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 tracciare meglio i prodotti che utilizzano codici diversi (ad esempio, SKU, UPC) nei tuoi negozi. 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
- Configurazione 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 interattiva o un editor JSON. 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 lettere minuscole. 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 l'API AWS Management Console e/o AWS CLI, puoi eseguire l'elaborazione manuale in blocco su richiesta, in base alla pipeline di dati di estrazione, trasformazione e caricamento (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'operazione AWS Entity Resolution GetMatchId API consente di recuperare in modo sincrono un Match ID esistente. Puoi chiamare AWS Entity Resolution con attributi di informazioni di identificazione personale (PII) 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'operazione AWS Entity Resolution GetMatchId API per scoprire se questo cliente o entità esiste già nei risultati corrispondenti archiviati 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 tue applicazioni di origine, come i sistemi di gestione delle relazioni con i clienti (CRM) o della piattaforma dati con i 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 Servizi AWS 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 Cos'è AWS Glue? nella Guida per gli AWS Glue sviluppatori.

- AWS CloudTrail

  AWS Entity Resolution Utilizzalo con CloudTrail i log per migliorare l'analisi delle Servizio AWS 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 Creazione di risorse AWS Entity Resolution 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/.
- A livello di codice tramite l'API. AWS Entity Resolution Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS Entity Resolution .
  - Se prevedi di chiamare l' AWS Entity Resolution API in AWS Lambda Runtime, crea il tuo pacchetto di distribuzione e includi la versione desiderata della libreria AWS SDK. Per ulteriori informazioni, consulta i seguenti esempi nella Guida per gli AWS Lambda sviluppatori:
    - Implementa le funzioni Java Lambda con archivi di file.zip o JAR
    - 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.

Configurazione AWS Entity Resolution

Prima di AWS Entity Resolution utilizzarlo per la prima volta, completa le seguenti attività.

Argomenti

Iscriviti per AWS

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

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
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 Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

Creare 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 Best practice per la sicurezza in IAM nella Guida per l'utente di IAM.	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.	Segui le istruzioni in Creazione del primo utente e gruppo di utenti IAM di amministrazione nella Guida per l'utente di IAM.	Configura l'accesso programmatico seguendo quanto riportato in Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM.

Iscriviti a un provider di servizi su AWS Data Exchange

Completa la procedura seguente se utilizzi un flusso di lavoro di abbinamento basato sui servizi del provider o un flusso di lavoro di mappatura degli ID. Se non utilizzi un flusso di lavoro di abbinamento basato sui servizi del provider o un flusso di lavoro di mappatura degli ID, puoi saltare questo passaggio.

In AWS Entity Resolution, puoi scegliere di eseguire un flusso di lavoro corrispondente con uno dei seguenti servizi del provider se hai un abbonamento con quel provider attivo. AWS Data Exchange I tuoi dati verranno abbinati a una serie di input definiti dal tuo provider preferito.

- LiveRamp
  - LiveRamp Risoluzione dell'identità
  - LiveRamp Transcodifica
- 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

Inoltre, puoi eseguire un flusso di lavoro di mappatura degli ID LiveRamp se hai un abbonamento con quel provider.

- LiveRamp
  - LiveRamp Transcodifica

Esistono due modi per abbonarsi a un servizio fornito da un provider:

- 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'offerta BYOS. AWS Data Exchange

Dopo esserti abbonato a un servizio fornito da un provider 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 provider che contiene API, consulta Accedere a un prodotto API nella Guida per l'utente.AWS Data Exchange

Preparare le tabelle di dati

In AWS Entity Resolution, ciascuna delle 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 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 CatalogÈ quindi possibile utilizzare la tabella dati come input per. AWS Entity Resolution

La preparazione delle tabelle di dati prevede i seguenti passaggi:

Argomenti

Fase 1: Preparare i dati di input

Completate la seguente procedura se utilizzate un flusso di lavoro corrispondente con un servizio fornito da un provider. Se non stai utilizzando un flusso di lavoro corrispondente a un servizio del provider, puoi saltare questo passaggio.

Per ulteriori informazioni, consulta Iscriviti a un provider di servizi su AWS Data Exchange.

Se desideri eseguire un flusso di lavoro corrispondente con un flusso di lavoro di abbinamento basato sui servizi del provider o un flusso di lavoro di mappatura degli ID, consulta la tabella seguente per preparare i dati di input:

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 per la formattazione dei file di input per il flusso di lavoro corrispondente, consulta Eseguire la risoluzione delle identità tramite 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 Eseguire la transcodifica tramite ADX nella documentazione. LiveRamp
TransUnion	Sì	Verificate quanto segue: • Esiste un ID univoco per l'arricchimento TransUnion dei dati.

Servizio del fornitore	È necessario un ID univoco?	Azioni

		Note
		Gli attributi di trasmissione possono persistere in input e output a. TransUnion Le chiavi Household E 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
		• **`Email addresses`** deve essere in testo semplice.
		• **`First Name`** può essere minuscolo o maiuscolo, i soprannomi sono supportati, ma

Servizio del fornitore	È necessario un ID univoco?	Azioni
		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. • UID2 supporta sia l'e-mail che il numero di telefono per la generazione di UID2. 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 generazione di UID2 e il secondo record utilizza il numero di telefono. Se i dati includono una combinazione di e-mail e numeri di telefono e non si desidera 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.

Servizio del fornitore	È necessario un ID univoco?	Azioni
		Note Un indirizzo email o un numero di telefono specifico, in un momento specifico, restituisce lo stesso valore UID2 non elaborato, indipendentemente da chi ha effettuato la richiesta. Gli UID2 grezzi vengono creati aggiungendo sali provenienti da secchi di sale che vengono ruotati circa una volta all'anno, facendo ruotare anche l'UID2 grezzo. I diversi secchi di sale ruotano in momenti diversi durante l'anno. AWS Entity Resolution attualmente non tiene traccia dei secchi di sale rotanti e degli UID2 grezzi, quindi si consiglia di rigenerare gli UID2 grezzi ogni giorno. Per ulteriori informazioni, vedi Con che frequenza devono essere aggiornati gli UID2 per gli aggiornamenti incrementali? nella documentazione UID 2.0.

Fase 2: Salvate la tabella dei dati di input in un formato di dati supportato

Se hai già salvato i dati di input 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 3: 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 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 4: 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. Accedere AWS Management Console e aprire 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 ruolo IAM, scegli Scegli un ruolo IAM esistente, quindi scegli Avanti.

   Puoi anche scegliere Crea un ruolo IAM o chiedere al tuo amministratore di creare il ruolo IAM, 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 tuo database}.
    a. Visualizza le tabelle nel AWS Glue database.
    b. Per visualizzare lo schema di una tabella, seleziona una tabella specifica.
13. Prendi nota del nome del AWS Glue database e del nome della AWS Glue tabella.

Crea un ruolo IAM per un utente della console

Per creare un ruolo IAM

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

   Puoi utilizzare Roles per creare credenziali a breve termine, operazione consigliata per una maggiore sicurezza. Puoi anche scegliere Utenti per creare credenziali a lungo termine.
3. Scegli 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 scheda JSON, 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 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. Scegli Crea ruolo.

Crea 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. Puoi creare questo ruolo utilizzando la console se disponi delle autorizzazioni IAM 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 console IAM all'indirizzo https://console.aws.amazon.com/iam/ con il tuo account amministratore.
2. In Access management (Gestione accessi), scegli Roles (Ruoli).

   Puoi utilizzare Roles per creare credenziali a breve termine, operazione consigliata per una maggiore sicurezza. Puoi anche scegliere Utenti per creare credenziali a lungo termine.
3. Scegli 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'editor JSON.

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

6. Seleziona Successivo.
7. Per Aggiungi autorizzazioni, scegli Crea politica.

   Viene visualizzata una nuova scheda.

   a. Copia e incolla la seguente politica nell'editor JSON.

   > **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 uguali Regione AWS a. 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 ogni *{{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 uguali Regione AWS a. `AWS Entity Resolution`
accountId	Il tuo Account AWS ID.
bucket di input	Bucket Amazon S3 che contengono gli oggetti dati sottostanti da AWS Glue cui `AWS Entity Resolution` verranno letti.
bucket di uscita	Bucket Amazon S3 in cui `AWS Entity Resolution` verranno generati i dati di output.
database di input	AWS Glue database da cui `AWS Entity Resolution` leggerà.

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

```
        {
```

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

Sostituisci ogni *{{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 uguali Regione AWS a. `AWS Entity Resolution`
accountId	Il tuo Account AWS ID.
Tasti di input	Chiavi gestite in ingresso. AWS Key Management Service Se le fonti di input sono crittografate, 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 ogni *{{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 uguali Regione AWS a. `AWS Entity Resolution`
accountId	Il tuo Account AWS ID.
Chiavi di uscita	Chiavi gestite in ingresso. AWS Key Management Service Se è necessari o 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 nell'asset 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 console. AWS Data Exchange
ID revisione	La revisione del set di dati, trovata sulla console. AWS Data Exchange
AssetID	L'ID della risorsa, che si trova 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. Scegli Crea ruolo.

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

Creazione di una mappatura dello schema

Per definire i dati di input che desideri risolvere, crea una mappatura dello schema. Il processo di mappatura dello schema guida l'utente attraverso una serie di passaggi per definire i dati da risolvere definendo i campi di input e i tipi di attributi e quindi definendo e raggruppando le chiavi di confronto.

Esistono tre modi per creare una mappatura dello schema in: AWS Entity Resolution

- Utilizzo di un flusso guidato per importare le informazioni sullo schema esistente.
- Utilizzo di un flusso guidato per definire manualmente i dati di input.
- Utilizzo dell'editor JSON per creare, incollare o importare una mappatura dello schema.

Il seguente processo guida l'utente attraverso i tre diversi metodi per creare una mappatura dello schema.

Argomenti

- Creare una mappatura dello schema (colonne precompilate)
- Crea una mappatura dello schema (colonne definite manualmente)
- Crea una mappatura dello schema (editor JSON)

Creare una mappatura dello schema (colonne precompilate)

Questa procedura descrive il processo di creazione di una mappatura dello schema utilizzando l' AWS Glue opzione Importa da sulla AWS Entity Resolution console. È possibile utilizzare questo metodo di creazione per definire i campi di input a partire da colonne precompilate di una tabella. AWS Glue

Per creare la mappatura dello schema utilizzando colonne precompilate:

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 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.

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 passthrough.

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

g. Seleziona Successivo.

5. Per il passaggio 2: mappare i campi di immissione, procedi come segue:

a. Per i campi di input da abbinare, specifica il tipo di input e il tasto Match per ogni campo 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.

   > **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.

b. Seleziona Successivo.

6. Per la Fase 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. Seleziona 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.

Crea una mappatura dello schema (colonne definite manualmente)

Questa procedura descrive il processo di creazione di una mappatura dello schema utilizzando l'opzione Crea schema personalizzato sulla AWS Entity Resolution console. Utilizzate questo metodo di creazione per definire manualmente i campi di input utilizzando un flusso guidato.

Per creare la mappatura dello schema utilizzando colonne definite manualmente

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 opzionale.

   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.

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

   e. Seleziona Successivo.
5. Per il passaggio 2: mappare i campi di immissione, procedi come segue:

   a. Per i campi di input da abbinare, aggiungi il campo di input, il tipo di input e la chiave Match.

      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.

> **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 dati PII nell'output, devi specificare il tipo di input come stringa personalizzata.

b. (Facoltativo) Per i campi di input da utilizzare, aggiungi i campi di input che non corrisponderanno.

c. Seleziona 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. Seleziona 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.

Crea una mappatura dello schema (editor JSON)

Questa procedura descrive il processo di creazione di una mappatura dello schema utilizzando l'opzione Usa editor JSON sulla console.AWS Entity Resolution Utilizzate questo metodo di creazione per utilizzare un editor JSON per creare, incollare o importare una mappatura dello schema. I campi ID univoco e input non sono disponibili con questa opzione.

Per creare la 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 opzionale.

    b. Per il metodo di creazione, scegli Usa l'editor JSON.

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

d. Seleziona Successivo.

5. Per il passaggio 2: Specificare la mappatura:

a. Inizia a creare lo schema nell'editor JSON o scegli una delle seguenti opzioni:

Se vuoi...	Allora scegli...
Inizia a creare la tua mappatura dello schema	Inserisci un JSON di esempio e modifica le informazioni secondo necessità.
Usa un file JSON esistente	Importa da file

b. Seleziona 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.

Creazione di un flusso di lavoro corrispondente

Dopo aver creato una mappatura dello schema, puoi creare uno o più flussi di lavoro corrispondenti per specificare gli input di dati, le fasi di normalizzazione e scegliere le tecniche di corrispondenza desiderate. Esistono tre tecniche di abbinamento:

- La corrispondenza basata su regole è un insieme gerarchico di regole di abbinamento a cascata, suggerite da AWS Entity Resolution, basate sui dati immessi e completamente configurabili dall'utente.
- La corrispondenza basata sull'apprendimento automatico è un processo preimpostato che tenterà di abbinare i record di tutti i dati inseriti.
- I servizi del fornitore ti consentono di abbinare i tuoi identificatori noti al tuo fornitore di servizi dati preferito.

  AWS Entity Resolution attualmente si integra con i seguenti fornitori di servizi dati: LiveRamp TransUnion, e UID 2.0. È possibile utilizzare un abbonamento pubblico per questi provider AWS Data Exchange o negoziare un'offerta privata direttamente con il fornitore di dati. Per ulteriori informazioni, consulta Iscriviti a un provider di servizi su AWS Data Exchange.

AWS Entity Resolution legge i dati dalle posizioni specificate dall'utente e scrive i risultati 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 tuoi dati.

Puoi anche utilizzare l'output della corrispondenza basata su regole o ML come input per la corrispondenza basata sui servizi del provider o viceversa per soddisfare le tue esigenze aziendali. Ad esempio, puoi prima eseguire la corrispondenza basata su regole per trovare corrispondenze nei tuoi dati e quindi inviare un sottoinsieme di record non corrispondenti alla corrispondenza basata sui servizi del provider per risparmiare sui costi di abbonamento del provider.

Argomenti

Crea un flusso di lavoro di abbinamento basato su regole

Il flusso di lavoro di abbinamento basato su regole ti 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.

Per la corrispondenza basata su regole, applica il numero della regola 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. Specificate le autorizzazioni di accesso al servizio selezionando Crea e utilizza un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

Se scegli...	THEN
Crea e utilizza un nuovo ruolo di servizio	• AWS Entity Resolution crea un ruolo di servizio con la politica richiesta per questa tabella.

Se scegli...	THEN
	• 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 chiave KMS e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati di input.

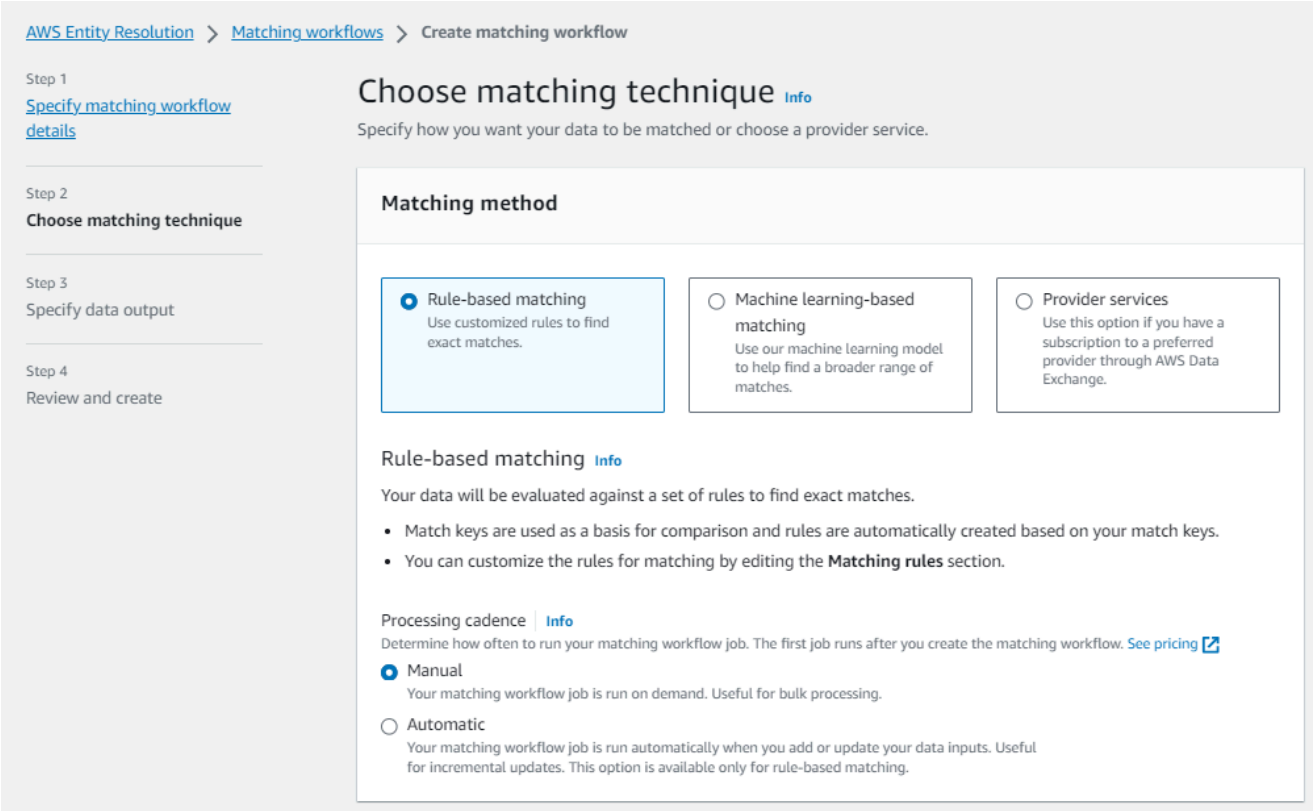
Se scegli...	THEN
Usa un ruolo di servizio esistente	1. Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. L'elenco dei ruoli viene visualizzato se si dispone delle autorizzazioni per elencare i ruoli. Se non disponi delle autorizza zioni per elencare i ruoli, puoi inserire l'Amazon 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 esterno View in IAM. 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. Seleziona Successivo.

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

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



b. Per Processing cadence, scegliete una delle seguenti opzioni.

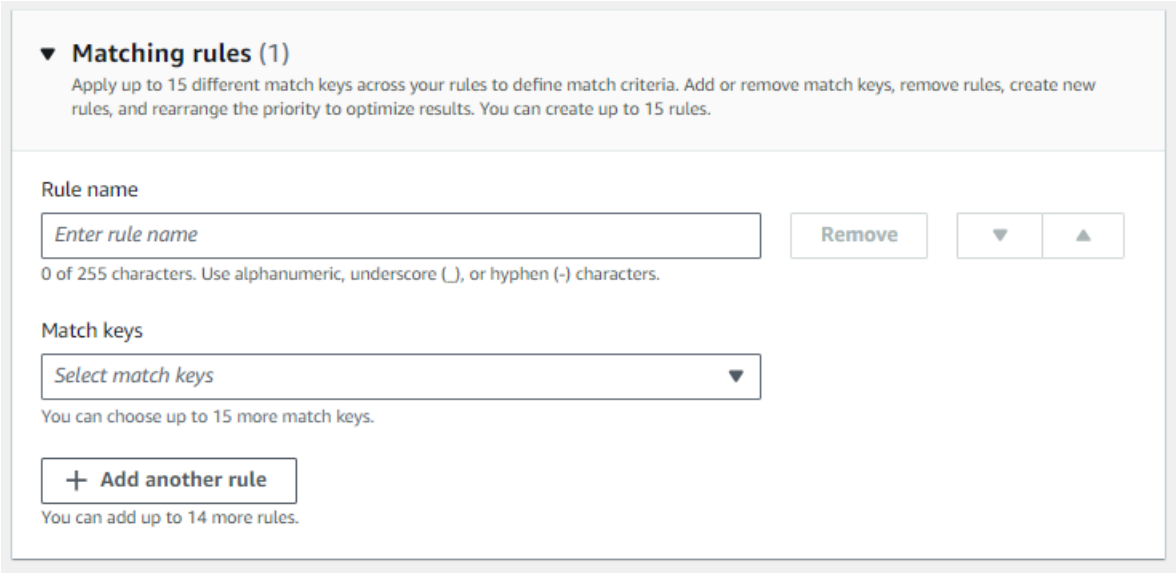
Se vuoi...	Allora scegli...
Esegui un flusso di lavoro su richiesta per un aggiornamento collettivo	Manuale
Esegui un flusso di lavoro non appena nuovi dati sono presenti nel tuo bucket S3	Automatica

> **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. Per le regole di abbinamento, inserisci il nome di una regola e poi scegli i tasti Match per quella regola.

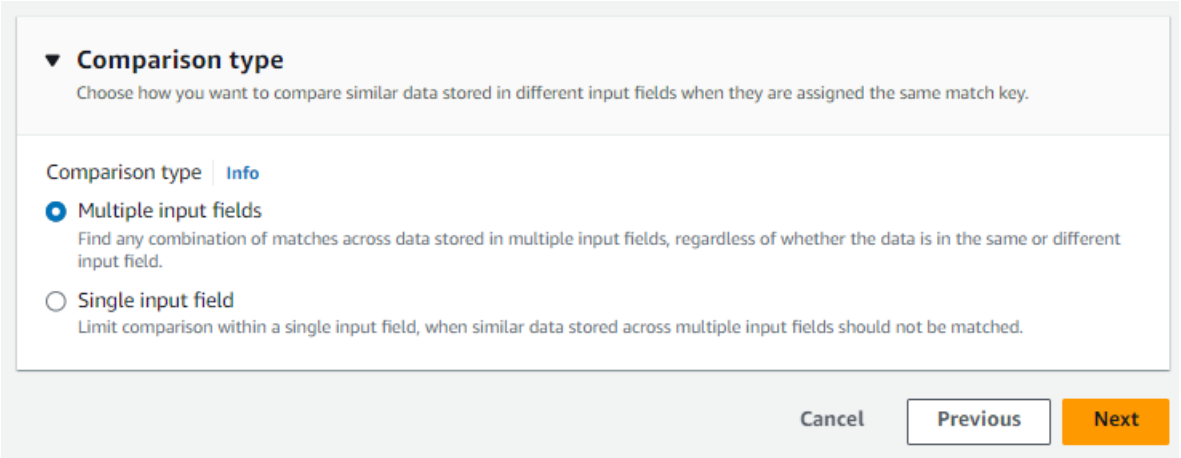
Puoi applicare fino a 15 chiavi di abbinamento diverse alle tue regole per definire i criteri di corrispondenza.

Puoi creare fino a 15 regole.



d. Per Tipo di confronto, scegli una delle seguenti opzioni.

Se vuoi...	Allora scegli...
Trova qualsiasi combinazione di corrispondenze tra i dati memorizzati in più campi di input	Confronto tra più campi di input
Limita il confronto a un singolo campo di input	Confronto tra campi di input singoli



e. Seleziona 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, visualizza tutti i campi inclusi.

   e. Determina se desideri includere, nascondere o mascherare i campi.

Se vuoi...	Allora scegli...
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.

   f. Seleziona 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.
   - Gli ID di corrispondenza univoci generati.
   - 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.

Ora sei pronto per:

- Modifica un flusso di lavoro corrispondente
- Elimina un flusso di lavoro corrispondente
- Eseguire un flusso di lavoro corrispondente

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

Il flusso di lavoro di abbinamento basato sull'apprendimento automatico consente di confrontare 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.

Per la corrispondenza basata sull'apprendimento automatico, applica la percentuale del livello di confidenza delle 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. Specificate le autorizzazioni di accesso al servizio selezionando Crea e utilizza un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

Se scegli...	THEN
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 chiave KMS e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati di input.

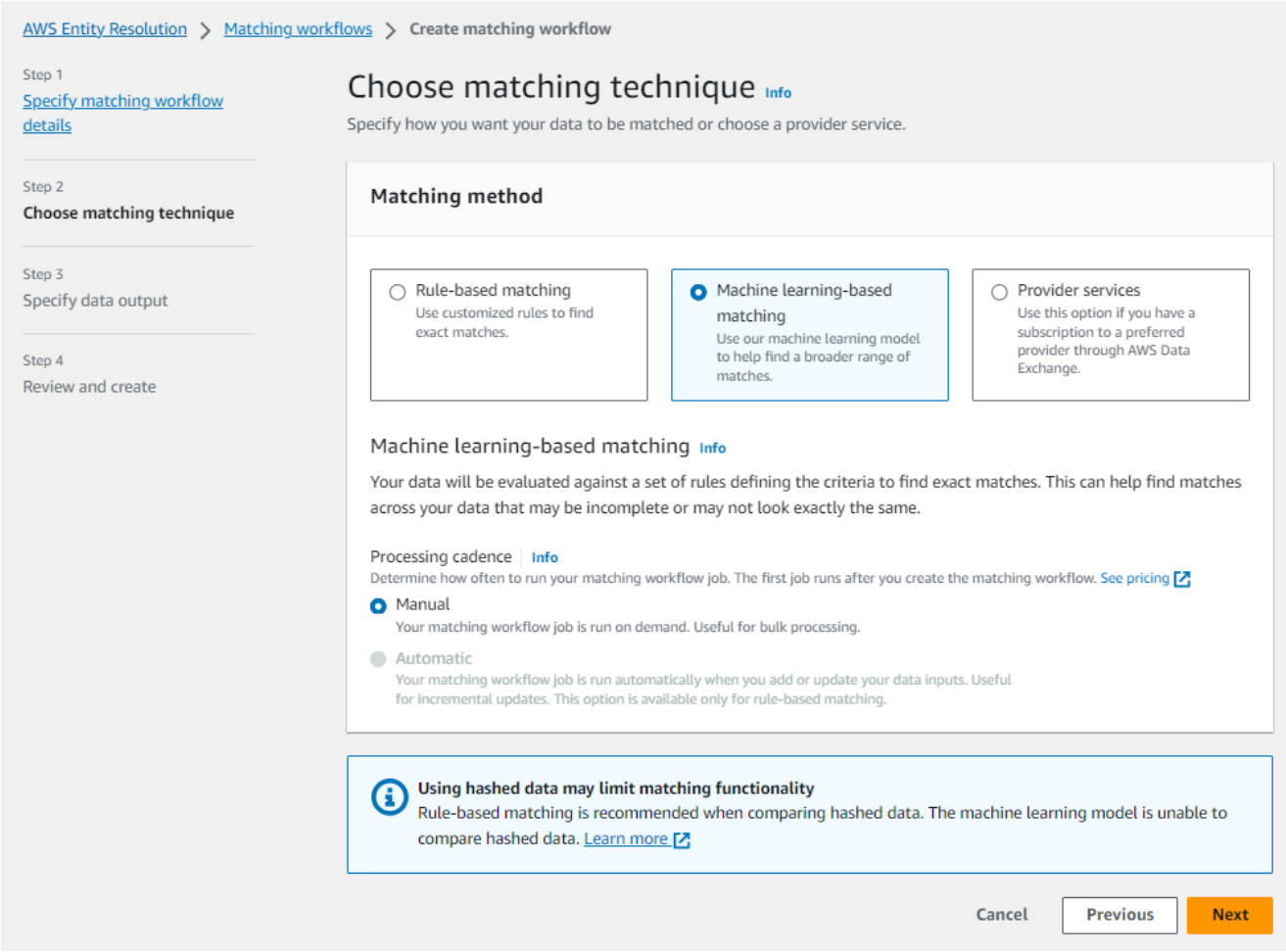
Se scegli...	THEN
Usa un ruolo di servizio esistente	1. Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. L'elenco dei ruoli viene visualizzato se si dispone delle autorizzazioni per elencare i ruoli. Se non disponi delle autorizza zioni per elencare i ruoli, puoi inserire l'Amazon 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 esterno View in IAM. 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. Seleziona Successivo.

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

   a. Per il metodo di abbinamento, scegli l'abbinamento basato 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. Seleziona 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, visualizza tutti i campi inclusi.

   e. Determina se desideri includere, nascondere o mascherare i campi.

Se vuoi...	Allora scegli...
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.

f. Seleziona 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.
   - Gli ID di corrispondenza univoci generati.
   - 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.

Ora sei pronto per:

- Modifica un flusso di lavoro corrispondente
- Elimina un flusso di lavoro corrispondente
- Eseguire un flusso di lavoro corrispondente

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

Se hai un abbonamento con un provider di servizi tramite AWS Data Exchange, puoi abbinare i tuoi identificatori noti al tuo provider preferito. AWS Entity Resolution attualmente supporta i seguenti servizi di provider di dati:

- LiveRamp
- TransUnion
- ID unificato 2.0

Per ulteriori informazioni sulla creazione di un nuovo abbonamento o sul riutilizzo di un abbonamento esistente a un servizio di un provider, consulta. Iscriviti a un provider di servizi 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
- Creare un flusso di lavoro corrispondente con TransUnion
- Creare un flusso di lavoro corrispondente con UID 2.0

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 uno degli ID più comunemente utilizzati nelle piattaforme lato domanda per creare un pubblico per una campagna pubblicitaria. Utilizzando un flusso di lavoro corrispondente con LiveRamp, puoi convertire gli indirizzi e-mail con hash in RAMPID.

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

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 ognuna <user input placeholder>con le tue informazioni.

secchio di allestimento	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. Specificate le autorizzazioni di accesso al servizio selezionando Crea e utilizza un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

Se scegli...	THEN
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 chiave KMS e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati di input.

Se scegli...	THEN
Usa 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 esterno View in IAM. 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. Seleziona Successivo.

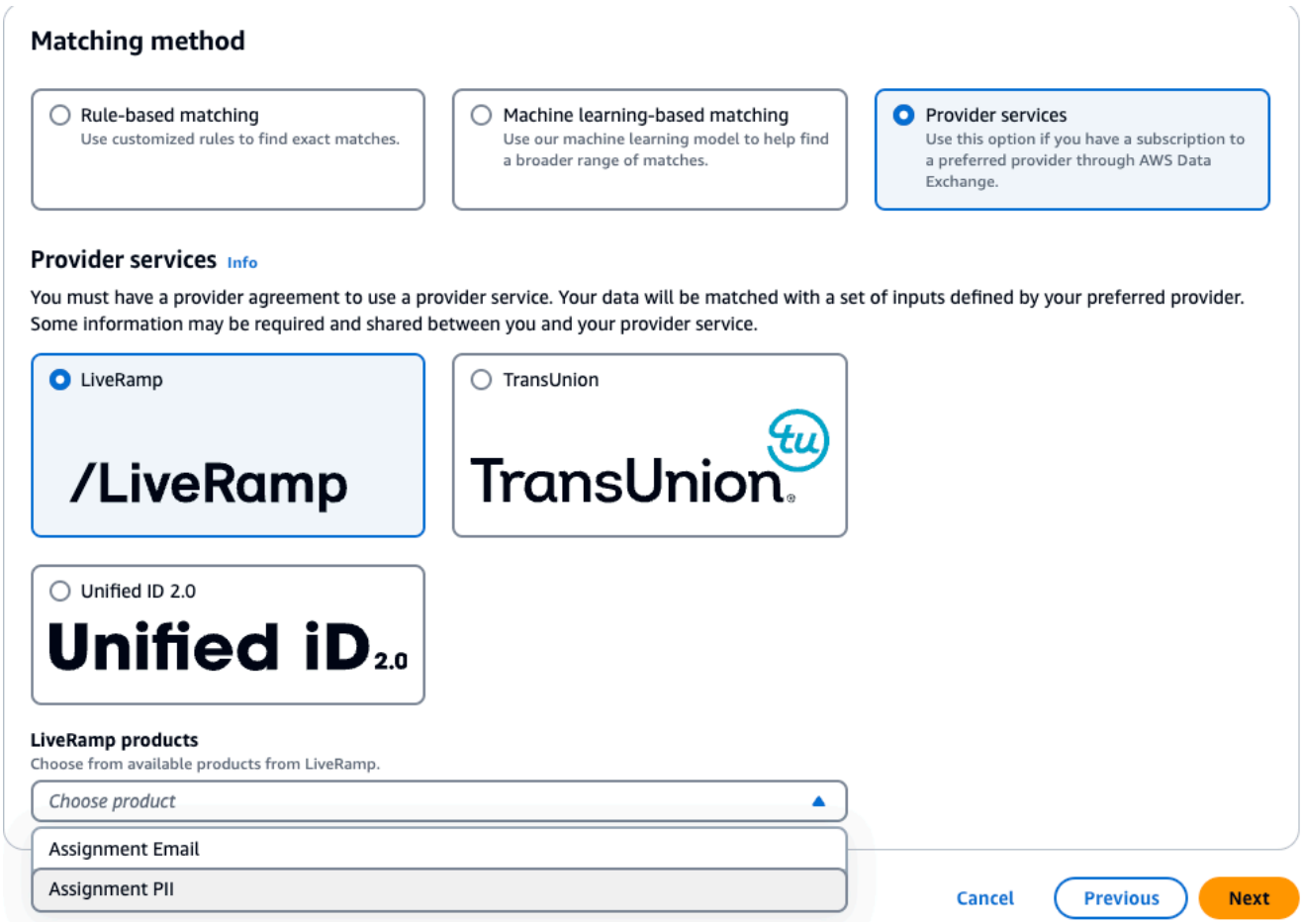
5. Per la fase 2: Scegli la tecnica di abbinamento:

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

   b. Per i servizi del fornitore, scegli LiveRamp.

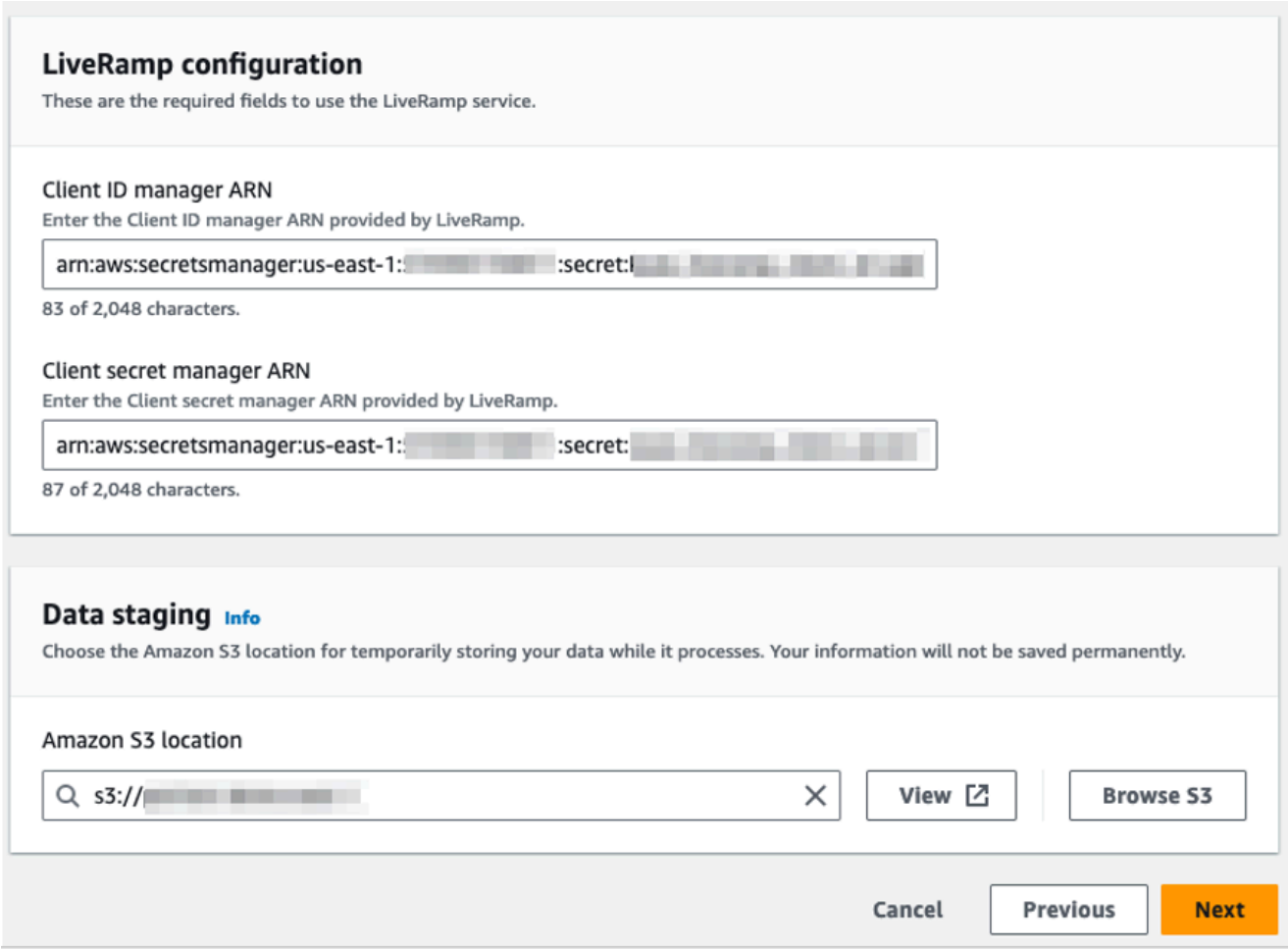
> **Note**
>
> Assicurati che il formato e la normalizzazione del file di input dei dati siano in linea con le linee guida del servizio del provider.
> Per ulteriori informazioni sulle linee guida per la formattazione dei file di input per il flusso di lavoro corrispondente, consulta Eseguire la risoluzione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

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



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

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



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 la posizione di data staging di Amazon S3. Per ulteriori informazioni, consulta la pagina the section called “Crea un ruolo lavorativo nel flusso di lavoro per AWS Entity Resolution”.

f. Seleziona 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.

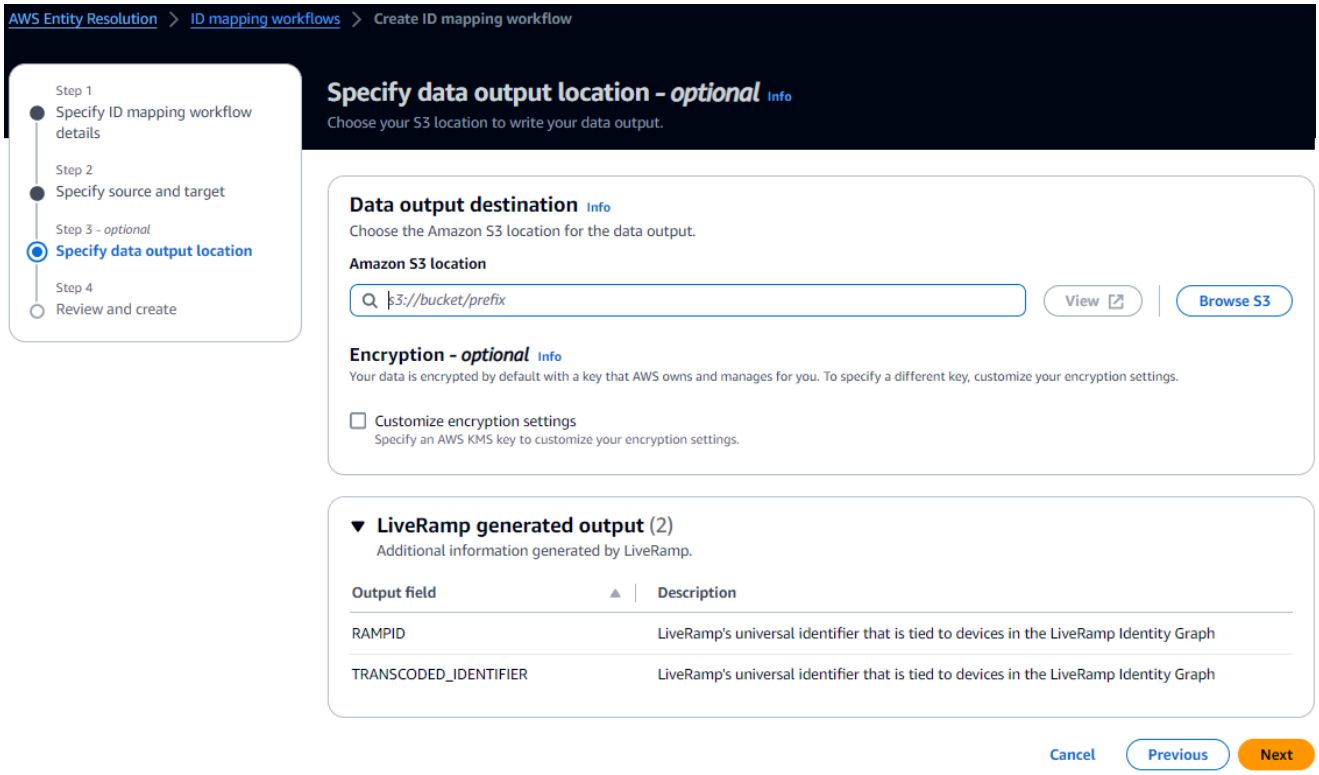
c. Visualizza l'output LiveRamp generato.

   Queste sono le informazioni aggiuntive generate da LiveRamp.

d. Per l'output dei dati, visualizza tutti i campi inclusi e determina se desideri includere, nascondere o mascherare i campi.

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

Se vuoi...	Allora scegli...
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. Seleziona 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.
   - Gli ID di corrispondenza univoci generati.

- 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.

Ora sei pronto per:

- Modifica un flusso di lavoro corrispondente
- Elimina un flusso di lavoro corrispondente

Creare 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 ID individuali e familiari. TransUnion TransUnionfornisce l'assegnazione degli 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 ognuna <user input placeholder>con le tue informazioni.

secchio di allestimento	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. Specificate le autorizzazioni di accesso al servizio selezionando Crea e utilizza un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

Se scegli...	THEN
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 chiave KMS e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati di input.

Se scegli...	THEN
Usa 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 esterno View in IAM. 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. Seleziona Successivo.

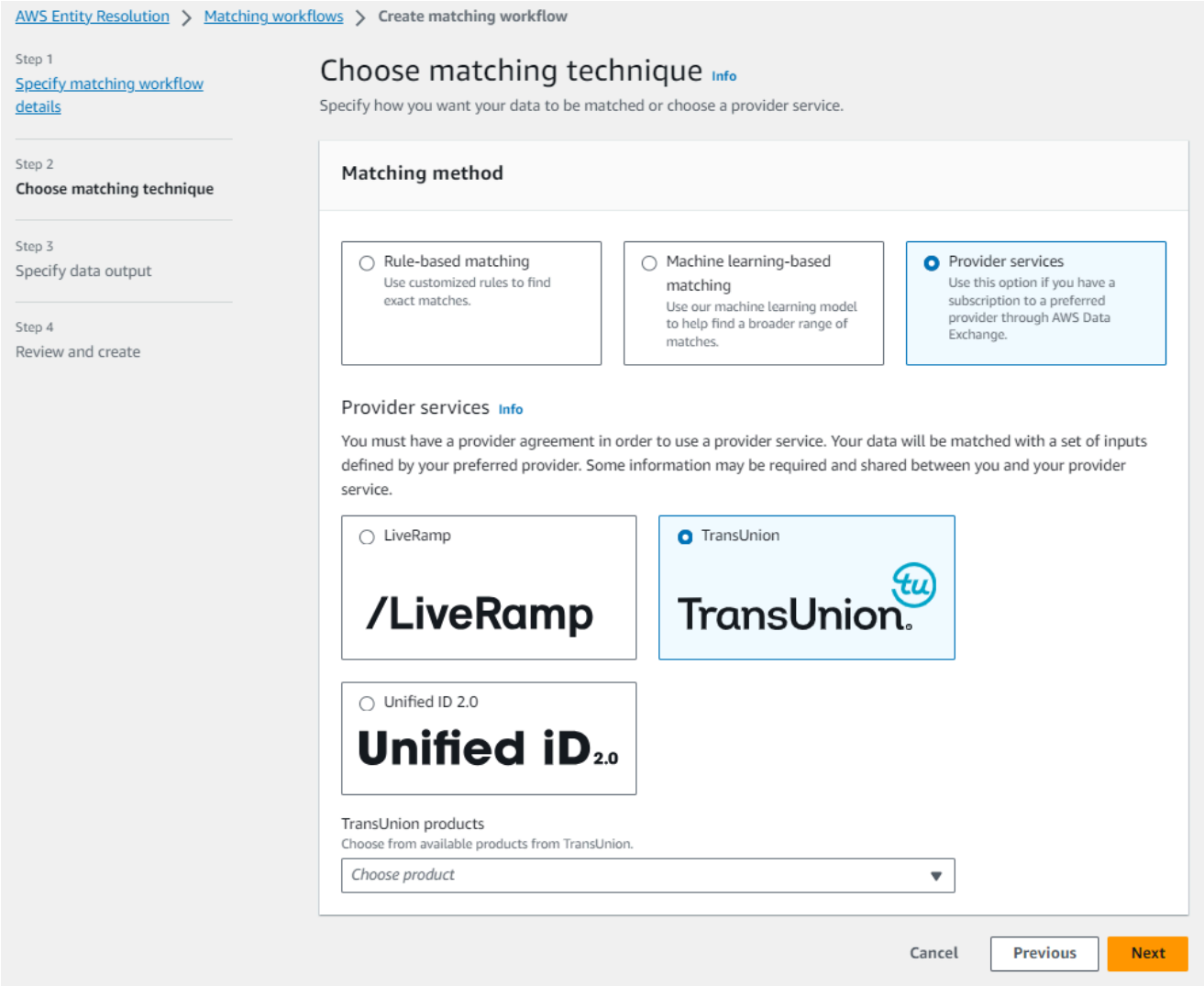
5. Per la fase 2: Scegli la tecnica di abbinamento:

   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.



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 la posizione di data staging di Amazon S3. Per ulteriori informazioni, consulta la pagina the section called “Crea un ruolo lavorativo nel flusso di lavoro per AWS Entity Resolution”.

6. Seleziona 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, visualizza tutti i campi inclusi e determina se desideri includere, nascondere o mascherare i campi.

Se vuoi...	Allora scegli...
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. Seleziona 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.
   - Gli ID di corrispondenza univoci generati.
   - 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.

Ora sei pronto per:

- Modifica un flusso di lavoro corrispondente
- Elimina un flusso di lavoro corrispondente

Creare un flusso di lavoro corrispondente con UID 2.0

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

Il servizio Unified ID 2.0 fornisce un UID 2 non elaborato, utilizzato per creare campagne pubblicitarie nella piattaforma The Trade Desk. L'UID 2.0 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 generazione di UID2 non elaborati, ma non entrambi. Se entrambi sono presenti nella mappatura dello schema, il flusso di lavoro selezionerà il campo **`Email Address`** e **`Phone number`** sarà un campo pass-through. Per supportare entrambi, crea una nuova mappatura dello schema in cui

`Phone number` è mappato ma non lo è. **`Email Address`** Quindi, crea un secondo flusso di lavoro utilizzando questa nuova mappatura dello schema.

> **Note**
>
> Gli UID2 grezzi vengono creati aggiungendo sali da secchi di sale che vengono ruotati all'incirca una volta all'anno, facendo ruotare anche l'UID2 grezzo con esso, quindi si consiglia di aggiornare gli UID2 grezzi ogni giorno. Per ulteriori informazioni, consulta how-often-should-uid https://unifiedid.com/docs/getting-started/gs-faqs # 2 -incremental-updates s-be-refreshed-for

Per creare un flusso di lavoro corrispondente con 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 UID 2.0.

      Per ulteriori informazioni sulla **`Phone number`** normalizzazione, consulta Normalizzazione dei numeri di telefono nella documentazione UID 2.0.
   d. Specificate le autorizzazioni di accesso al servizio selezionando Crea e utilizza un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

Se scegli...	THEN
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 chiave KMS e quindi inserire una AWS KMS chiave che verrà utilizzata per decrittografare i dati di input.

Se scegli...	THEN
Usa 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 esterno View in IAM. Per impostazione predefinita, AWS Entity Resolution non tenta di aggiornare la politica esistente sui ruoli per aggiunger e le autorizzazioni necessarie.

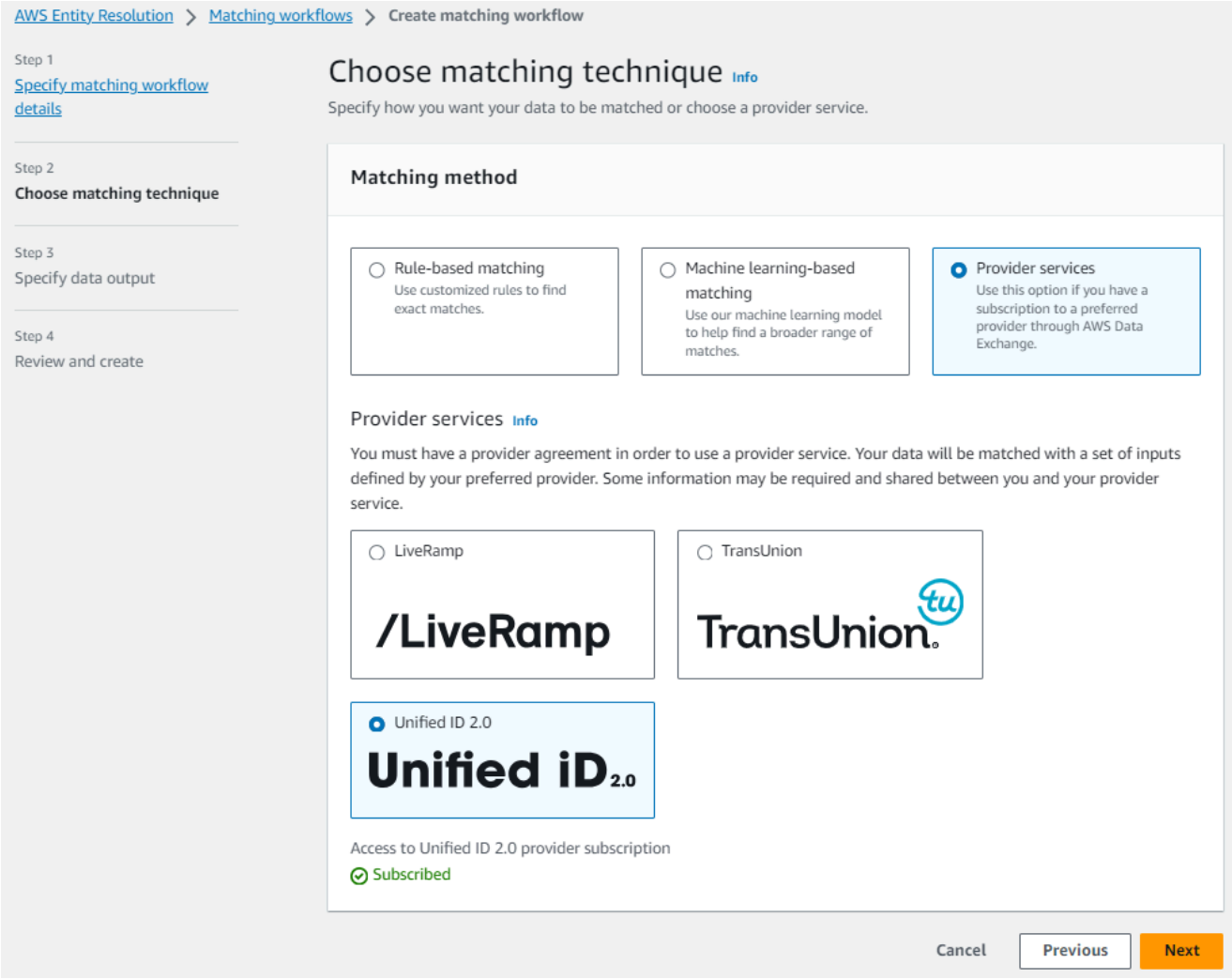
e. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

f. Seleziona 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.



c. Seleziona 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 UID 2.0

   d. Per l'output dei dati, visualizza tutti i campi inclusi e determina se desideri includere, nascondere o mascherare i campi.

Se vuoi...	Allora scegli...
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. Seleziona 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.
   - Gli ID di corrispondenza univoci generati.
   - 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.

Ora sei pronto per:

- Modifica un flusso di lavoro corrispondente
- Elimina un flusso di lavoro corrispondente

Eseguire un flusso di lavoro corrispondente

Dopo aver creato un flusso di lavoro di abbinamento basato su regole o sull'apprendimento automatico con il tipo di elaborazione manuale, puoi eseguire un processo di abbinamento corrispondente.

> **Note**
>
> Se crei un flusso di lavoro corrispondente con il tipo di elaborazione automatica, i processi del flusso di lavoro corrispondenti verranno eseguiti ogni volta che viene aggiornato un input di dati.

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 ID di corrispondenza ai record nel set di dati corrispondente.

- Se hai specificato la tecnica di abbinamento basata su regole, AWS Entity Resolution assegnerà anche il numero di regola applicato che ha generato la corrispondenza.
- Se hai specificato la tecnica di abbinamento basata sull'apprendimento automatico, AWS Entity Resolution assegnerà anche la percentuale del livello di confidenza della partita.

AWS Entity Resolution quindi scrive i file di output dei dati in una posizione scelta dall'utente.

Un flusso di lavoro 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 conterrà più file, ciascuno contenente un sottoinsieme dei record di successo. 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 dei flussi di lavoro.

Per eseguire 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 Esegui flusso di lavoro.

   Viene visualizzato un messaggio che indica che il processo è iniziato.
5. Nella scheda Metriche, in Cronologia lavori, visualizza quanto segue:
   - Lo stato del processo del flusso di lavoro corrispondente: In corso, Completato, Non riuscito
   - Il numero di record elaborati.
   - Il numero di corrispondenze trovate.
   - Il numero di record univoci.
   - La durata del lavoro.
   - Il Job ID.
6. 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.

Passaggi successivi

Ora sei pronto per:

- Modifica un flusso di lavoro corrispondente
- Elimina un flusso di lavoro corrispondente

Creazione di un namespace ID

Un namespace ID è un involucro attorno alla tabella di dati che viene utilizzato per fornire metadati che spiegano i dati 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.

I seguenti argomenti ti guidano attraverso una serie di passaggi per creare i namespace ID di origine e di destinazione e quindi specificare l'output dei dati in Amazon Simple Storage Service (Amazon S3).

> **Note**
>
> AWS Entity Resolution attualmente offre la LiveRamp transcodifica per il metodo dello spazio dei nomi ID quando crei uno spazio dei nomi ID.

Argomenti

Crea una fonte di namespace ID

Questo argomento descrive il processo di creazione di un'origine dello spazio dei nomi ID sulla console.AWS Entity Resolution Questa è l'origine dei dati in un flusso di lavoro di mappatura degli ID.

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

Per creare una fonte di namespace 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. 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. Visualizzate il metodo dello spazio dei nomi ID.

   > **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 abbonarsi LiveRamp, consultaIscriviti a un provider di servizi 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 Crea e utilizza un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

Se scegli...	THEN
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 chiave KMS. Quindi, inserisci una AWS KMS chiave che viene utilizzata per decrittografare i dati in ingresso.

Se scegli...	THEN
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.

Crea un target di namespace ID

Questo argomento descrive il processo di creazione di un target di namespace ID sulla console.AWS Entity Resolution Questa è la destinazione dei dati in un flusso di lavoro di mappatura degli ID. Tutte le fonti raggiungono la destinazione.

Per creare un target ID namespace

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. Visualizza il metodo dello spazio dei nomi ID.

   > **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 abbonarsi LiveRamp, consultaIscriviti a un provider di servizi 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.

Dopo aver creato i namespace degli ID necessari per un flusso di lavoro di mappatura degli ID su due Account AWS, sei pronto per creare il flusso di lavoro di mappatura degli ID.

Creazione di un flusso di lavoro di mappatura degli ID

Il flusso di lavoro di mappatura degli ID 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 RAMPID di origine in qualsiasi RAMPID di destinazione. Utilizzando RAMpid come token per rappresentare i vostri clienti, potete evitare di condividere i dati dei clienti direttamente con le piattaforme pubblicitarie.

È possibile eseguire la mappatura degli ID tra due set di dati da soli Account AWS o tra due diversi. Account AWS L'origine e la destinazione di input dei dati dipendono dal tipo di mappatura degli ID che si desidera eseguire.

Per ulteriori informazioni, consulta Eseguire la traduzione tramite ADX nel sito Web della LiveRamp documentazione.

Argomenti

Prerequisito

Questo flusso di lavoro di mappatura degli ID richiede 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. Prima di creare un flusso di lavoro di mappatura degli ID con LiveRamp, 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>/*"
            ]
        }
    ]
}
```

<user input placeholder>Nella precedente politica di autorizzazione, sostituisci ciascuna 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.

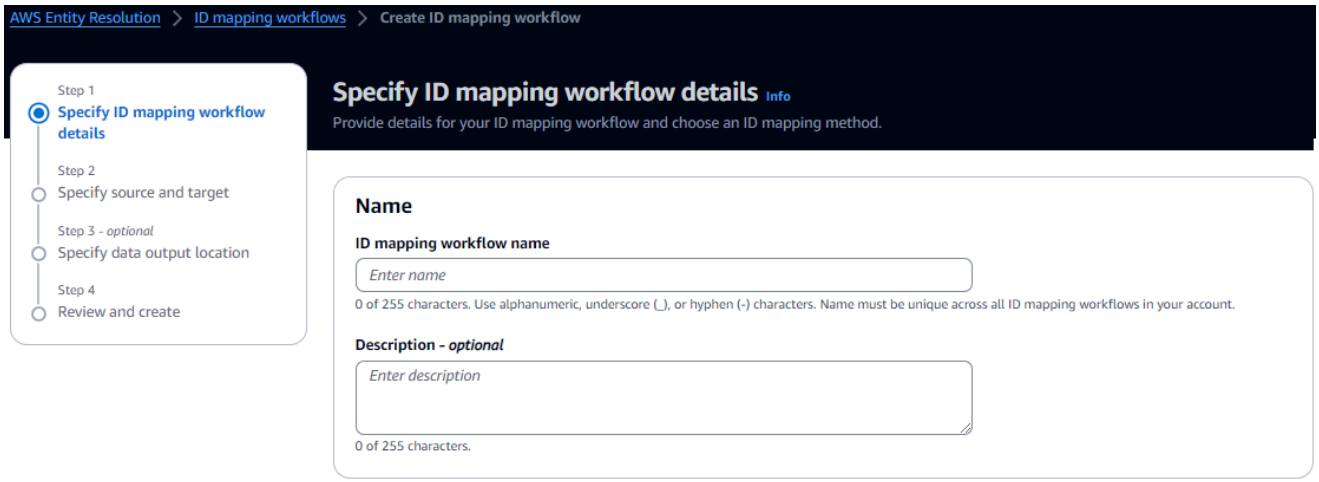
Creazione di un flusso di lavoro di mappatura degli ID per uno Account AWS

Dopo aver completato i passaggi di configurazione e creato una mappatura dello schema, puoi creare uno o più flussi di lavoro di mappatura degli ID per tradurre un set di RAMPID di origine in un altro utilizzando RAMPID gestiti o derivati.

Per creare un flusso di lavoro di mappatura degli ID per uno Account AWS

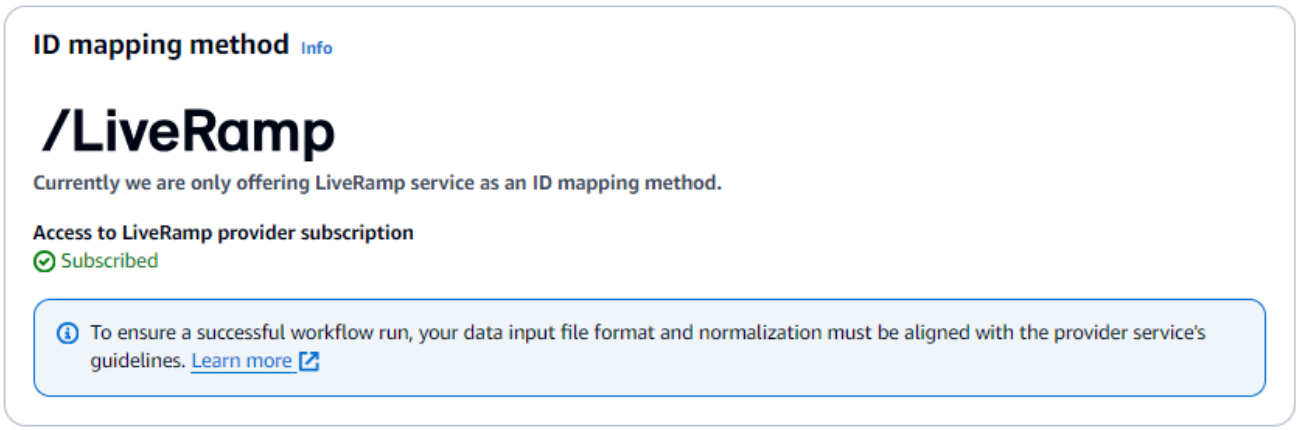
1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Nella pagina Flussi di lavoro di mappatura degli ID, nell'angolo in alto a destra,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

    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, consultaIscriviti a un provider di servizi su AWS Data Exchange.



> **Note**
>
> Assicurati che il formato del file di input dei dati sia in linea con le linee guida del servizio del provider. Per ulteriori informazioni sulle linee guida per LiveRamp la formattazione dei file di input, consulta Eseguire la traduzione tramite ADX nel sito Web della LiveRamp documentazione.

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

- ARN del gestore di ID client
- ARN, gestore segreto del cliente

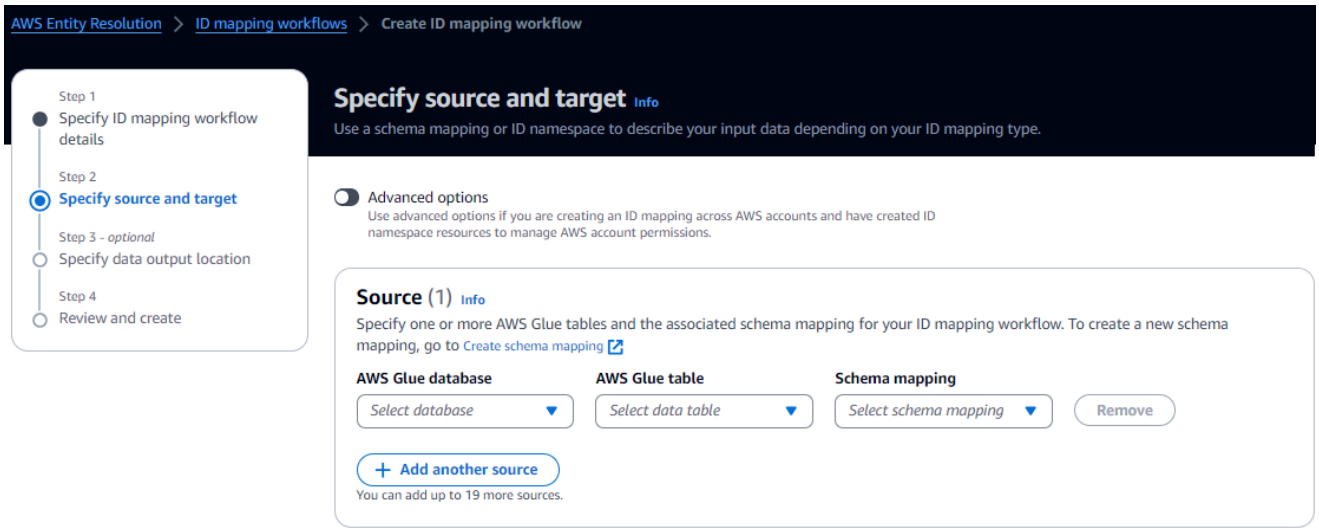
d. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

e. Seleziona Successivo.

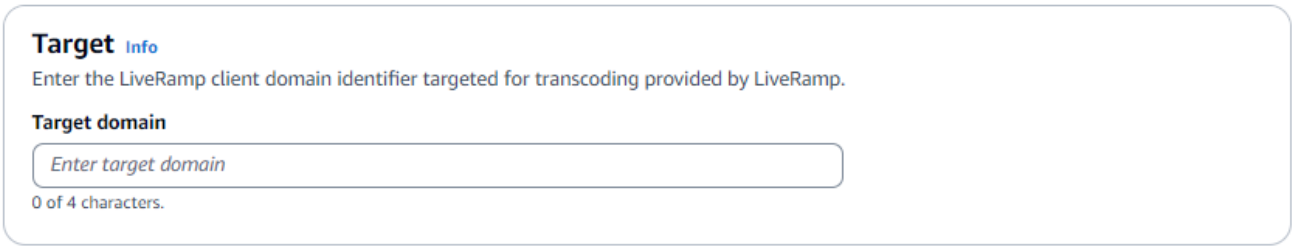
5. Per il passaggio 2: Specificate l'origine e la destinazione, effettuate le seguenti operazioni:

a. Per Origine, seleziona un AWS Gluedatabase dal menu a discesa, seleziona la AWS Glue tabella, quindi seleziona la mappatura dello schema corrispondente.

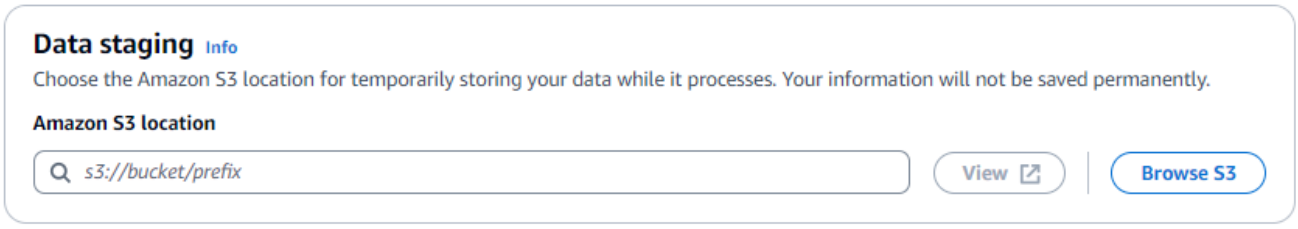
   È possibile aggiungere fino a 19 input di dati.



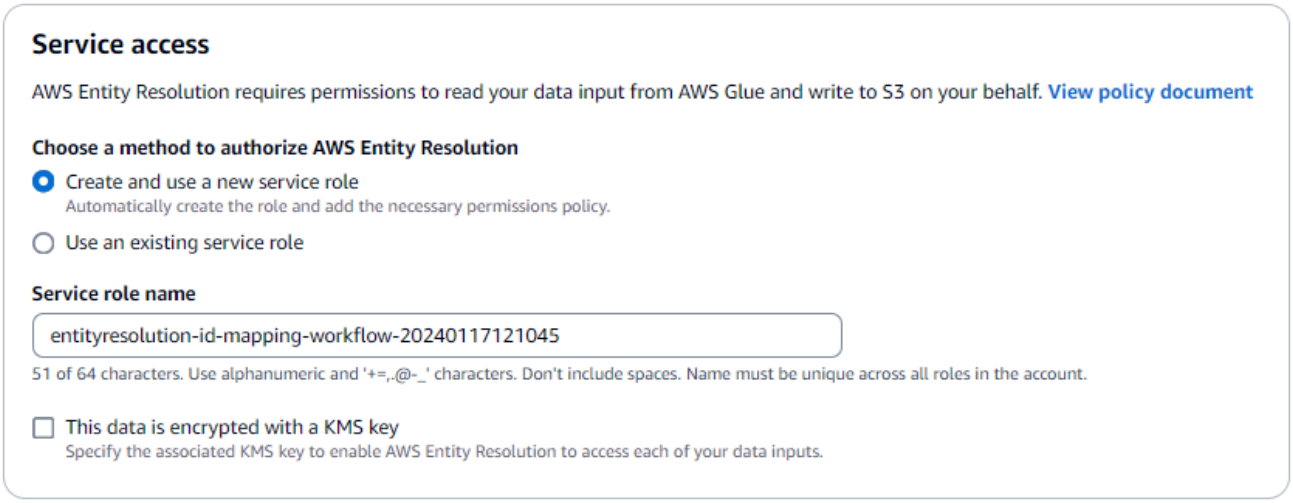
b. Per Target, inserisci l'identificatore del dominio LiveRamp del client destinato alla transcodifica che fornisce. LiveRamp



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.



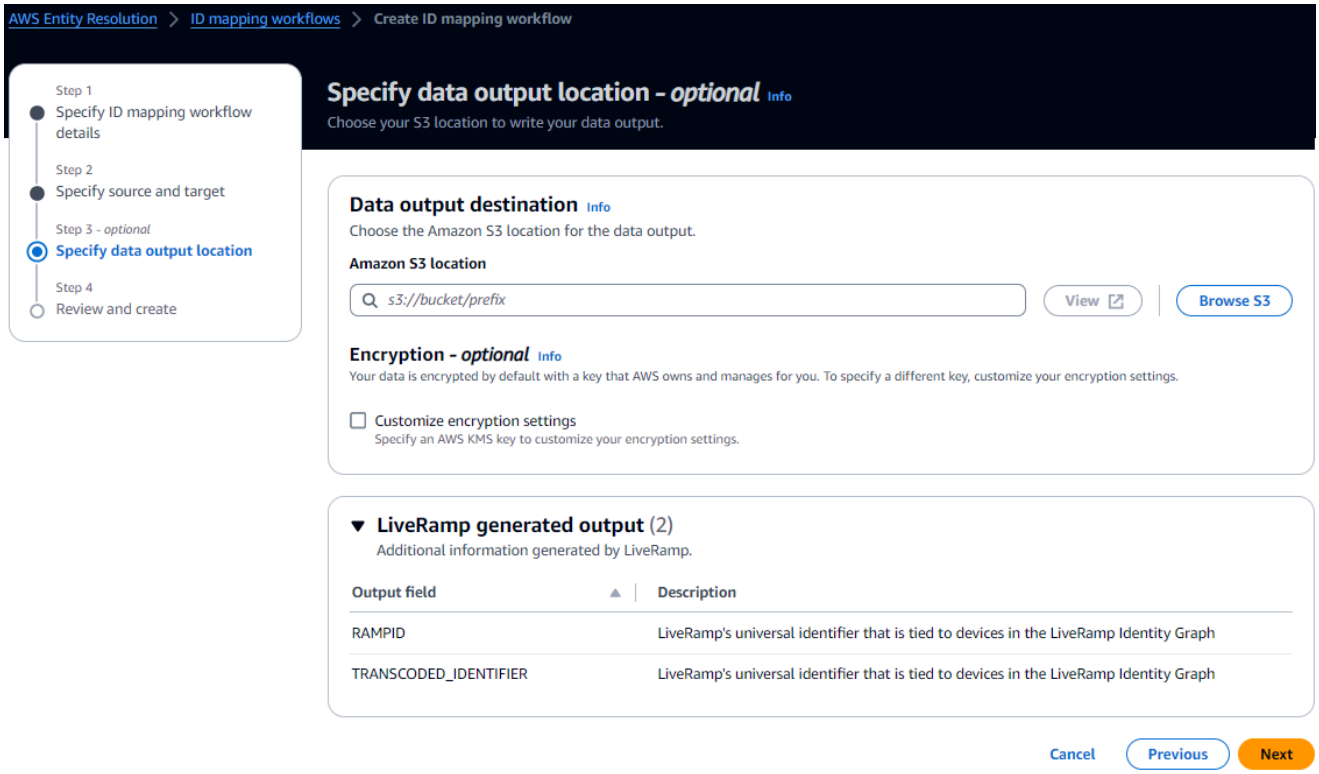
d. Per specificare le autorizzazioni di accesso al servizio, scegli Crea e usa un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.



Se scegli...	THEN
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 chiave KMS. Quindi, inserisci una AWS KMS chiave che viene utilizzata per decrittografare i dati in ingresso.

Se scegli...	THEN
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. Seleziona 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 l'ARN della AWS KMS chiave o scegli Crea una AWS KMS chiave.
   b. Visualizza l'output LiveRamp generato.
   c. Seleziona 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 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 su due Account AWS

Prerequisito

La creazione di un flusso di lavoro di mappatura degli ID su due Account AWS richiede l'autorizzazione per accedere LiveRamp al bucket S3 e alla AWS Key Management Service (AWS KMS) chiave gestita dal cliente. 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"
            }
        }
    }]
}
```

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

<KMSKeyARN>	L'ARN di una chiave gestita AWS KMS dal cliente.

Crea un flusso di lavoro di mappatura degli ID

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

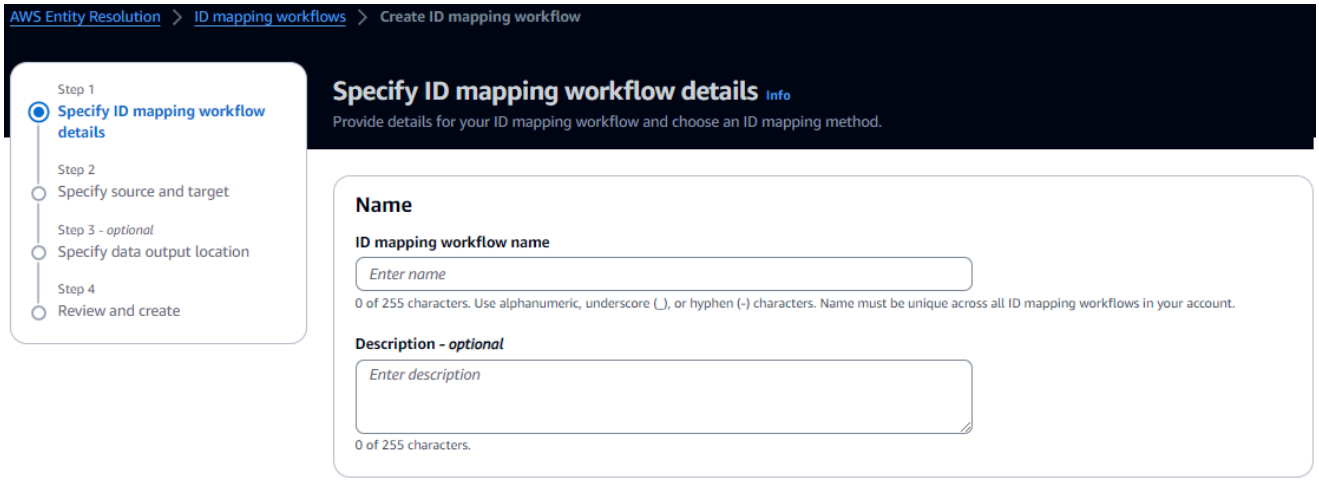
- Completa il prerequisito per aggiungere le autorizzazioni alla chiave gestita dal cliente.
- Completare le operazioni descritte in Configurazione AWS Entity Resolution.
- Crea una fonte di namespace ID.
- Crea un target ID namespace.

Dopo aver completato le attività elencate in precedenza, è possibile creare uno o più flussi di lavoro di mappatura degli ID per tradurre un set di RAMPID di origine in un altro utilizzando RAMPID gestiti o derivati.

Per creare un flusso di lavoro di mappatura degli ID tra due Account AWS

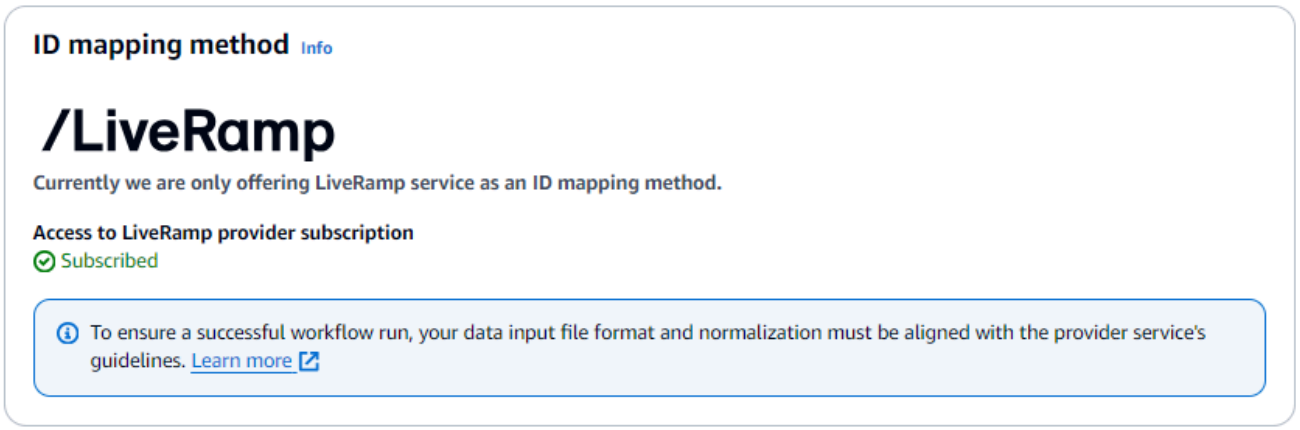
1. Accedi a AWS Management Console e apri la AWS Entity Resolution console con il tuo Account AWS, se non l'hai ancora fatto.
2. Nel riquadro di navigazione a sinistra, in Flussi di lavoro, scegli Mappatura degli ID.
3. Nella pagina Flussi di lavoro di mappatura degli ID, nell'angolo in alto a destra,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

    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, consultaIscriviti a un provider di servizi su AWS Data Exchange.



> **Note**
>
> Assicurati che il formato del file di input dei dati sia in linea con le linee guida del servizio del provider. Per ulteriori informazioni sulle linee guida per LiveRamp la formattazione dei file di input, consulta Eseguire la traduzione tramite ADX nel sito Web della LiveRamp documentazione.

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

- ARN del gestore di ID client
- ARN, gestore segreto del cliente

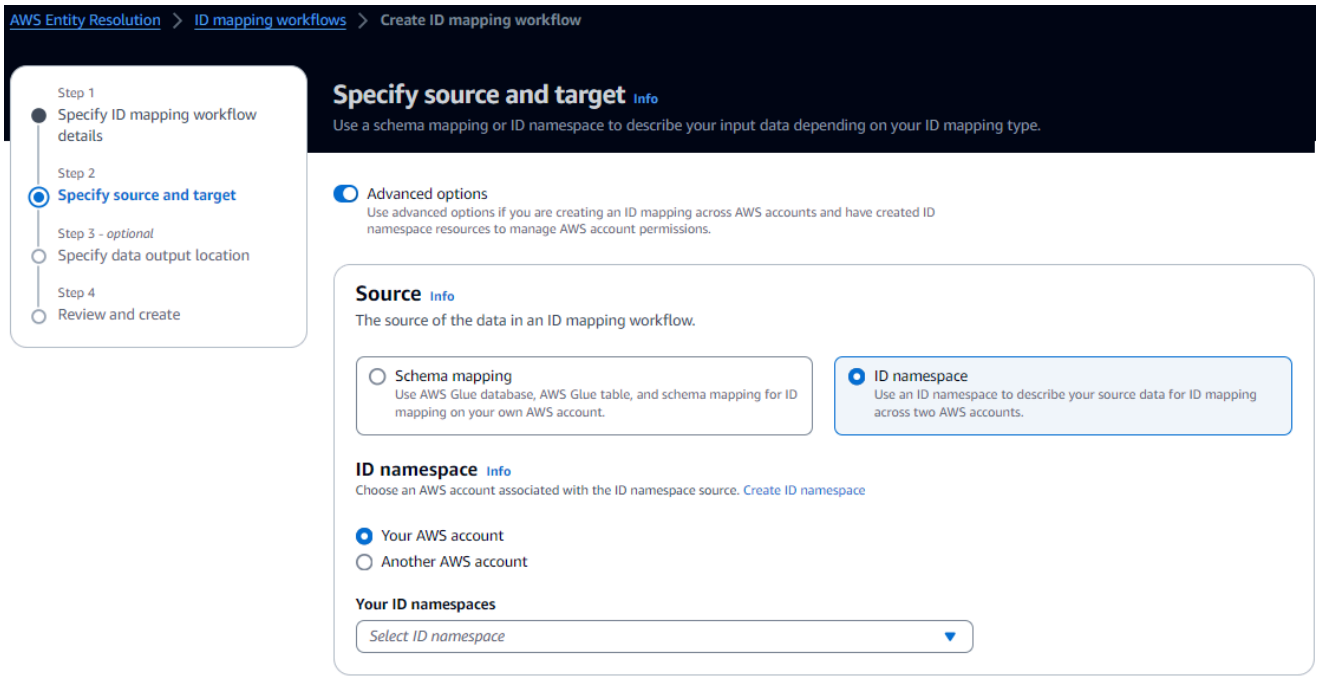
d. (Facoltativo) Per abilitare i tag per la risorsa, scegliete Aggiungi nuovo tag, quindi immettete la coppia Chiave e Valore.

e. Seleziona Successivo.

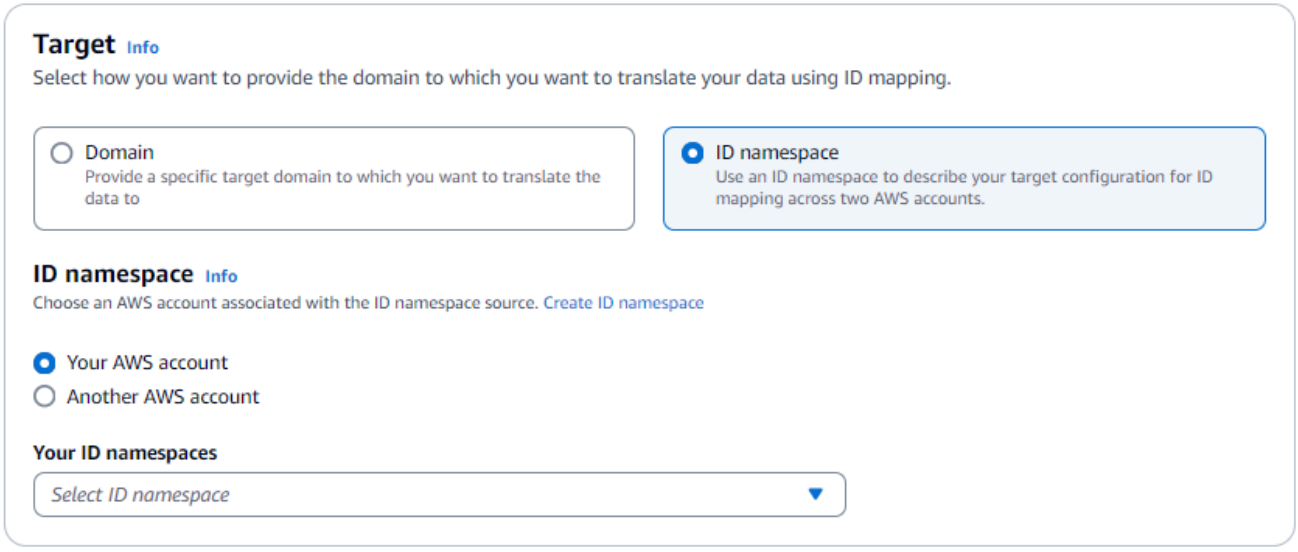
5. Per il passaggio 2: Specificate l'origine e la destinazione, effettuate le seguenti operazioni:

a. Attiva le opzioni avanzate.

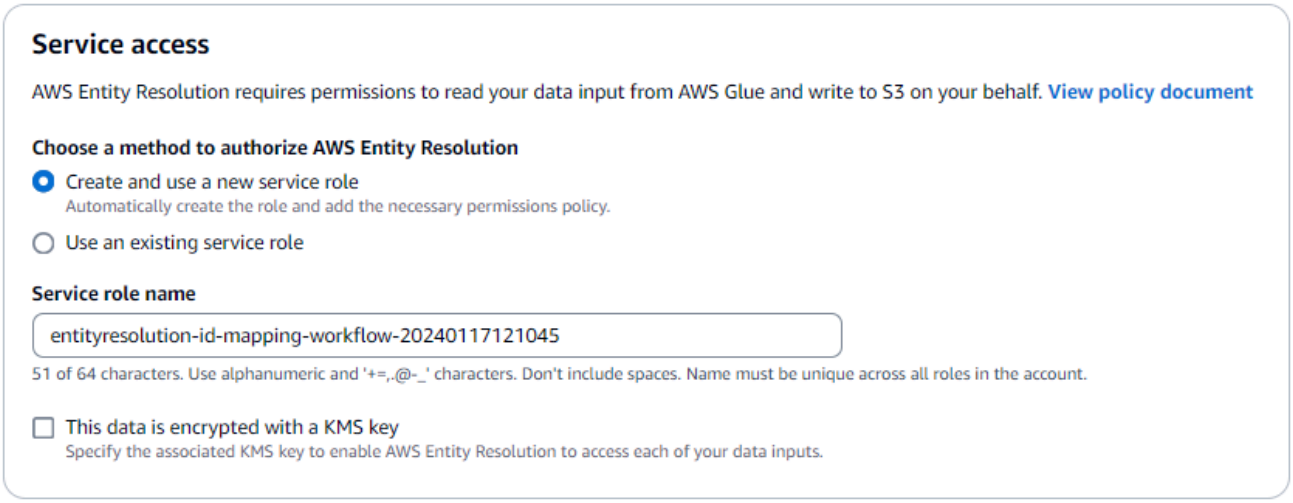
b. Per Source, scegli ID namespace.



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



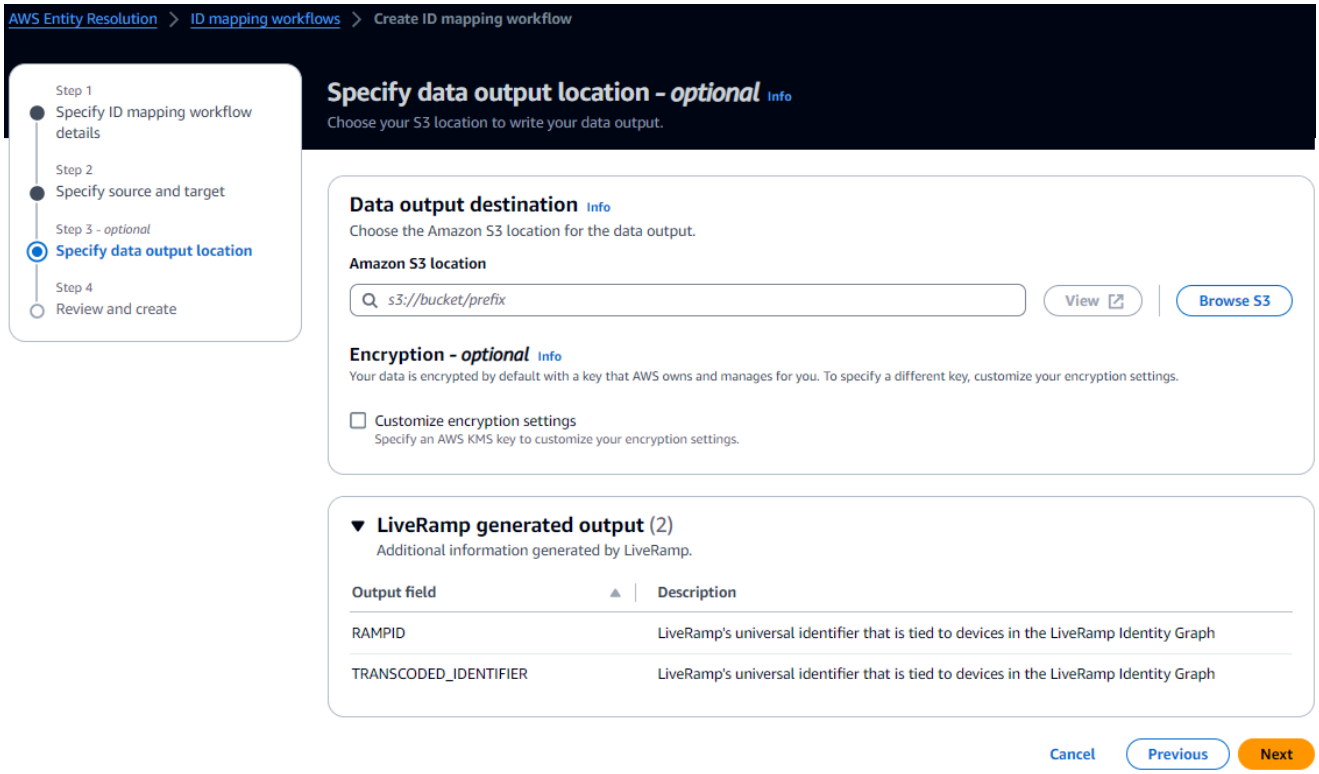
d. Per specificare le autorizzazioni di accesso al servizio, scegli Crea e utilizza un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.



Se scegli...	THEN
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 chiave KMS. Quindi, inserisci una AWS KMS chiave che viene utilizzata per decrittografare i dati in ingresso.

Se scegli...	THEN
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. Seleziona 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 l'ARN della AWS KMS chiave o scegli Crea una AWS KMS chiave.
   b. Visualizza l'output LiveRamp generato.
   c. Seleziona 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 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.

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 ottenuto il file CSV, 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 l'ARN della AWS KMS chiave o scegli Crea una AWS KMS chiave.
6. Per specificare le autorizzazioni di accesso al servizio, scegli Crea e usa un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

Se scegli...	THEN
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 chiave KMS. Quindi, inserisci una AWS KMS

Se scegli...	THEN
	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 ottenuto il file CSV, puoi unirti a. `RAMPID TRANSCODED_ID`

Gestire AWS Entity Resolution

I seguenti argomenti spiegano come gestire i flussi di lavoro utilizzando la console. AWS Entity Resolution

Per informazioni su come gestire l' AWS Entity Resolution utilizzo degli AWS SDK, consulta l'AWS Entity Resolution API Reference.

Argomenti

Gestione delle mappature degli schemi

I seguenti argomenti spiegano come gestire le mappature dello schema utilizzando la console. AWS Entity Resolution

Argomenti

Clonare 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 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.

Eliminare 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.

Gestione dei flussi di lavoro corrispondenti

Dopo aver creato un flusso di lavoro di abbinamento basato su regole, un abbinamento basato sull'apprendimento automatico o un flusso di lavoro di abbinamento basato sui servizi del fornitore, puoi gestire i flussi di lavoro di abbinamento nei seguenti modi.

Argomenti

- Modifica un flusso di lavoro corrispondente
- Elimina un flusso di lavoro corrispondente
- Trova un Match ID per un flusso di lavoro di abbinamento basato su regole
- Elimina i record da un flusso di lavoro di abbinamento basato su regole o ML

Modifica 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.

Elimina 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.

Trova 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.

Elimina i 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 ID univoci dall'elenco a discesa Azioni.
5. Inserisci l'ID univoco che desideri eliminare nella sezione ID univoci.

   Puoi inserire fino a 10 ID univoci.
6. Specificare la sorgente di input da cui eliminare gli ID univoci.

   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, gli ID univoci delle altre fonti di input non subiranno alcuna modifica.
7. Scegli Elimina ID univoci.

Gestione dei namespace degli ID

Puoi gestire i namespace degli ID nei seguenti modi.

Argomenti

- Modifica uno spazio dei nomi ID
- Elimina uno spazio dei nomi ID
- Aggiungi o aggiorna una politica delle risorse

Modifica uno spazio dei nomi ID

È possibile 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.

Elimina uno spazio dei nomi ID

Non è possibile 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.

Aggiungi o aggiorna una politica delle risorse

Una politica delle risorse consente al creatore della risorsa di mappatura degli ID di accedere alla risorsa del namespace 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'editor JSON.
7. Seleziona Salvataggio delle modifiche.

Gestione dei flussi di lavoro di mappatura degli ID

Puoi gestire i flussi di lavoro di mappatura degli ID nei seguenti modi.

Argomenti

Modifica 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.

Eliminare 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.

Aggiungi o aggiorna una politica delle risorse

Una politica delle risorse consente al creatore della risorsa di mappatura degli ID di accedere alla risorsa del namespace 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'editor JSON.
7. Seleziona Salvataggio delle modifiche.

Risoluzione dei problemi dei flussi di lavoro

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

Ho ricevuto un file di errore.

I record nel file di errore possono essere creati 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
- Uno dei campi della mappatura dello schema include un nome riservato:
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - ID partita
  - HashingProtocol
  - ConfidenceLevel
  - Origine

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.

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 Servizi AWS 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 Servizio AWS 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 Servizi AWS 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 Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or 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.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- 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 moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

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 o Servizi AWS utilizzi la console, l'API AWS Entity Resolution o gli SDK. AWS CLI AWS 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. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al 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.

Chiavi di proprietà di AWS: AWS Entity Resolution utilizza queste chiavi per impostazione predefinita per crittografare automaticamente i dati di identificazione personale. Non puoi visualizzare, gestire o utilizzare chiavi AWS di proprietà o verificarne l'utilizzo. Tuttavia, non è necessario intraprendere alcuna azione per proteggere le chiavi che crittografano i dati. Per ulteriori informazioni, consulta le chiavi di proprietà di AWS nella AWS Key Management Service Developer Guide.

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 chiave KMS gestita dal cliente per la crittografia quando crei la risorsa di flusso di lavoro corrispondente.

Chiavi gestite dal cliente: AWS Entity Resolution supporta l'uso di una chiave KMS 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 le policy e le sovvenzioni IAM
- 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 la chiave gestita dal cliente nella Guida per gli AWS Key Management Service sviluppatori.

Per ulteriori informazioni su AWS KMS, consulta What is AWS Key Management Service?

Gestione delle chiavi

In che modo 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

chiave KMS in un account cliente. AWS Entity Resolution richiede la concessione per utilizzare la 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 le AWS Management Console, o le AWS KMS API.

Per creare una chiave simmetrica gestita dal cliente

AWS Entity Resolution supporta la crittografia utilizzando chiavi KMS di crittografia simmetrica. 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 policy chiave devono essere consentite le seguenti operazioni API:

- `kms:DescribeKey`— Fornisce informazioni quali l'ARN della chiave, 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, ad esempio`KeySpec`, aiutano a distinguere

diversi tipi di chiavi KMS. Visualizza anche l'utilizzo delle chiavi (crittografia, firma o generazione e verifica di MAC) e gli algoritmi supportati dalla chiave KMS. AWS Entity Resolution convalida che è ed è. `KeySpec` `SYMMETRIC_DEFAULT` `KeyUsage` `ENCRYPT_DECRYPT`

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

questa chiave KMS per crittografare o decrittografare le risorse. È necessario concedere agli utenti il permesso di eseguire le seguenti azioni per utilizzare la crittografia a chiave KMS gestita 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'entità IAM che effettua la `CreateMatchingWorkflow` richiesta con una chiave KMS gestita dal cliente disponga delle `kms:DescribeKey` autorizzazioni sulla politica della chiave KMS.

Durante una `StartIdMappingJob`richiesta `CreateIdMappingWorkflow`e, AWS Entity Resolution invierà una richiesta DescribeKeye una a per CreateGranttuo AWS KMS conto. Ciò richiederà che l'entità IAM che effettua la `StartIdMappingJob` richiesta `CreateIdMappingWorkflow` e con una chiave KMS gestita dal cliente disponga `kms:DescribeKey` delle autorizzazioni relative alla politica della chiave KMS. 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 di essi <user input placeholder>con le tue informazioni.

<KMSKeyARN>	AWS KMS Nome della risorsa Amazon.

Analogamente, l'entità IAM che richiama l'`StartMatchingJob`API deve disporre `kms:Decrypt` `kms:GenerateDataKey` delle autorizzazioni sulla chiave KMS gestita dal cliente fornite nel flusso di lavoro corrispondente.

Per ulteriori informazioni sulla specificazione delle autorizzazioni in una policy, 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 memorizzati dalla risorsa.

KMSarn — Inserisci una chiave ARN, che è un identificatore chiave per una chiave gestita dal cliente. AWS KMS

Puoi specificare una chiave gestita dal cliente come crittografia di secondo livello per le seguenti risorse se stai creando o eseguendo un flusso di lavoro di mappatura degli ID su due: Account AWS

Flusso di lavoro di mappatura degli ID o Avvia 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 — Inserisci una chiave ARN, 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 CloudTrail o Amazon 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 chiave KMS del 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 chiave KMS gestita dal cliente. In questi casi, puoi creare un nuovo flusso di lavoro con la chiave KMS gestita dal cliente.

Ulteriori informazioni

Le seguenti risorse forniscono ulteriori informazioni sulla crittografia dei dati a riposo.

Per ulteriori informazioni sui concetti di base di AWS Key Management Service, consulta la AWS Key Management Service Developer Guide.

Per ulteriori informazioni sulle best practice di sicurezza per AWS Key Management Service, consulta la AWS Key Management Service Developer Guide.

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 Servizi AWS 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 software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Entity Resolution IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

> **Note**
>
> AWS Entity Resolution supporta le politiche relative a più account. Per ulteriori informazioni, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS Entity Resolution svolgi.

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. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS Entity Resolution, consultaCome AWS Entity Resolution funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS Entity Resolution. Per visualizzare esempi di policy AWS Entity Resolution basate sull'identità che puoi utilizzare in IAM, 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. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi 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 (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. 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 Signing AWS API request nella IAM User Guide.

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'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS 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 un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

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 Servizi AWS 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 Servizi AWS 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 ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM 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, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

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 utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM 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 ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per

conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale 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 diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS 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 amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole 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 documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON 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 operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente 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 nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket 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. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

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 delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo 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 IAM nella Guida per l'utente IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON 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 in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

- 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 Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS Entity Resolution funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Entity Resolution, scopri con quali funzionalità IAM è disponibile l'uso AWS Entity Resolution.

Funzionalità IAM che puoi utilizzare con AWS Entity Resolution

Funzionalità IAM	AWS Entity Resolution supporto
Policy basate su identità	Sì
Policy basate su risorse	Sì
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì

Funzionalità IAM	AWS Entity Resolution supporto
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	No

Per avere una panoramica di alto livello su come AWS Entity Resolution e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per AWS Entity Resolution

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. 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 informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche 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 le policy basate su risorse	Sì

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket 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. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy 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 amministratore IAM dell'account affidabile 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 Cross Account Resource Access in IAM nella IAM User Guide.

Azioni politiche per AWS Entity Resolution

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. 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, consulta Actions Defined by 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 le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (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 dei relativi ARN, consulta Resources Defined by AWS Entity Resolution nel Service Authorization Reference. Per informazioni

sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni 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 le policy AWS JSON 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, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

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'utente IAM.

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

ACL in AWS Entity Resolution

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AWS Entity Resolution

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

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 su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AWS Entity Resolution

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua 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 sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS 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, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per AWS Entity Resolution

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM 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. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per AWS Entity Resolution

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

> **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. Servizio AWS 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 amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da 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 l'API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore

IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS Entity Resolution, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Actions, Resources and Condition Keys AWS Entity Resolution nel Service Authorization Reference.

Argomenti

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 Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste 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 di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio

se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console di AWS Entity Resolution

Per accedere alla AWS Entity Resolution console, devi 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 consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora 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 Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica

include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 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 Servizio AWS 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 Servizi AWS 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 un 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'utente `mateojackson` IAM prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `entityresolution:`*`GetWidget`* fittizie.

```
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 Servizi AWS 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 utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS Entity Resolution. Tuttavia, l'operazione 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 aiuto, contatta il tuo AWS 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 servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy 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, consultaCome AWS Entity Resolution funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Convalida della conformità per AWS Entity Resolution

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di 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 Servizi AWS 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.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- 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 Servizi AWS 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)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS 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: Servizio AWS 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, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS Entity Resolution

L'infrastruttura globale dei servizi AWS è progettata attorno a regioni Regioni AWS e zone di disponibilità. Le regioni di Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e a velocità effettiva elevata. Con le Zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico 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.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

Oltre all'infrastruttura globale di AWS, AWS Entity Resolution offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup.

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.

Creazione di risorse AWS Entity Resolution con AWS CloudFormation

AWS Entity Resolution è integrato con AWS CloudFormation, un servizio che ti aiuta a modellare e configurare AWS le tue risorse in modo da poter dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (come AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e AWS::EntityResolution::PolicyStatement) e fornisce e AWS CloudFormation configura tali risorse per te.

Quando lo usi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse 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.

AWS Entity Resolution e AWS CloudFormation modelli

Per fornire e configurare risorse per AWS Entity Resolution e i servizi correlati, devi conoscere AWS CloudFormation i modelli. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse che desideri fornire nei tuoi AWS CloudFormation stack. Se non conosci JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a usare i modelli. AWS CloudFormation Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation .

AWS Entity 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 di modelli JSON e YAML per AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace e AWS::EntityResolution::PolicyStatement, consulta 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

CreateMatchingWorkflow nel documento di riferimento delle API AWS Entity Resolution

- 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

  CreateSchemaMapping nel documento di riferimento delle API AWS Entity Resolution

- 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

  CreateIdMappingWorkflow nel documento di riferimento delle API AWS Entity Resolution

- Spazio dei nomi 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

  CreateIdNamespace nel documento di riferimento delle API AWS Entity Resolution

- PolicyStatement

Crea un oggetto `PolicyStatement`.

Per ulteriori informazioni, consulta i seguenti argomenti:

AWS::EntityResolution::PolicyStatement nella Guida per l'utente di AWS CloudFormation

AddPolicyStatement nel documento di riferimento delle API AWS Entity Resolution

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- Riferimento API AWS CloudFormation
- 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. Servizio AWS 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 corrispondenti 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 della documentazione, puoi sottoscrivere il feed RSS. Per sottoscrivere gli aggiornamenti RSS, è necessario che un plug-in RSS sia abilitato per il browser in uso.

Modifica	Descrizione	Data
Flusso di lavoro corrispondente: 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 utilizzare un flusso di lavoro di mappatura degli ID su più piattaforme. Account AWS	2 aprile 2024
CloudFormation Risorse AWS: risorse nuove e aggiornate	AWS Entity Resolution ha aggiunto le seguenti risorse: `AWS::EntityResolution::IdNamespace` `AWS::EntityResolution::PolicyStatement` e ha aggiornato la seguente risorsa:`AWS::EntityResolution::IdMappingWorkflow` .	2 aprile 2024
Trova Match ID	I clienti possono ora trovare il Match ID corrispondente e la regola associata per un flusso	25 marzo 2024

	di lavoro elaborato basato su regole.	
Flusso di lavoro corrispondente: aggiornamento	AWS Entity Resolution ora supporta l'assegnazione RAMPID basata su PII nel flusso di lavoro di abbinamento basato sui LiveRamp servizi del 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 della risorsa Amazon (ARN)

Un identificatore univoco per le risorse. AWS Gli ARN sono necessari quando è necessario specificare una risorsa in modo univoco su tutti i fronti AWS Entity Resolution, ad esempio nelle AWS Entity Resolution policy, nei tag Amazon Relational Database Service (Amazon RDS) 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 chiave KMS AWS Entity Resolution gestita.

Testo 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 del flusso di lavoro corrispondenti che verranno inclusi nell'output.

Workflow di mappatura degli ID

Il processo che configuri per specificare i dati di input per tradurre i tuoi ID e il modo in cui desideri che venga eseguita la mappatura degli ID.

AWS Entity Resolution attualmente è supportato LiveRamp come metodo di mappatura degli ID. È necessario disporre di un abbonamento a LiveRamp Through per utilizzare il AWS Data Exchange flusso di lavoro di mappatura degli ID.

Per ulteriori informazioni, consulta Iscriviti a un provider di servizi su AWS Data Exchange.

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 ingresso ARN (InputSourceARN)

L'Amazon Resource Name (ARN) 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 di 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 i 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 = Elimina gli spazi bianchi iniziali e finali
- LOWERCASE = Mette in minuscolo tutti i caratteri alfa
- CONVERT_ACCENT = Converte 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 = Converte da lettera accentata a lettera normale
- REMOVE_ALL_NON_EMAIL_CHARS = Rimuove tutti i caratteri [a-zA-Z0-9] e [.@ -] non-alpha-numeric

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 = Converte da lettera accentata a lettera normale
- REMOVE_ALL_NON_ALPHA = Rimuove tutti i caratteri non alfa [a-zA-Z]
- RENAME_WORDS utilizzando ADDRESS_RENAME_WORD_MAP = sostituisce le parole nella stringa di indirizzo con le parole di ADDRESS_RENAME_WORD_MAP
- RENAME_DELIMITERS utilizzando ADDRESS_RENAME_DELIMITER_MAP = sostituisci i delimitatori nella stringa di indirizzo con la stringa di ADDRESS_RENAME_DELIMITER_MAP
- RENAME_DIRECTIONS utilizzando ADDRESS_RENAME_DIRECTION_MAP = sostituisce i delimitatori nella stringa di indirizzo con la stringa di ADDRESS_RENAME_DIRECTION_MAP
- RENAME_NUMBERS utilizzando ADDRESS_RENAME_NUMBER_MAP = sostituisce i numeri nella stringa di indirizzo con la stringa di ADDRESS_RENAME_NUMBER_MAP
- RENAME_SPECIAL_CHARS utilizzando ADDRESS_RENAME_SPECIAL_CHAR_MAP = sostituisci i caratteri speciali nella stringa di indirizzo con la stringa di ADDRESS_RENAME_SPECIAL_CHAR_MAP

INDIRIZZO_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 "
```

INDIRIZZO_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"
```

INDIRIZZO_RINOMINA_NUMERO_MAPPA

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, AND. `Record One mobile_phone = Record Two mobile_phone` `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
- UID 2.0

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 trovati risultati secondo la Regola 2 perché sarebbero stati tutti trovati 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.

ARN di mappatura dello schema

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.

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.