aprile 2024
AWS CloudFormation Risorse - Risorse nuove e aggiornate	AWSEntity Resolution ha aggiunto le seguenti risorse:	2 aprile 2024

	`AWS::EntityResolution::IdNamespace` `AWS::EntityResolution::PolicyStatement` e ha aggiornato la seguente risorsa:`AWS::EntityResolution::IdMappingWorkflow` .	
Trova Match ID	I clienti possono ora trovare il Match ID corrispondente e la regola associata per un flusso di lavoro elaborato basato su regole.	25 marzo 2024
Flusso di lavoro corrispondente: aggiornamento	AWS Entity Resolution ora supporta l'RAMPIDassegnazione PII basata sul flusso di lavoro di abbinamento basato sui servizi del LiveRamp provider.	12 febbraio 2024
AWS PrivateLink	AWS Entity Resolution ora supporta una sicurezza dei dati aggiuntiva AWS PrivateLink che aiuta i clienti ad accedere privatamente ai servizi ospitati su. AWS	20 ottobre 2023

AWS CloudFormation Risorse: risorse nuove e aggiornate	AWS Entity Resolution ha aggiunto la seguente risorsa `AWS::EntityResolution:IdMappingWorkflow` e aggiornato le seguenti risorse: `AWS::EntityResolution::MatchingWorkflow` e `AWS::EntityResolution::Schemamapping` .	19 ottobre 2023
Aggiornamento alla politica esistente	Le seguenti nuove autorizzazioni sono state aggiunte alla politica `AWSEntityResolutionConsoleFullAccess` gestita: `ADXReadAccess` e `ManageEventBridgeRules` .	16 ottobre 2023
Mappatura dello schema: aggiornamento	I clienti ora hanno la possibilità di modificare e aggiornare uno schema di dati esistente.	16 ottobre 2023
Flusso di lavoro corrispondente: aggiornamento	I clienti possono ora selezionare un servizio di fornitore di dati preferito per abbinare e collegare i propri dati.	16 ottobre 2023
Workflow di mappatura degli ID	I clienti possono utilizzare questo nuovo flusso di lavoro per specificare i dettagli della mappatura degli ID, scegliere il metodo di mappatura degli ID desiderato e specificare i campi di input e output dei dati.	16 ottobre 2023

AWS CloudFormation integration	AWS Entity Resolution ora si integra con. AWS CloudFormation	24 agosto 2023
AWS aggiornamento gestito delle politiche - Nuove politiche	AWS Entity Resolution ha aggiunto due nuove politiche gestite.	18 agosto 2023
Versione iniziale	Versione iniziale della Guida per l' AWS Entity Resolution utente	26 luglio 2023

AWS Entity Resolution Glossario

Nome risorsa Amazon (ARN)

Un identificatore univoco per AWS le risorse. ARNssono obbligatori quando è necessario specificare una risorsa in modo inequivocabile per tutti AWS Entity Resolution, ad esempio nelle AWS Entity Resolution policy, nei tag di Amazon Relational Database Service (AmazonRDS) e nelle chiamate. API

Elaborazione automatica

Un'opzione di cadenza di elaborazione per un processo corrispondente al flusso di lavoro che ne consente l'esecuzione automatica quando l'immissione dei dati cambia.

Questa opzione è disponibile solo per la corrispondenza basata su regole.

Per impostazione predefinita, la cadenza di elaborazione per un processo di workflow corrispondente è impostata su Manuale, il che consente l'esecuzione su richiesta. È possibile impostare l'elaborazione automatica per eseguire automaticamente il processo del flusso di lavoro corrispondente quando l'immissione dei dati cambia. Ciò mantiene l'output del flusso di lavoro corrispondente up-to-date.

AWS KMS key ARN

Questo è il tuo AWS KMS Amazon Resource Name (ARN) per la crittografia a riposo. Se non viene fornita, il sistema utilizzerà una KMS chiave AWS Entity Resolution gestita.

Testo in chiaro

Dati che non sono protetti crittograficamente.

Livello di confidenza () ConfidenceLevel

Per la corrispondenza ML, questo è il livello di confidenza applicato AWS Entity Resolution quando ML identifica un set di record corrispondente. Questo fa parte dei metadati del flusso di lavoro corrispondenti che verranno inclusi nell'output.

Decrittografia

Il processo di riconversione dei dati crittografati nella loro forma originale. La decrittografia può essere eseguita solo se si ha accesso alla chiave segreta.

Crittografia

Processo di codifica dei dati in un formato che appare casuale utilizzando un valore segreto chiamato chiave. È impossibile determinare il testo in chiaro originale senza accedere alla chiave.

Group name (Nome gruppo)

Il nome del gruppo fa riferimento all'intero gruppo di campi di input e può aiutarti a raggruppare i dati analizzati per scopi corrispondenti.

Ad esempio, se sono presenti tre campi di input:**`first_name`**,**`middle_name`**, e**`last_name`**, puoi raggrupparli inserendo il nome del gruppo **`full_name`** per la corrispondenza e l'output.

Hash

L'hashing significa applicare un algoritmo crittografico che produce una stringa irreversibile e unica di caratteri di dimensione fissa, chiamata hash. AWS Entity Resolution utilizza il protocollo hash Secure Hash Algorithm a 256 bit (SHA256) e restituirà una stringa di caratteri da 32 byte. In AWS Entity Resolution, puoi scegliere se eseguire l'hash dei valori dei dati nell'output.

Protocollo hash () HashingProtocol

AWS Entity Resolution utilizza il protocollo hash Secure Hash Algorithm a 256 bit (SHA256) e restituirà una stringa di caratteri da 32 byte. Questo fa parte dei metadati corrispondenti del flusso di lavoro che verranno inclusi nell'output.

Metodo di mappatura degli ID

Come desideri che venga eseguita la mappatura degli ID.

Esistono due metodi di mappatura degli ID:

- Basato su regole: il metodo con cui si utilizzano le regole di corrispondenza per tradurre i dati di prime parti da un'origine a una destinazione in un flusso di lavoro di mappatura degli ID.

- Servizi provider: il metodo con cui si utilizza un servizio provider per tradurre dati codificati da terze parti da un'origine a una destinazione in un flusso di lavoro di mappatura degli ID.

  AWS Entity Resolution attualmente supporta LiveRamp come metodo di mappatura degli ID basato sui servizi del provider. È necessario disporre di un abbonamento a LiveRamp through per AWS Data Exchange utilizzare questo metodo. Per ulteriori informazioni, consulta Fase 1: Abbonarsi a un servizio fornito da un provider su AWS Data Exchange.

Workflow di mappatura degli ID

Un processo di elaborazione dati che mappa i dati da un'origine dati di input a una destinazione di dati di input in base al metodo di mappatura ID specificato. Produce una tabella di mappatura degli ID. Questo flusso di lavoro richiede di specificare il metodo di mappatura degli ID e i dati di input che si desidera tradurre da un'origine a una destinazione.

È possibile configurare un flusso di lavoro di mappatura degli ID da eseguire autonomamente Account AWS o tra due. Account AWS

Spazio dei nomi ID

Una risorsa AWS Entity Resolution che contiene metadati che spiegano i set di dati suddivisi in più set Account AWS e come utilizzarli in un flusso di lavoro di mappatura degli ID.

Esistono due tipi di namespace ID: e. `SOURCE` `TARGET` `SOURCE`Contiene configurazioni per i dati di origine che verranno elaborati in un flusso di lavoro di mappatura degli ID. `TARGET`Contiene una configurazione dei dati di destinazione in cui verranno risolte tutte le fonti. Per definire i dati di input che desideri risolvere tra due Account AWS, crea un'origine dello spazio dei nomi ID e una destinazione dello spazio dei nomi ID per tradurre i dati da un set () all'altro ()`SOURCE`. `TARGET`

Dopo che tu e un altro membro avete creato gli spazi dei nomi ID ed eseguito un flusso di lavoro di mappatura degli ID, potete partecipare a una collaborazione AWS Clean Rooms per eseguire un join multitavola sulla tabella di mappatura degli ID e analizzare i dati.

Per ulteriori informazioni, consulta la Guida per l'utente AWS Clean Rooms.

Campo di input

Un campo di input corrisponde al nome di una colonna della tabella dei dati AWS Glue di input.

Fonte di input ARN (InputSourceARN)

L'Amazon Resource Name (ARN) che è stato generato per l'input di una AWS Glue tabella. Questo fa parte della corrispondenza dei metadati del flusso di lavoro che verranno inclusi nell'output.

Input type (Tipo input)

Il tipo di dati di input. Lo si seleziona da un elenco preconfigurato di valori come nome, indirizzo, numero di telefono o indirizzo e-mail. Il tipo di input indica il AWS Entity Resolution tipo di dati che gli stai presentando, consentendone la corretta classificazione e normalizzazione.

Abbinamento basato sull'apprendimento automatico

La corrispondenza basata sull'apprendimento automatico (corrispondenza ML) trova corrispondenze tra i dati che potrebbero essere incomplete o che potrebbero non avere esattamente lo stesso aspetto. La corrispondenza ML è un processo preimpostato che tenterà di abbinare i record di tutti i dati inseriti. La corrispondenza ML restituisce un ID di corrispondenza e un livello di confidenza per ogni set di dati corrispondente.

Elaborazione manuale

Un'opzione di cadenza di elaborazione per un processo corrispondente al flusso di lavoro che ne consente l'esecuzione su richiesta.

Questa opzione è impostata di default ed è disponibile sia per la corrispondenza basata su regole che per la corrispondenza basata sull'apprendimento automatico.

Abbinamento da molti a molti

M any-to-many matching confronta più istanze di dati simili. I valori nei campi di input a cui è stata assegnata la stessa chiave di confronto verranno confrontati tra loro, indipendentemente dal fatto che si trovino nello stesso campo di input o in campi di input diversi.

Ad esempio, potresti avere più campi di immissione del numero di telefono come `mobile_phone` e `home_phone` con la stessa chiave di corrispondenza «Telefono». Utilizza la many-to-many corrispondenza per confrontare i dati nel campo `mobile_phone` di input con i dati nel campo `mobile_phone` di input e i dati nel campo `home_phone` di input.

Le regole di corrispondenza valutano i dati in più campi di input con la stessa chiave di corrispondenza con un'operazione (or) e la one-to-many corrispondenza confronta i valori tra più campi di input. Ciò significa che se una combinazione `mobile_phone` o `home_phone` corrisponde tra due record, la chiave di corrispondenza «Telefono» restituirà una corrispondenza. Per trovare una corrispondenza, digita «Telefono» per trovare una corrispondenza, `Record One mobile_phone = Record Two mobile_phone` `Record One mobile_phone = Record Two home_phone` OR `Record One home_phone = Record Two home_phone` OR`Record One home_phone = Record Two mobile_phone`.

ID della partita (MatchID)

Per la corrispondenza basata su regole e la corrispondenza ML, questo è l'ID generato AWS Entity Resolution e applicato a ciascun set di record corrispondente. Questo fa parte dei metadati del flusso di lavoro corrispondenti che verranno inclusi nell'output.

Chiave Match () MatchKey

La chiave Match indica AWS Entity Resolution quali campi di input considerare come dati simili e quali come dati diversi. Questo aiuta a configurare AWS Entity Resolution automaticamente le regole di corrispondenza basate su regole e a confrontare dati simili memorizzati in diversi campi di input.

Se nei dati sono presenti più tipi di informazioni relative ai numeri di telefono, ad esempio un campo `home_phone` di immissione e un campo di input, che desideri confrontare, puoi assegnare a entrambi il tasto di corrispondenza «Telefono». `mobile_phone` È quindi possibile configurare la corrispondenza basata su regole per confrontare i dati utilizzando le istruzioni «or» in tutti i campi di input con la chiave di corrispondenza «Telefono» (vedi le definizioni di corrispondenza uno-a-uno e di corrispondenza manto-a-molti nella sezione Corrispondenza tra flussi di lavoro).

Se desideri che la corrispondenza basata su regole consideri diversi tipi di informazioni sui numeri di telefono in modo completamente separato, puoi creare chiavi di corrispondenza più specifiche come «Mobile_Phone» e «Home_Phone». Quindi, quando configuri un flusso di lavoro di corrispondenza, puoi specificare come verrà utilizzata ogni chiave di corrispondenza telefonica nella corrispondenza basata su regole.

Se MatchKey si specifica no per un particolare campo di input, questo non può essere utilizzato per la corrispondenza, ma può essere eseguito attraverso il processo del flusso di lavoro di abbinamento e, se lo si desidera, può essere emesso.

Nome della chiave corrispondente

Il nome assegnato a una Match Key.

Regola del match (MatchRule)

Per la corrispondenza basata su regole, questo è il numero della regola applicata che ha generato un set di record corrispondente. Questo fa parte dei metadati del flusso di lavoro corrispondenti che verranno inclusi nell'output.

Corrispondenza

Il processo di combinazione e confronto dei dati provenienti da diversi campi, tabelle o database di input e la determinazione di quali di essi sono simili, o «corrispondono», in base al soddisfacimento di determinati criteri di corrispondenza (ad esempio, attraverso regole o modelli di corrispondenza).

Flusso di lavoro corrispondente

Il processo impostato per specificare i dati di input da abbinare e il modo in cui deve essere eseguita la corrispondenza.

Descrizione del flusso di lavoro corrispondente

Una descrizione opzionale del flusso di lavoro corrispondente che puoi scegliere di inserire. Le descrizioni ti aiutano a distinguere tra flussi di lavoro corrispondenti se ne crei più di uno.

Nome del flusso di lavoro corrispondente

Il nome del flusso di lavoro corrispondente specificato.

> **Note**
>
> I nomi dei flussi di lavoro corrispondenti devono essere univoci. Non possono avere lo stesso nome o verrà restituito un errore.

Metadati del flusso di lavoro corrispondenti

Informazioni generate e prodotte da AWS Entity Resolution durante un processo di workflow corrispondente. Queste informazioni sono obbligatorie in fase di output.

Normalizzazione () ApplyNormalization

Scegli se normalizzare i dati di input come definito nello schema. La normalizzazione standardizza i dati rimuovendo spazi aggiuntivi e caratteri speciali e standardizzandoli in formato minuscolo.

Ad esempio, se un campo di input ha un tipo di input di `PHONE_NUMBER` e i valori nella tabella di input sono formattati come`(123) 456-7890`, AWS Entity Resolution i valori verranno normalizzati in. `1234567890`

Le seguenti sezioni descrivono le regole di normalizzazione.

Argomenti

Nome

- TRIM= Taglia gli spazi bianchi iniziali e finali
- LOWERCASE= Mette in minuscolo tutti i caratteri alfa
- CONVERT_ ACCENT = Trasforma da lettera accentata a lettera normale
- REMOVE_ _ ALL NON _ ALPHA = Rimuove tutti i caratteri non alfa [a-zA-Z]

E-mail

- TRIM= Taglia gli spazi bianchi iniziali e finali
- LOWERCASE= Mette in minuscolo tutti i caratteri alfa

- CONVERT_ ACCENT = Trasforma da lettera accentata a lettera normale
- REMOVE_ _ ALL _ NON EMAIL _ CHARS = Rimuove tutti i non-alpha-numeric caratteri [a-zA-Z0-9] e [.@-]

Telefono

- TRIM= Taglia gli spazi bianchi iniziali e finali
- REMOVE_ _ ALL NON _ NUMERIC = Rimuove tutti i caratteri non numerici [0-9]
- REMOVE_ _ ALL LEADING _ ZEROES = Rimuove tutti gli zeri iniziali

Indirizzo

- TRIM= Taglia gli spazi bianchi iniziali e finali
- LOWERCASE= Mette in minuscolo tutti i caratteri alfa
- CONVERT_ ACCENT = Trasforma da lettera accentata a lettera normale
- REMOVE_ _ ALL NON _ ALPHA = Rimuove tutti i caratteri non alfa [a-zA-Z]
- RENAME_ WORDS usando _ ADDRESS _ RENAME WORD _ MAP = sostituisce le parole nella stringa di indirizzo con le parole di _ _ _ ADDRESS RENAME WORD MAP
- RENAME_ DELIMITERS usando ADDRESS _ _ RENAME DELIMITER _ MAP = sostituisci i delimitatori nella stringa di indirizzo con la stringa di ADDRESS_ _ _ RENAME DELIMITER MAP
- RENAME_ DIRECTIONS usando _ ADDRESS _ RENAME DIRECTION _ MAP = sostituisci i delimitatori nella stringa di indirizzo con la stringa di _ _ _ ADDRESS RENAME DIRECTION MAP
- RENAME_ NUMBERS usando ADDRESS _ _ RENAME NUMBER _ MAP = sostituisci i numeri nella stringa di indirizzo con la stringa di ADDRESS_ _ _ RENAME NUMBER MAP
- RENAME_ SPECIAL _ CHARS usando ADDRESS _ _ RENAME _ SPECIAL CHAR _ MAP = sostituisci i caratteri speciali nella stringa di indirizzo con la stringa di ADDRESS_ RENAME _ SPECIAL _ CHAR _ MAP

ADDRESS_RENAME_WORD_MAP

Queste sono le parole che verranno rinominate durante la normalizzazione della stringa di indirizzo.

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

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

ADDRESS_RENAME_DELIMITER_MAP

Questi sono i delimitatori che verranno rinominati durante la normalizzazione della stringa di indirizzo.

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

ADDRESS_RENAME_DIRECTION_MAP

Questi sono gli identificatori di direzione che verranno rinominati durante la normalizzazione della stringa di indirizzo.

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

ADDRESS_RENAME_NUMBER_MAP

Queste sono le stringhe numeriche che verranno rinominate durante la normalizzazione della stringa di indirizzo.

```
"número": "number",
 "numero": "number",
 "no": "number",
 "núm": "number",
 "num": "number"
```

ADDRESS_RENAME_SPECIAL_CHAR_MAP

Queste sono le stringhe di caratteri speciali che verranno rinominate durante la normalizzazione della stringa di indirizzo.

```
"ß": "ss",
 "ä": "ae",
 "ö": "oe",
 "ü": "ue",
 "ø": "o",
 "æ": "ae"
```

Con hash

- TRIM= Taglia gli spazi bianchi iniziali e finali

ID_origine

- TRIM= Taglia gli spazi bianchi iniziali e finali

Abbinamento uno a uno

O ne-to-one matching confronta singole istanze di dati simili. I campi di input con la stessa chiave di corrispondenza e i valori nello stesso campo di input verranno confrontati tra loro.

Ad esempio, potresti avere più campi di immissione del numero di telefono come `mobile_phone` e `home_phone` con la stessa chiave di corrispondenza «Telefono». Utilizza la one-to-one corrispondenza per confrontare i dati nel campo `mobile_phone` di input con i dati nel campo `mobile_phone` di input e per confrontare i dati nel campo `home_phone` di input con i dati nel campo `home_phone` di input. I dati nel campo `mobile_phone` di input non verranno confrontati con i dati nel campo `home_phone` di input.

Le regole di corrispondenza valutano i dati in più campi di input con la stessa chiave di corrispondenza con un'operazione (or) e la one-to-many corrispondenza confronta i valori all'interno di un singolo campo di input. Ciò significa che se `mobile_phone` o `home_phone` corrisponde tra due record, la chiave di corrispondenza «Telefono» restituirà una corrispondenza. Per trovare una corrispondenza, digita «Telefono» per trovare una corrispondenza, `Record One mobile_phone = Record Two mobile_phone` OR`Record One home_phone = Record Two home_phone`.

Le regole di corrispondenza valutano i dati nei campi di input con chiavi di corrispondenza diverse con un'operazione (and). Se desideri che la corrispondenza basata su regole consideri diversi tipi di informazioni sui numeri di telefono in modo completamente separato, puoi creare chiavi di corrispondenza più specifiche come «mobile_phone» e «home_phone». Se desideri utilizzare entrambi i tasti di corrispondenza in una regola per trovare le corrispondenze,. `Record One mobile_phone = Record Two mobile_phone` AND `Record One home_phone = Record Two home_phone`

Output

Un elenco di OutputAttributeoggetti, ognuno dei quali ha i campi Name e Hashed. Ciascuno di questi oggetti rappresenta una colonna da includere nella tabella di AWS Glue output e indica se si desidera che i valori nella colonna vengano sottoposti a hash.

Outputs3Path

La destinazione S3 in cui AWS Entity Resolution verrà scritta la tabella di output.

OutputSourceConfig

Un elenco di OutputSource oggetti, ognuno dei quali ha i campi outputs3Path e Output. ApplyNormalization

Abbinamento basato sui servizi del provider

L'abbinamento basato sui servizi dei provider è un processo progettato per abbinare, collegare e migliorare i record con i fornitori di servizi di dati preferiti e i set di dati con licenza. È necessario disporre di un abbonamento al AWS Data Exchange servizio del provider per utilizzare questa tecnica di abbinamento.

AWS Entity Resolution attualmente si integra con i seguenti fornitori di servizi di dati:

- LiveRamp
- TransUnion
- UID2.0

Abbinamento basato su regole

La corrispondenza basata su regole è un processo progettato per trovare corrispondenze esatte. La corrispondenza basata su regole è un insieme gerarchico di regole di abbinamento a cascata, suggerite da AWS Entity Resolution, basate sui dati inseriti e completamente configurabili dall'utente. Tutte le chiavi di corrispondenza fornite nell'ambito dei criteri delle regole devono corrispondere esattamente affinché i dati confrontati vengano dichiarati corrispondenti e i metadati associati vengano emessi. La corrispondenza basata su regole restituisce un Match ID e un numero di regola per ogni set di dati corrispondente.

Consigliamo di definire regole che possano identificare in modo univoco un'entità. Ordina prima le tue regole per trovare corrispondenze più precise.

Ad esempio, supponiamo che tu abbia due regole, la Regola 1 e la Regola 2.

Queste regole hanno le seguenti chiavi di abbinamento:

- La regola 1 include nome completo e indirizzo
- La regola 2 include nome completo, indirizzo e telefono

Poiché la Regola 1 viene eseguita per prima, non verranno trovate corrispondenze secondo la Regola 2 perché sarebbero state tutte trovate secondo la Regola 1.

Per trovare le corrispondenze differenziate per telefono, riordina le regole, in questo modo:

- La regola 2 include nome completo, indirizzo e telefono
- La regola 1 include nome completo e indirizzo

Schema

Termine usato per una struttura o un layout che definisce come un insieme di dati è organizzato e connesso.

Descrizione dello schema

Una descrizione facoltativa dello schema che puoi scegliere di inserire. Le descrizioni consentono di distinguere tra le mappature dello schema se ne vengono create più di una.

Nome dello schema

Il nome dello schema.

> **Note**
>
> I nomi degli schemi devono essere univoci. Non possono avere lo stesso nome o verrà restituito un errore.

Mappatura dello schema

La mappatura dello schema AWS Entity Resolution è il processo mediante il quale si spiega AWS Entity Resolution come interpretare i dati per la corrispondenza. Definisci lo schema della tabella dei dati di input che desideri AWS Entity Resolution leggere in un flusso di lavoro corrispondente.

Mappatura dello schema ARN

L'Amazon Resource Name (ARN) generato per la mappatura dello schema.

ID univoco

Un identificatore univoco designato dall'utente e che deve essere assegnato a ogni riga di dati di input che AWS Entity Resolution viene letta.

Example

Ad esempio: **`Primary_key`**, **`Row_ID`** o **`Record_ID`**.

La colonna ID univoco è obbligatoria.

L'ID univoco deve essere un identificatore univoco all'interno di una singola tabella.

In tabelle diverse, l'ID univoco può avere valori duplicati.

Quando viene eseguito il flusso di lavoro corrispondente, il record verrà rifiutato se l'ID univoco:

- non è specificato
- non è unico all'interno della stessa tabella
- si sovrappone in termini di nome dell'attributo tra le fonti.
- supera i 38 caratteri (solo flussi di lavoro di abbinamento basati su regole)

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.