ユーザーガイド

AWS Entity Resolution

AWS Entity Resolution: ユーザーガイド

Table of Contents

とは AWS Entity Resolution

AWS Entity Resolution は、複数のアプリケーション、チャネル、データストアに保存された関連レコードの照合、リンク、および強化に役立つサービスです。柔軟でスケーラブルで、既存のアプリケーションやデータサービスプロバイダーに接続できるエンティティ解決ワークフローの使用を開始できます。

AWS Entity Resolution は、ルールベースのマッチング、機械学習ベースのマッチング (ML マッチング) 、データサービスプロバイダー主導のマッチングなどの高度なマッチング手法を提供します。これらの手法は、顧客情報、製品コード、またはビジネスデータコードの関連レコードをより正確にリンクして強化するのに役立ちます。

を使用して AWS Entity Resolution 、最近のイベント (広告クリック、カートの放棄、購入など) をデータサービスプロバイダーからの仮名化されたシグナルと一意のエンティティ ID にリンクすることで、カスタマーインタラクションの統合ビューを作成できます。また、ストア全体で異なるコード (SKU、UPC など) を使用する製品をより適切に追跡することもできます。を使用すると AWS Entity Resolution 、データの移動を最小限に抑えながら、マッチングの精度を制御し、データセキュリティをより適切に保護できます。

トピック

- 初めての AWS Entity Resolution ユーザーですか？
- の機能 AWS Entity Resolution
- 関連サービス
- アクセス AWS Entity Resolution
- の料金 AWS Entity Resolution

初めての AWS Entity Resolution ユーザーですか？

を初めて使用する場合は AWS Entity Resolution、まず以下のセクションを読むことをお勧めします。

- の機能 AWS Entity Resolution
- アクセス AWS Entity Resolution
- セットアップ AWS Entity Resolution

の機能 AWS Entity Resolution

AWS Entity Resolution には以下の機能が含まれています。

- 柔軟でカスタマイズ可能なデータ準備

  AWS Entity Resolution は からデータを読み取り AWS Glue 、一致処理の入力として使用します。最大 20 個のデータ入力を指定できます。 はデータ入力テーブルの各行をレコードとして AWS Entity Resolution 処理し、一意のエンティティをプライマリキーとして使用します。 AWS Entity Resolution は暗号化されたデータセットで動作できます。まず、 のスキーママッピングを定義して AWS Entity Resolution 、一致するワークフロー で使用する入力フィールドを理解します。既存の AWS Glue データ入力から独自のデータスキーマまたはブループリントを取り込むことができます。または、インタラクティブユーザーインターフェイスまたは JSON エディタを使用してカスタムスキーマを構築することもできます。 AWS Entity Resolution また、デフォルトでは、 は一致する前にデータ入力を正規化し、特殊文字や余分なスペースの削除、テキストの小文字へのフォーマットなど、一致処理を改善します。データ入力が既に正規化されている場合は、正規化をオフにできます。また、GitHub ライブラリ も用意されています。これを使用して、ニーズに合わせてデータの正規化プロセスをさらにカスタマイズできます。

- 設定可能なエンティティマッチングワークフロー

  エンティティマッチングワークフローは、データ入力を照合 AWS Entity Resolution する方法と、統合データ出力をどこに書き込むかを示すためにセットアップする一連のステップです。1 つ以上のマッチングワークフローを設定して、異なるデータ入力を比較し、エンティティ解決や ML エクスペリエンスのないルールベースのマッチング、機械学習マッチング、データサービスプロバイダー主導のマッチングなど、さまざまなマッチング手法を使用できます。リソース番号、処理されたレコード数、見つかった一致の数など、既存の一致ワークフローとメトリクスのジョブステータスを表示することもできます。

  - R eady-to-use ルールベースのマッチング

    このマッチング手法には、 または AWS Command Line Interface () AWS Management Console の一連の ready-to-use ルールが含まれますAWS CLI。これらのルールを使用して、入力フィールドに基づいて関連レコードを検索できます。ルールごとに入力フィールドを追加または削除したり、ルールを削除したり、ルールの優先度を再配置したり、新しいルールを作成したりして、ルールをカスタマイズすることもできます。ルールをリセットして元の設定に戻すこともできます。Amazon Simple Storage Service (Amazon S3) バケットのデータ出力には、ルールベースのマッチング手法 を使用して が AWS Entity Resolution 生成する一致グループがあります。各一致グループには、一致を理解するのに役立つように、それに関連付けられた一致を生成するため

に使用されるルール番号があります。例えば、ルール番号は、ルール 1 がルール 2 よりも正確になるように、各一致グループの精度を示すことができます。

- 事前設定された機械学習ベースのマッチング (ML マッチング)

  このマッチング手法には、すべてのデータ入力、特にコンシューマーベースのレコードの一致を見つけるための事前設定された ML モデルが含まれています。このモデルでは、名前、E メールアドレス、電話番号、住所、生年月日のデータ型に関連付けられたすべての入力フィールドを使用します。このモデルは、他のマッチグループと比較したマッチの品質を説明する各グループの信頼スコアを含む関連レコードのマッチグループを生成します。このモデルは欠落している入力フィールドを考慮し、レコード全体をまとめて分析してエンティティを表します。Amazon S3 バケットのデータ出力には、ML マッチングを使用して が AWS Entity Resolution 生成する一致グループがあります。これは、各マッチグループに関連付けられた信頼スコアが 0.0 ~ 1.0 の場合で、マッチの精度を示します。

- レコードとデータサービスプロバイダーの照合

  AWS Entity Resolution を使用すると、主要なデータサービスベンダーやライセンスデータセットとレコードを照合、リンク、強化して、顧客を理解し、到達し、サービスを提供する能力を高めることができます。例えば、データに属性を追加してレコードを強化したり、ビジネス目標を達成するために と連携するシステムとプラットフォームの相互運用性を改善したりできます。このマッチングワークフローを数回クリックするだけで、複雑な独自統合を構築して維持する必要がなくなります。このマッチング手法を利用するには、これらのデータサービスプロバイダーとのライセンス契約が必要です。

- 手動一括処理と自動増分処理

  データ処理を使用すると、エンティティマッチングワークフロー設定を使用して生成された共通の一致 ID を持つ同様のレコードを含む統合データ出力テーブルに、データ入力を変換できます。API および AWS Management Console または を使用すると AWS CLI、既存の抽出、変換、ロード (ETL) データパイプラインに基づいて、オンデマンドで手動一括処理を実行できます。ETL データパイプラインは、新しい一致と既存の一致の更新についてすべてのデータを再処理します。また、ルールベースのマッチングシナリオでは、自動増分処理を開始して、Amazon S3 バケットで新しいデータが利用可能になるとすぐに、サービスはそれらの新しいレコードを読み取り、既存のレコードと比較できます。これにより、Amazon S3 データの変更と一致が最新の状態になります。

- ほぼリアルタイムの検索

  AWS Entity Resolution GetMatchId API オペレーションを使用してエンティティフィールドを検索すると、既存の一致 ID を同期的に取得できます。さまざまなソースやチャネルを通じて取得さ

れた個人を特定できる情報 (PII) 属性 AWS Entity Resolution を使用して を呼び出すことができます。 は、データ保護のためにこれらの属性を AWS Entity Resolution ハッシュし、対応する一致 ID を取得して、顧客をリンクして一致させます。例えば、関連付けられた名前、E メール、および郵送先住所を含むウェブサインアップを取得できます。 GetMatchId API AWS Entity Resolution オペレーションを使用して、この顧客またはエンティティが S3 バケットに保存されている一致結果に既に存在するかどうか、およびそれに関連付けられた対応するエンティティー致 ID を確認します。エンティティー致 ID を取得したら、顧客関係管理 (CRM) や顧客データプラットフォーム (CDP) システムなど、ソースアプリケーションでエンティティー致 ID に関連付けられたトランザクション情報を確認できます。

- データ保護と設計による地域化

  AWS Entity Resolution は、データの保護に役立つデフォルトの暗号化機能を提供し、サービスへのすべてのデータ入力に暗号化キーを提供します。例えば、 AWS Entity Resolution では、サーバー側の暗号化データとハッシュ化されたデータを使用してルールベースのマッチングワークフローを柔軟に実行できます。 はリージョン化 AWS Entity Resolution をサポートしています。つまり、一致するワークフローを実行して、サービスを使用している AWS リージョン のと同じ でデータを処理します。また、他のアプリケーションで解決されたデータを使用する前に、Amazon S3 でデータ出力を暗号化してハッシュ化することもできます。

- マルチパーティートランスコード

  AWS Entity Resolution は、 など、データコラボレーションを使用する複数の当事者間でデータソースとマッチング設定を定義するのに役立ちます AWS Clean Rooms。

関連サービス

以下は、 に関連して AWS のサービス います AWS Entity Resolution。

- Amazon S3

  Amazon S3 AWS Entity Resolution に取り込むデータを保存します。

  詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 とは」を参照してください。

- AWS Glue

  で使用する Amazon S3 のデータから AWS Glue テーブルを作成します AWS Entity Resolution。

詳細については、「 AWS Glue デベロッパーガイド」の「 とは AWS Glue」を参照してください。

- AWS CloudTrail

  CloudTrail を ログ AWS Entity Resolution とともに使用して、アクティビティの分析 AWS のサービス を強化します。

  詳細については、「を使用した AWS Entity Resolution API コールのログ記録 AWS CloudTrail」を参照してください。

- AWS CloudFormation

  ： AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace and で次のリソースを作成します AWS CloudFormation。 AWS::EntityResolution::PolicyStatement

  詳細については、「を使用した AWS エンティティ解決リソースの作成 AWS CloudFormation」を参照してください。

アクセス AWS Entity Resolution

には、次のオプション AWS Entity Resolution を使用してアクセスできます。

- https://console.aws.amazon.com/entityresolution/ の AWS Entity Resolution コンソールから直接。
- AWS Entity Resolution API を使用してプログラムで。詳細については、「AWS Entity Resolution APIリファレンス」を参照してください。
  - AWS Lambda ランタイムで AWS Entity Resolution API を呼び出す場合は、独自のデプロイパッケージを作成し、目的のバージョンの AWS SDK ライブラリを含めます。詳細については、「 AWS Lambda デベロッパーガイド」の以下の例を参照してください。
    - .zip または JAR ファイルアーカイブを使用して Java Lambda 関数をデプロイする
    - Python Lambda 関数の .zip ファイルアーカイブの使用

の料金 AWS Entity Resolution

料金に関する情報については、[AWS Entity Resolution の料金]を参照してください。

セットアップ AWS Entity Resolution

AWS Entity Resolution を初めて使用する場合は、事前に以下のタスクを完了してください。

トピック

にサインアップする AWS

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

管理者ユーザーの作成

管理者ユーザーを作成するには、以下のいずれかのオプションを選択します。

管理者を管理する方法を 1 つ選択します	目的	方法	以下の操作も可能
IAM Identity Center 内 (推奨)	短期の認証情報を使用して AWSにアクセスします。 これはセキュリティのベストプラクティスと一致しています。ベストプラクティスの詳細については、IAM ユーザーガイドの「IAM でのセキュリティのベストプラクティス」を参照してください。	AWS IAM Identity Center ユーザーガイドの「開始方法」の手順に従います。	ユーザーガイド の を使用する AWS CLI ように を設定 AWS IAM Identity Centerして、プログラムによるアクセスを設定します。 AWS Command Line Interface
IAM 内 (非推奨)	長期認証情報を使用して AWSにアクセスする。	IAM ユーザーガイドの「最初の IAM 管理者のユーザーおよびグループの作成」の手順に従います。	IAM ユーザーガイドの「IAM ユーザーのアクセスキーの管理」に従って、プログラムによるアクセスを設定します。

でプロバイダーサービスをサブスクライブする AWS Data Exchange

プロバイダーのサービスベースのマッチングワークフロー または ID マッピングワークフロー を使用している場合は、次の手順を実行します。プロバイダーのサービスベースのマッチングワークフローまたは ID マッピングワークフローを使用していない場合は、このステップをスキップできます。

で AWS Entity Resolution、そのプロバイダーのサブスクリプションを で持っている場合は、次のいずれかのプロバイダーサービスで一致するワークフローを実行できます AWS Data Exchange。データは、希望するプロバイダーによって定義された入力のセットと照合されます。

- LiveRamp
  - LiveRamp ID 解決
  - LiveRamp トランスコード
- TransUnion
  - TransUnion TruAudience Transfer-less Identity Resolution & Enrichment
  - TransUnion TruAudience 転送レス ID 解決
- 統合 ID 2.0
  - 統合 ID 2.0 アイデンティティ解決

さらに、そのプロバイダーのサブスクリプション LiveRamp がある場合は、 で ID マッピングワークフローを実行できます。

- LiveRamp
  - LiveRamp トランスコード

プロバイダーサービスをサブスクライブするには、次の 2 つの方法があります。

- プライベートオファー – プロバイダーと既存の関係がある場合は、 AWS Data Exchange ユーザーガイドの「プライベート製品とオファー」の手順に従って、 でプライベートオファーを承諾します AWS Data Exchange。
- 独自のサブスクリプションの持ち込み – プロバイダーと既存のデータサブスクリプションがある場合は、 AWS Data Exchange ユーザーガイドの Bring Your Own Subscription (BYOS) オファー手順に従って、 で BYOS オファーを承諾します AWS Data Exchange。

でプロバイダーサービスをサブスクライブしたら AWS Data Exchange、そのプロバイダーサービスで一致するワークフローまたは ID マッピングワークフローを作成できます。

APIsAWS Data Exchange ユーザーガイド」の「 での API 製品へのアクセス」を参照してください。

データテーブルを準備する

では AWS Entity Resolution、各入力データテーブルにソースレコードが含まれています。これらのレコードには、名、姓、E メールアドレス、電話番号などのコンシューマー識別子が含まれます。これらのソースレコードは、同じまたは他の入力データテーブル内で指定した他のソースレコードと照合できます。各レコードには一意のレコード ID (一意の ID) が必要です。また、 内でスキーママッピングを作成するときに、プライマリキーとして定義する必要があります AWS Entity Resolution。

すべての入力データテーブルは、Amazon S3 にバックアップされた AWS Glue テーブルとして使用できます。Amazon S3 内に既にあるファーストパーティデータを使用することも、他の SaaS プロバイダーから Amazon S3 にデータテーブルをインポートすることもできます。データが Amazon S3 にアップロードされたら、 AWS Glue クローラを使用して にデータテーブルを作成できます AWS Glue Data Catalog。その後、データテーブルを への入力として使用できます AWS Entity Resolution。

データテーブルを準備するには、以下のステップに従います。

トピック

- ステップ 1: 入力データを準備する
- ステップ 2: 入力データテーブルをサポートされているデータ形式で保存する
- ステップ 3: 入力データテーブルを Amazon S3 にアップロードする
- ステップ 4: AWS Glue テーブルを作成する

ステップ 1: 入力データを準備する

プロバイダーサービスで一致するワークフローを使用している場合は、次の手順を実行します。プロバイダーサービスで一致するワークフローを使用していない場合は、このステップをスキップできます。

詳細については、「でプロバイダーサービスをサブスクライブする AWS Data Exchange」を参照してください。

プロバイダーのサービスベースのマッチングワークフローまたは ID マッピングワークフローを使用してマッチングワークフローを実行する場合は、次の表を参照して入力データを準備します。

プロバイダーサービス	一意の ID が必要ですか？	アクション
LiveRamp	はい	以下を確認してください。 • 一意の ID は、独自の仮名識別子または行 ID のいずれかです。 • データ入力ファイルの形式と正規化は、 LiveRamp ガイドラインに沿ったものです。 マッチングワークフローの入力ファイルフォーマットガイドラインの詳細については、 LiveRamp ドキュメントの「ADX によるアイデンティティ解決の実行」を参照してください。 ID マッピングワークフローの入力ファイルフォーマットガイドラインの詳細については、LiveRamp ドキュメントの「ADX によるトランスコーディングの実行」を参照してください。
TransUnion	はい	以下を確認してください。 • TransUnion データエンリッチメントには一意の ID が存在します。 **Note** パススルー属性は、 への入力と出力に保持できます TransUnion。世帯 E キーと HHID は、クライ

プロバイダーサービス	一意の ID が必要ですか？	アクション

		アント名前空間に固有です。
		• **Phone number** は 10 桁で、スペースやハイフンなどの特殊文字は使用できません。
		• **Addresses** を に分割する必要があります
		  • 1 つのアドレス行 (アドレス行 1 と 2 が混在している場合)
		  • city
		  • zip (または zip plus4)、スペースやハイフンなどの特殊文字なし
		  • 状態、2 文字コード 3 として指定
		• **Email addresses** はプレーンテキストである必要があります。
		• **First Name** は小文字でも大文字でもかまいませんが、ニックネームはサポートされていますが、タイトルとサフィックスは除外する必要があります。
		• **Last Name** は小文字でも大文字でもかまいません。ミドルネームは除外します。

プロバイダーサービス	一意の ID が必要ですか？	アクション
統合 ID 2.0	はい	以下を確認してください。 • 一意の ID をハッシュにすることはできません。 • UID2 は、UID2 生成用の E メールと電話番号の両方をサポートします。ただし、両方の値がスキーママッピングに存在する場合、ワークフローは出力の各レコードを複製します。1 つのレコードは UID2 生成用の E メールを使用し、2 番目のレコードは電話番号を使用します。データに E メールと電話番号が混在していて、このレコードの重複を出力にしたくない場合は、それぞれに個別のワークフローを作成し、個別のスキーママッピングを使用するのが最善の方法です。このシナリオでは、ステップを 2 回実行します。E メールの場合は 1 つのワークフローを作成し、電話番号の場合は別のワークフローを作成します。 **Note** 特定の E メールまたは電話番号は、リクエストを行ったユーザーに関係なく、任意の時点で同じ raw UID2 値になります。

プロバイダーサービス	一意の ID が必要ですか？	アクション
		Raw UID2sは、ソルトバケットからソルトを追加することで作成されます。ソルトバケットは 1 年に約 1 回ローテーションされるため、raw UID2 もローテーションされます。異なるソルトバケットは 1 年を通して異なる時間にローテーションされます。 AWS Entity Resolution は現在、ローテーションするソルトバケットと未加工の UID2s を追跡していないため、未加工UID2s を毎日再生成することをお勧めします。詳細については、UID2s「増分更新のために UID2 を更新する頻度」を参照してください。

ステップ 2: 入力データテーブルをサポートされているデータ形式で保存する

サポートされているデータ形式で入力データを既に保存している場合は、このステップをスキップできます。

を使用するには AWS Entity Resolution、入力データが AWS Entity Resolution をサポートする形式である必要があります。 は次のデータ形式 AWS Entity Resolution をサポートしています。

- カンマ区切り値 (CSV)

> **Note**
>
> LiveRamp は CSV ファイルのみをサポートします。

- Parquet

ステップ 3: 入力データテーブルを Amazon S3 にアップロードする

Amazon S3 にファーストパーティーデータテーブルがすでにある場合は、このステップをスキップできます。

> **Note**
>
> 入力データは、一致するワークフローを実行する同じ AWS アカウント と AWS リージョンの Amazon Simple Storage Service (Amazon S3) に保存する必要があります。

入力データテーブルを Amazon S3 にアップロードするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. バケット を選択し、データテーブルを保存するバケットを選択します。
3. [アップロード] を選択し、プロンプトに従います。
4. [オブジェクト] タブを選択し、データが保存されているプレフィックスを表示します。フォルダの名前を書き留めます。

   フォルダを選択すると、データテーブルを表示できます。

ステップ 4: AWS Glue テーブルを作成する

Amazon S3 の入力データは、 でカタログ化 AWS Glue され、テーブルとして AWS Glue 表される必要があります。Amazon S3 を入力として AWS Glue テーブルを作成する方法の詳細については、「 デベロッパーガイド」の「 AWS Glue コンソールでのクローラの使用」を参照してください。 AWS Glue

> **Note**
>
> AWS Entity Resolution はパーティションテーブルをサポートしていません。

このステップでは、S3 バケット内のすべてのファイルをクロール AWS Glue し、 AWS Glue テーブルを作成するクローラーを にセットアップします。

> **Note**
>
> AWS Entity Resolution は現在、 に登録されている Amazon S3 ロケーションをサポートしていません AWS Lake Formation。

AWS Glue テーブルを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/glue/ で AWS Glue コンソールを開きます。
2. ナビゲーションバーから、[クローラ] を選択します。
3. リストから S3 バケットを選択し、[クローラを追加] を選択します。
4. [クローラを追加] ページで [クローラの名前] を入力し、[次へ] を選択します。
5. 引き続き [クローラを追加] ページで、詳細を指定します。
6. [IAM ロールの選択] ページで [既存の IAM ロールを選択] を選択し [次へ] 選択します。

   [IAM ロールを作成する] を選択することも、必要に応じて管理者に IAM ロールを作成してもらうこともできます。
7. [このクローラのスケジュールを設定する] で、[頻度] をデフォルト ([オンデマンドで実行]) のままにして、[次へ] を選択します。
8. [クローラの出力を設定する] に AWS Glue データベースを入力し、[次へ] を選択します。
9. 詳細を確認し、[完了] を選択します。
10. [クローラ] ページで、S3 バケットの横にあるチェックボックスをオンにし、[クローラの実行] を選択します。
11. クローラーの実行が完了したら、 AWS Glue ナビゲーションバーでデータベース を選択し、データベース名を選択します。
12. [データベース] ページで、[{データベース名} のテーブル] を選択します。

a. AWS Glue データベース内のテーブルを表示します。

b. テーブルのスキーマを表示するには、特定のテーブルを選択します。

13. AWS Glue データベース名と AWS Glue テーブル名を書き留めます。

コンソールユーザーの IAM ロールを作成する

IAM ロールを作成するには

1. 管理者アカウントを使用して、IAM コンソール (https：//console.aws.amazon.com/iam/) にサインインします。
2. [アクセス管理] で、[ロール] を選択します。

   ロールを使用して短期認証情報を作成できます。これはセキュリティを強化するために推奨されます。[ユーザー] を選択して長期間の認証情報を作成することもできます。
3. [ロールの作成] を選択します。
4. ロールの作成ウィザードで、信頼されたエンティティタイプ で、 を選択しますAWS アカウント。
5. このアカウントを選択したまま、次へ を選択します。
6. アクセス許可の追加 で、ポリシーの作成 を選択します。

   新しいタブが開きます。

   a. JSON タブを選択し、コンソールユーザーに付与された機能に応じてポリシーを追加します。 は、一般的なユースケースに基づいて次の管理ポリシー AWS Entity Resolution を提供します。

      - AWS 管理ポリシー: AWSEntityResolutionConsoleFullAccess
      - AWS マネージドポリシー: AWSEntityResolutionConsoleReadOnlyAccess

   b. [次へ: タグ] を選択し、タグを追加して (オプション)、[次へ: 確認] を選択します。

   c. [ポリシーの確認] で [名前] と [説明] を入力し、[概要] を確認します。

   d. [ポリシーを作成] を選択します。

      コラボレーションメンバー用のポリシーが作成されました。

   e. 元のタブに戻り、「アクセス許可を追加」で、先ほど作成したポリシーの名前を入力します。(ページを再度読み込む必要がある場合があります)。

f. 作成したポリシーの名前の横にあるチェックボックスを選択し、次へ を選択します。

7. [名前、確認、および作成] で、[ロール名] と [説明] を入力します。

   a. [信頼されたエンティティを選択] を確認し、ロールを引き受ける人物 (複数可) の AWS アカウント を入力します (必要な場合)。

   b. [許可を追加] でアクセス許可を確認し、必要に応じて編集します。

   c. [タグ] を確認し、必要に応じてタグを追加します。

   d. [ロールを作成] を選択します。

のワークフロージョブロールを作成する AWS Entity Resolution

AWS Entity Resolution はワークフロージョブロールを使用してワークフローを実行します。必要な IAM アクセス許可がある場合には、コンソールを使用してこのロールを作成できます。アクセス`CreateRole`許可がない場合は、管理者にロールの作成を依頼してください。

のワークフロージョブロールを作成するには AWS Entity Resolution

1. 管理者アカウントで https://console.aws.amazon.com/iam/ の IAM コンソールにサインインします。
2. [アクセス管理] で、[ロール] を選択します。

   ロールを使用して短期認証情報を作成できます。これはセキュリティを強化するために推奨されます。[ユーザー] を選択して長期間の認証情報を作成することもできます。
3. [ロールの作成] を選択します。
4. [ロールの作成] ウィザードの [信頼されたエンティティタイプ] で [カスタム信頼ポリシー] を選択します。
5. 次のカスタム信頼ポリシーをコピーして JSON エディタに貼り付けます。

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

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

6. [次へ] をクリックします。
7. アクセス許可の追加 で、ポリシーの作成 を選択します。

   新しいタブが表示されます。

   a. 次のポリシーをコピーして JSON エディタに貼り付けます。

> **Note**
>
> 次のポリシー例では、Amazon S3 や などの対応するデータリソースを読み取るために必要なアクセス許可をサポートしています AWS Glue。ただし、データソースの設定方法によっては、このポリシーの変更が必要になる場合があります。
> AWS Glue リソースと基盤となる Amazon S3 リソースは、 AWS リージョン と同じ にある必要があります AWS Entity Resolution。
> データソースが暗号化または復号化されていない場合、アクセス AWS KMS 許可を付与する必要はありません。

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

```
}
```

各 *{{user input placeholder}}* を独自の情報に置き換えます。

aws-#####	AWS リージョン リソースの 。 AWS Glue リソース、基盤となる Amazon S3 リソース、リソース AWS KMS は、 AWS リージョン と同じ にある必要がありますAWS Entity Resolution 。
accountId	AWS アカウント ID。
######	が読み取り元の の基盤となるデータオブジェクトを含む Amazon S3 AWS Glue AWS Entity Resolution バケット。
######	AWS Entity Resolution が出力データを生成する Amazon S3 バケット。
########	AWS Glue AWS Entity Resolution が読み取り元のデータベース。

b. (オプション) 入力 Amazon S3 バケットが顧客の KMS キーを使用して暗号化されている場合は、以下を追加します。

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

各 *{{user input placeholder}}* を独自の情報に置き換えます。

aws-#####	AWS リージョン リソースの 。 AWS Glue リソース、基盤となる Amazon S3 リソース、リソース AWS KMS は、 AWS リージョン と同じ にある必要がありますAWS Entity Resolution 。
accountId	AWS アカウント ID。
inputKeys	のマネージドキー AWS Key Management Service。入力ソースが暗号化されている場合、 AWS Entity Resolution はキーを使用してデータを復号する必要があります。

c. (オプション) 出力 Amazon S3 バケットに書き込まれるデータを暗号化する必要がある場合は、以下を追加します。

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

各 *{{user input placeholder}}* を独自の情報に置き換えます。

aws-#####	AWS リージョン リソースの 。 AWS Glue リソース、基盤となる Amazon S3 リソース、リソース AWS KMS は、 AWS リージョン と同じ にある必要がありますAWS Entity Resolution 。
accountId	AWS アカウント ID。

outputKeys	のマネージドキー AWS Key Management Service。出力ソースを暗号化する必要がある場合、 は キーを使用して出力データを暗号化AWS Entity Resolution する必要があります。

d. (オプション) を通じてプロバイダーサービスのサブスクリプションがあり AWS Data Exchange、プロバイダーのサービスベースのワークフローに既存のロールを使用する場合は、以下を追加します。

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

各 *{{user input placeholder}}* を独自の情報に置き換えます。

aws-#####	プロバイダーリソース AWS リージョンが付与される 。この値は、 AWS Data Exchange コンソールのアセット ARN にあります。例 : `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
datasetId	AWS Data Exchange コンソールにあるデータセットの ID。
revisionId	AWS Data Exchange コンソールにあるデータセットのリビジョン。

assetId	コンソールにある AWS Data Exchange アセットの ID。

8. 元のタブに戻り、「アクセス許可を追加」で、先ほど作成したポリシーの名前を入力します。(ページを再度読み込む必要がある場合があります)。
9. 作成したポリシーの名前の横にあるチェックボックスを選択し、次へ を選択します。
10. [名前、確認、および作成] で、[ロール名] と [説明] を入力します。

> **Note**
>
> ロール名は、 を渡workflow job roleして一致するワークフローを作成できるメンバーに付与されたpassRoleアクセス許可のパターンと一致する必要があります。例えば、 AWSEntityResolutionConsoleFullAccess管理ポリシーを使用している場合は、ロール名に entityresolutionを含めることを忘れないでください。

   a. [信頼されたエンティティを選択] を確認し、必要に応じて編集します。
   b. [許可を追加] でアクセス許可を確認し、必要に応じて編集します。
   c. [タグ] を確認し、必要に応じてタグを追加します。
   d. [ロールを作成] を選択します。

のワークフロージョブロール AWS Entity Resolution が作成されました。

スキーママッピングの作成

解決する入力データを定義するには、スキーママッピングを作成します。スキーママッピングプロセスでは、入力フィールドと属性タイプを定義し、一致キーを定義してグループ化することで、解決するデータを定義する一連のステップをガイドします。

でスキーママッピングを作成するには、次の 3 つの方法があります AWS Entity Resolution。

- ガイド付きフローを使用して既存のスキーマ情報をインポートします。
- ガイド付きフローを使用して、入力データ を手動で定義します。
- JSON エディタを使用して、スキーママッピング を作成、貼り付け、またはインポートします。

以下のプロセスでは、スキーママッピングを作成する 3 つの異なる方法を説明します。

トピック

スキーママッピングを作成する (事前入力列)

この手順では、 AWS Entity Resolution コンソールの Import from AWS Glueオプションを使用してスキーママッピングを作成するプロセスについて説明します。この作成方法を使用して、 テーブルから AWS Glue 事前入力された列で始まる入力フィールドを定義できます。

事前入力された列を使用してスキーママッピングを作成するには：

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのデータ準備 で、スキーママッピング を選択します。
3. スキーママッピング ページの右上隅で、スキーママッピングの作成 を選択します。
4. ステップ 1: スキーマの詳細を指定するには、次の手順を実行します。
    a. 名前と作成方法 に、スキーママッピング名とオプションの説明 を入力します。
    b. 作成方法 で、 からインポート AWS Glueを選択します。

c. ドロップダウンからAWS Glue データベースを選択し、ドロップダウンからAWS Glue テーブルを選択します。

新しいテーブルを作成するには、 AWS Glue コンソール https://console.aws.amazon.com/glue/ に移動します。詳細については、「 ユーザーガイド」の「 AWS Glue テーブルAWS Glue 」を参照してください。

d. 一意の ID には、データの各行を区別して参照する列を指定します。

Example

たとえば、**`Primary_key`**、**`Row_ID`**、または **`Record_ID`** などです。

> **Note**
>
> 一意の ID 列は必須です。一意の ID は、1 つのテーブル内の一意の識別子である必要があります。ただし、異なるテーブル間では、一意の ID に重複する値を含めることができます。一意の ID が指定されていない場合、同じソース内で一意でない場合、またはソース間で属性名の点で重複している場合、 は一致するワークフローの実行時にレコード AWS Entity Resolution を拒否します。

e. 入力フィールド で、マッチングに使用する 1～25 列を選択し、オプションのパススルーに使用します。

i. マッチングに使用されない列を指定する場合は、パススルー用の列を追加を選択します。

ii. パススルー – オプションで、パススルー列として含める列を選択します。

f. (オプション) リソースのタグを有効にする場合は、新しいタグを追加 を選択し、キーと値のペアを入力します。

g. [次へ] をクリックします。

5. ステップ 2: 入力フィールド をマッピングするには、次の手順を実行します。

a. を照合する入力フィールドには、各入力フィールド の入力タイプと一致キーを指定します。

入力タイプは、データを分類するのに役立ちます。一致キーを使用すると、入力フィールドを一致するワークフローと比較できます。

> **Note**
>
> LiveRamp プロバイダーのサービスベースのマッチング手法で使用するスキーママッピングを作成する場合は、次のことができます。
>
> - 入力タイプを LiveRamp ID として指定します。
> - 名前フィールドを複数のフィールド (**first_name**、 など**last_name**) または 1 つのフィールドで指定します。
> - 住所フィールドを複数のフィールド (**address1**、 など**address2**) または 1 つのフィールドに指定します。
>
>   アドレスと照合する場合は、郵便番号が必要です。
> - 名前に E メールまたは電話を含めると、それらのフィールドは住所と照合できます。

b. [次へ] をクリックします。

6. ステップ 3: データ をグループ化するには、次の手順を実行します。

   a. 関連する名前フィールドを選択し、グループ名と一致キー を入力します。

      Example

      例えば、入力フィールド **First name**、、**Middle name**および を選択し**Last name**、**Full name**「」というグループ名と「」という一致キーを入力して比較**Full name**を有効にします。

   b. 関連するアドレスフィールドを選択し、グループ名 と一致キー を入力します。

      Example

      例えば、入力フィールド **Home street address 1**、、**Home street address 2**および を選択し**Home city**、**Shipping address**「」というグループ名と「」という一致キーを入力して比較**Shipping address**を有効にします。

   c. 関連する電話番号フィールドを選択し、グループ名 と一致キー を入力します。

Example

例えば、入力フィールド **Home phone 1**、、**Home phone 2**および を選択し**Cell phone**、**Shipping phone number**「」というグループ名と「」という一致キーを入力して比較**Shipping phone number**を有効にします。

複数のタイプのデータがある場合は、さらにグループを追加できます。

d. [次へ] をクリックします。

7. ステップ 4: を確認して作成するには、次の手順を実行します。

a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

b. スキーママッピングの作成 を選択します。

> **Note**
>
> スキーママッピングをワークフローに関連付けた後は変更できません。既存の設定を使用して新しいスキーママッピングを作成する場合は、スキーママッピングのクローンを作成できます。

スキーママッピングを作成したら、一致するワークフローを作成するか、ID 名前空間 を作成する準備が整います。

スキーママッピングを作成する (手動で定義された列)

この手順では、AWS Entity Resolution コンソール のカスタムスキーマの構築オプションを使用してスキーママッピングを作成するプロセスについて説明します。この作成方法を使用して、ガイド付きフローを使用して入力フィールドを手動で定義します。

手動で定義された列を使用してスキーママッピングを作成するには

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのデータ準備 で、スキーママッピング を選択します。
3. スキーママッピング ページの右上隅で、スキーママッピングの作成 を選択します。
4. ステップ 1: スキーマの詳細を指定するには、次の手順を実行します。

a. 名前と作成方法には、スキーママッピング名とオプションの説明 を入力します。

b. 作成方法 で、カスタムスキーマの構築 を選択します。

c. 一意の ID には、一意の ID を入力してデータの各行を識別します。

Example

たとえば、**`Primary_key`**、**`Row_ID`**、または **`Record_ID`** などです。

> **Note**
>
> 一意の ID 列は必須です。一意の ID は、単一のテーブル内の一意の識別子である必要があります。ただし、異なるテーブル間では、一意の ID に重複する値を含めることができます。一意の ID が指定されていない場合、同じソース内で一意でない場合、またはソース間で属性名の点で重複している場合 AWS Entity Resolution 、は一致するワークフローの実行時にレコードを拒否します。

d. (オプション) リソースのタグを有効にする場合は、新しいタグを追加 を選択し、キーと値のペアを入力します。

e. [次へ] をクリックします。

5. ステップ 2: 入力フィールド をマッピングするには、次の手順を実行します。

a. を照合するための入力フィールドには、入力フィールド 、入力タイプ 、一致キー を追加します。

最大 25 個の入力フィールドを追加できます。

入力タイプは、データを分類するのに役立ちます。一致キーを使用すると、入力フィールドを一致するワークフローと比較できます。

> **Note**
>
> LiveRamp プロバイダーのサービスベースのマッチング手法で使用するスキーママッピングを作成する場合は、入力タイプを LiveRamp ID として指定できます。出力に PII データを含める場合は、入力タイプをカスタム文字列 として指定する必要があります。

b. (オプション) パススルー の入力フィールドに、一致しない入力フィールドを追加します。

c. [次へ] をクリックします。

6. ステップ 3: データ をグループ化する：

a. 関連する名前フィールドを選択し、グループ名 と一致キー を入力します。

Example

例えば、入力フィールド **First name**、、**Middle name**および を選択し**Last name**、**Full name**「」というグループ名と「」という一致キーを入力して比較**Full name**を有効にします。

b. 関連するアドレスフィールドを選択し、グループ名 と一致キー を入力します。

Example

例えば、入力フィールド **Home street address 1**、、**Home street address 2**および を選択し**Home city**、**Shipping address**「」というグループ名と「」という一致キーを入力して比較**Shipping address**を有効にします。

c. 関連する電話番号フィールドを選択し、グループ名 と一致キー を入力します。

Example

例えば、入力フィールド **Home phone 1**、、**Home phone 2**および を選択し**Cell phone**、**Shipping phone number**「」というグループ名と「」という一致キーを入力して比較**Shipping phone number**を有効にします。

複数のタイプのデータがある場合は、さらにグループを追加できます。

d. [次へ] をクリックします。

7. ステップ 4: を確認して作成するには、次の手順を実行します。

a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

b. スキーママッピングの作成 を選択します。

> **Note**
>
> スキーママッピングをワークフローに関連付けた後は、スキーママッピングを変更することはできません。既存の設定を使用して新しいスキーママッピングを作成する場合は、スキーママッピングのクローンを作成できます。

スキーママッピングを作成したら、一致するワークフローを作成するか、ID 名前空間 を作成する準備が整います。

スキーママッピングを作成する (JSON エディタ)

この手順では、AWS Entity Resolution コンソール で JSON エディタを使用するオプションを使用してスキーママッピングを作成するプロセスについて説明します。この作成方法を使用して、JSON エディタを使用してスキーママッピングを作成、貼り付け、またはインポートします。このオプションでは、一意の ID フィールドと入力フィールドは使用できません。

JSON エディタを使用してスキーママッピングを作成するには

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのデータ準備 で、スキーママッピング を選択します。
3. スキーママッピング ページの右上隅で、スキーママッピングの作成 を選択します。
4. ステップ 1: スキーマの詳細を指定するには、次の手順を実行します。
   a. 名前と作成方法には、スキーママッピング名とオプションの説明を入力します。
   b. 作成方法 で、JSON エディタ を使用する を選択します。
   c. (オプション) リソースのタグを有効にする場合は、新しいタグを追加 を選択し、キーと値のペアを入力します。
   d. [次へ] をクリックします。
5. ステップ 2: マッピング を指定する :
   a. JSON エディタでスキーマの構築を開始するか、次のいずれかのオプションを選択します。

目的	選択内容
スキーママッピングの構築を開始する	サンプル JSON を挿入し、必要に応じて情報を編集します。
既存の JSON ファイルを使用する	ファイルからインポート

   b. [次へ] をクリックします。
6. ステップ 3: を確認して作成する :

a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

b. スキーママッピングの作成 を選択します。

> **Note**
>
> スキーママッピングをワークフローに関連付けた後は、スキーママッピングを変更することはできません。既存の設定を使用して新しいスキーママッピングを作成する場合は、スキーママッピングのクローンを作成できます。

スキーママッピングを作成したら、一致するワークフローを作成するか、ID 名前空間 を作成する準備が整います。

一致するワークフローの作成

スキーママッピングを作成したら、一致するワークフローを 1 つ以上作成して、データ入力、正規化ステップを指定し、目的のマッチング手法を選択できます。一致する手法は 3 つあります。

- ルールベースのマッチングは、入力したデータに基づいて によって提案されるウォーターフォールマッチングルールの階層セットであり AWS Entity Resolution、ユーザーが完全に設定できます。
- 機械学習ベースのマッチングは、入力したすべてのデータにわたってレコードのマッチングを試みるプリセットプロセスです。
- プロバイダーサービスを使用すると、既知の識別子を任意のデータサービスプロバイダーと照合できます。

  AWS Entity Resolution は現在、、 LiveRamp TransUnion、および UID 2.0 のデータサービスプロバイダーと統合されています。これらのプロバイダーのパブリックサブスクリプションを で使用する AWS Data Exchange か、プライベートオファーをデータプロバイダーと直接ネゴシエートできます。詳細については、「でプロバイダーサービスをサブスクライブする AWS Data Exchange」を参照してください。

AWS Entity Resolution は、ユーザーが指定した場所からデータを読み取り、選択した場所に結果を書き込みます (複数可) 。必要に応じて AWS Entity Resolution を使用して出力データをハッシュできるため、データの制御を維持できます。

また、ルールベースまたは ML マッチングの出力を、プロバイダーのサービスベースのマッチングへの入力として使用したり、ビジネスニーズを満たすための別の方法として使用することもできます。例えば、最初にルールベースのマッチングを実行してデータに対する一致を検索し、次に一致しないレコードのサブセットをプロバイダーのサービスベースのマッチングに送信して、プロバイダーのサブスクリプションコストを節約できます。

トピック

- ルールベースのマッチングワークフローを作成する
- 機械学習ベースのマッチングワークフローを作成する
- プロバイダーのサービスベースのマッチングワークフローを作成する
- 一致するワークフローを実行する
- 次のステップ

ルールベースのマッチングワークフローを作成する

ルールベースのマッチングワークフローでは、クリアテキストデータまたはハッシュデータを比較して、カスタマイズした基準に基づいて完全一致を見つけることができます。

がデータ内の 2 つ以上のレコード間の一致 AWS Entity Resolution を検出すると、一致したデータセット内のレコードに一致 ID が割り当てられます。

ルールベースのマッチングでは、一致を生成したルール番号が適用されます。

ルールベースのマッチングワークフローを作成するには：

1. にサインイン AWS Management Console し、 でAWS Entity Resolution コンソールを開きますAWS アカウント（まだ開いていない場合）。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. マッチングワークフローページの右上隅で、マッチングワークフローの作成を選択します。
4. ステップ 1: 一致するワークフローの詳細を指定するには、以下を実行します。

   a. 一致するワークフロー名とオプションの説明を入力します。

   b. データ入力 で、ドロップダウンからAWS Glue データベースを選択し、AWS Glue テーブル を選択し、対応するスキーママッピング を選択します。

      最大 19 個のデータ入力を追加できます。

   c. データの正規化オプションはデフォルトで選択され、一致する前にデータ入力が正規化されます。データを正規化しない場合は、データの正規化オプションの選択を解除します。

   d. [新しいサービスロールを作成して使用] または [既存のサービスロールを使用] を選択して、[サービスアクセス] 許可を指定します。

選択した場合	THEN
新しいサービスロールを作成して使用	• AWS Entity Resolution は、このテーブルに必要なポリシーを持つサービスロールを作成します。 • デフォルトの [サービスロール名] は `entityresolution-`

選択した場合	THEN
	`matching-workflow-<timestamp>` です。 • ロールを作成してポリシーをアタッチするアクセス許可が必要です。 • 入力データが暗号化されている場合は、KMS キーオプションで暗号化されたデータを選択し、データ入力の復号に使用される AWS KMS キーを入力できます。

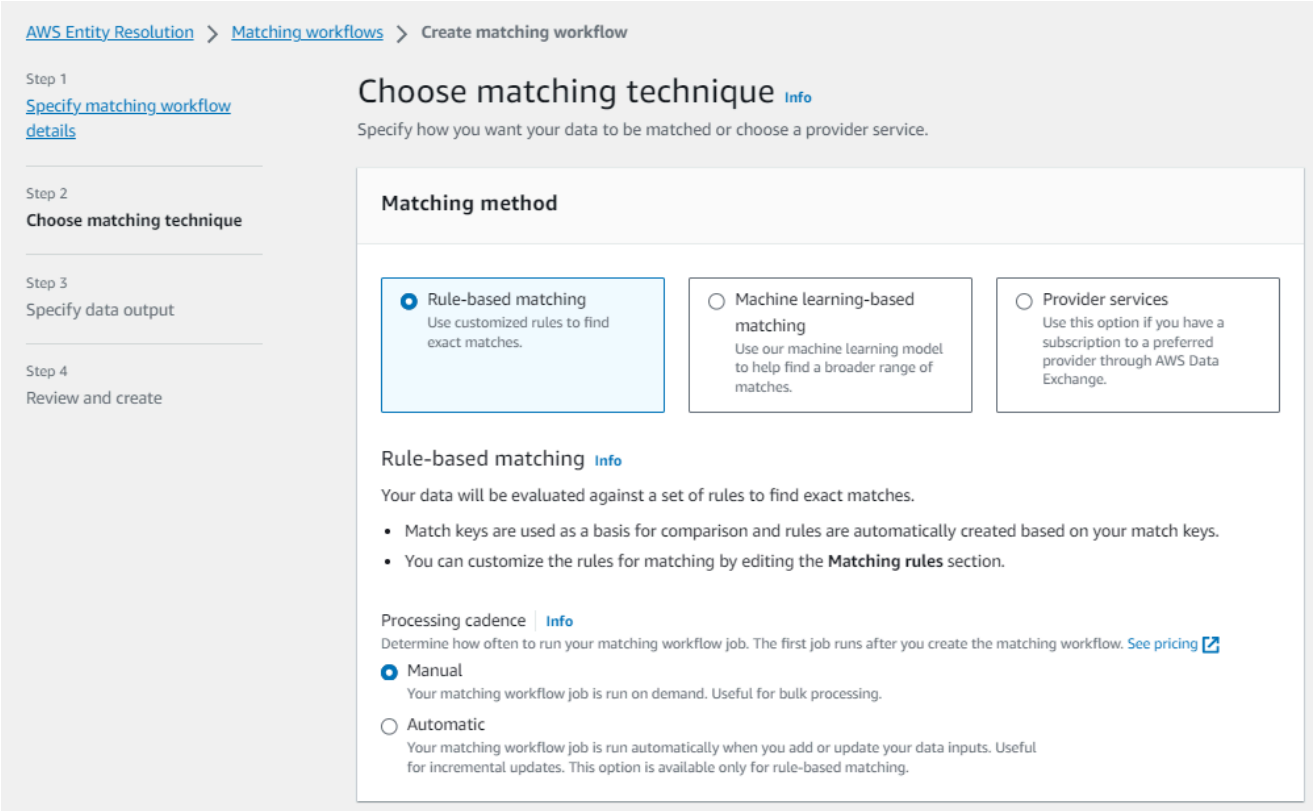
選択した場合	THEN
既存のサービスロールを使用	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. IAM 外部リンクで表示を選択して、サービスロールを表示します。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必要なアクセス許可を追加しようとしません。

e. （オプション) リソースのタグを有効にするには、新しいタグの追加 を選択し、キーと値のペアを入力します。

f. [次へ] をクリックします。

5. ステップ 2: 一致する手法を選択する：

   a. マッチング方法 で、ルールベースのマッチング を選択します。



b. 処理ケイデンス で、次のいずれかを選択します。

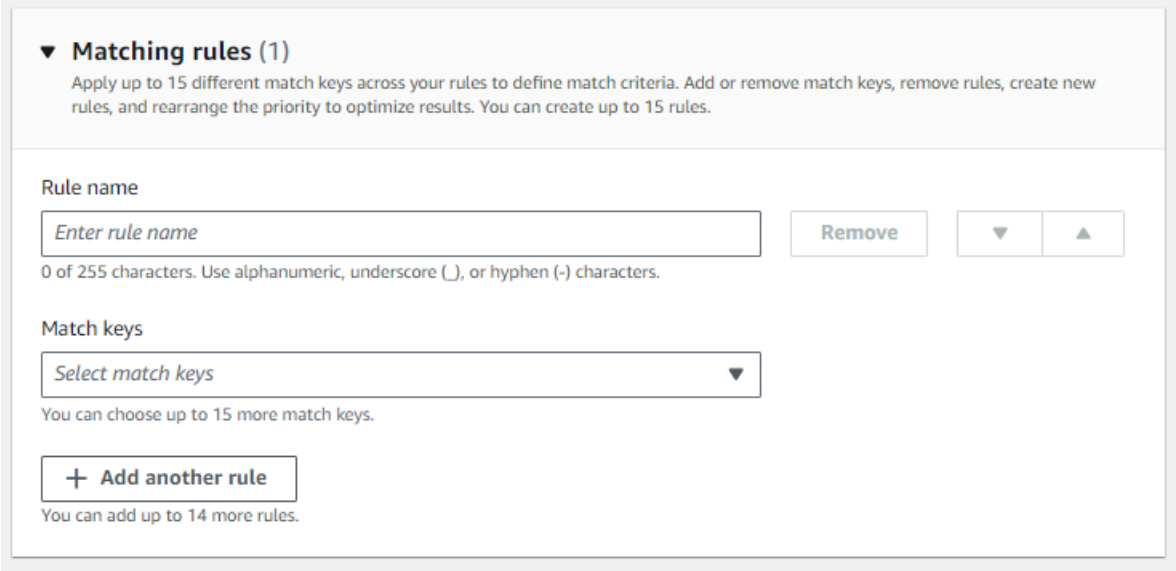
目的	選択内容
一括更新のワークフローをオンデマンドで実行する	手動
新しいデータが S3 バケットに保存されたらすぐにワークフローを実行する	自動

> **Note**
>
> 自動 を選択した場合は、S3 バケットに対して Amazon EventBridge 通知が有効になっていることを確認します。S3 コンソール EventBridge を使用して Amazon を有効にする手順については、「Amazon S3 EventBridgeユーザーガイド」のAmazon S3」を参照してください。

c. 一致ルール にルール名を入力し、そのルールの一致キーを選択します。

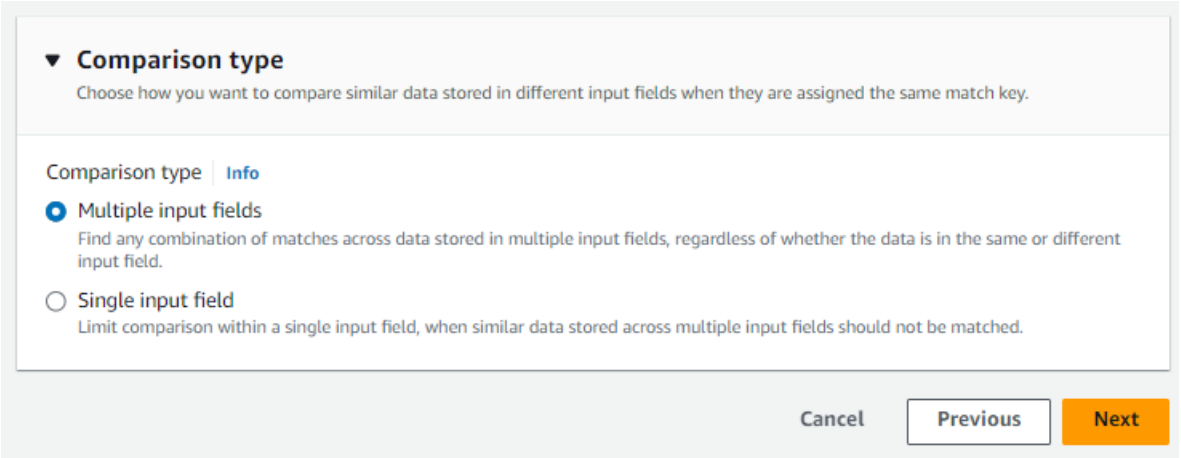
ルール全体に最大 15 の異なる一致キーを適用して、一致条件を定義できます。

最大 15 個のルールを作成できます。



d. 比較タイプ で、次のいずれかを選択します。

目的	選択内容
複数の入力フィールドに保存されているデータ間で一致の任意の組み合わせを検索する	複数の入力フィールドの比較
比較を単一の入力フィールドに制限する	単一入力フィールドの比較



e. [次へ] をクリックします。

6. ステップ 3: データ出力と形式を指定する :

   a. データ出力の送信先と形式 で、データ出力の Amazon S3 の場所と、データ形式を正規化されたデータか元のデータかを選択します。

   b. 暗号化 で、暗号化設定 をカスタマイズする場合は、AWS KMS キー ARN を入力します。

   c. システム生成の出力 を表示します。

   d. データ出力 には、含まれているすべてのフィールドを表示します。

   e. フィールドを含めるか、非表示にするか、マスクするかを決定します。

目的	選択内容
フィールドを含める	出力状態は「Included」のままにします。
フィールドを非表示にする (出力から除外)	出力フィールド を選択し、 を非表示 を選択します。
マスクフィールド	出力フィールド を選択し、ハッシュ出力 を選択します。
以前の設定をリセットする	[リセット] を選択します。

   f. [次へ] をクリックします。

7. ステップ 4: を確認して作成する :

a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

b. Create and run を選択します。

一致するワークフローが作成され、ジョブが開始されたことを示すメッセージが表示されます。

8. 一致するワークフローの詳細ページのメトリクスタブで、「最後のジョブメトリクス」で以下を表示します。

- ジョブ ID 。
- 一致するワークフロージョブのステータス: Queued 、In progress 、Completed 、Failed
- ワークフロージョブの完了時刻。
- 処理されたレコードの数。
- 処理されなかったレコードの数。
- 生成された一意の一致 IDs。
- 入力レコードの数。

ジョブ履歴 で以前に実行されたワークフロージョブを照合するためのジョブメトリクスを表示することもできます。

9. 一致するワークフロージョブが完了した後 (ステータスは完了) 、データ出力タブに移動し、Amazon S3 の場所を選択して結果を表示できます。

これで次の作業に進むことができます。

- 一致するワークフローを編集する
- 一致するワークフローを削除する
- 一致するワークフローを実行する

機械学習ベースのマッチングワークフローを作成する

機械学習ベースのマッチングワークフローを使用すると、クリアテキストデータを比較して、機械学習モデルを使用して幅広いマッチングを見つけることができます。

> **Note**
>
> 機械学習モデルは、ハッシュ化されたデータの比較をサポートしていません。

がデータ内の 2 つ以上のレコード間の一致 AWS Entity Resolution を検出すると、一致したデータセット内のレコードに一致 ID が割り当てられます。

機械学習ベースのマッチングでは、一致信頼度の割合が適用されます。

ML ベースのマッチングワークフローを作成するには：

1. にサインイン AWS Management Console し、 でAWS Entity Resolution コンソールを開きますAWS アカウント（まだ開いていない場合）。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. マッチングワークフローページの右上隅で、マッチングワークフローの作成を選択します。
4. ステップ 1: 一致するワークフローの詳細を指定するには、次の手順を実行します。

   a. 一致するワークフロー名とオプションの 説明を入力します。

   b. データ入力 で、ドロップダウンからAWS Glue データベースを選択し、AWS Glue テーブル を選択し、対応するスキーママッピング を選択します。

      最大 20 個のデータ入力を追加できます。

   c. データの正規化オプションはデフォルトで選択され、一致する前にデータ入力が正規化されます。データを正規化しない場合は、データの正規化オプションの選択を解除します。

   d. [新しいサービスロールを作成して使用] または [既存のサービスロールを使用] を選択して、[サービスアクセス] 許可を指定します。

選択した場合	THEN
新しいサービスロールを作成して使用	• AWS Entity Resolution は、このテーブルに必要なポリシーを持つサービスロールを作成します。 • デフォルトの [サービスロール名] は `entityresolution-`

選択した場合	THEN
	`matching-workflow-<timestamp>` です。 • ロールを作成してポリシーをアタッチするアクセス許可が必要です。 • 入力データが暗号化されている場合は、KMS キーオプションで暗号化されたデータを選択し、データ入力の復号に使用される AWS KMS キーを入力できます。

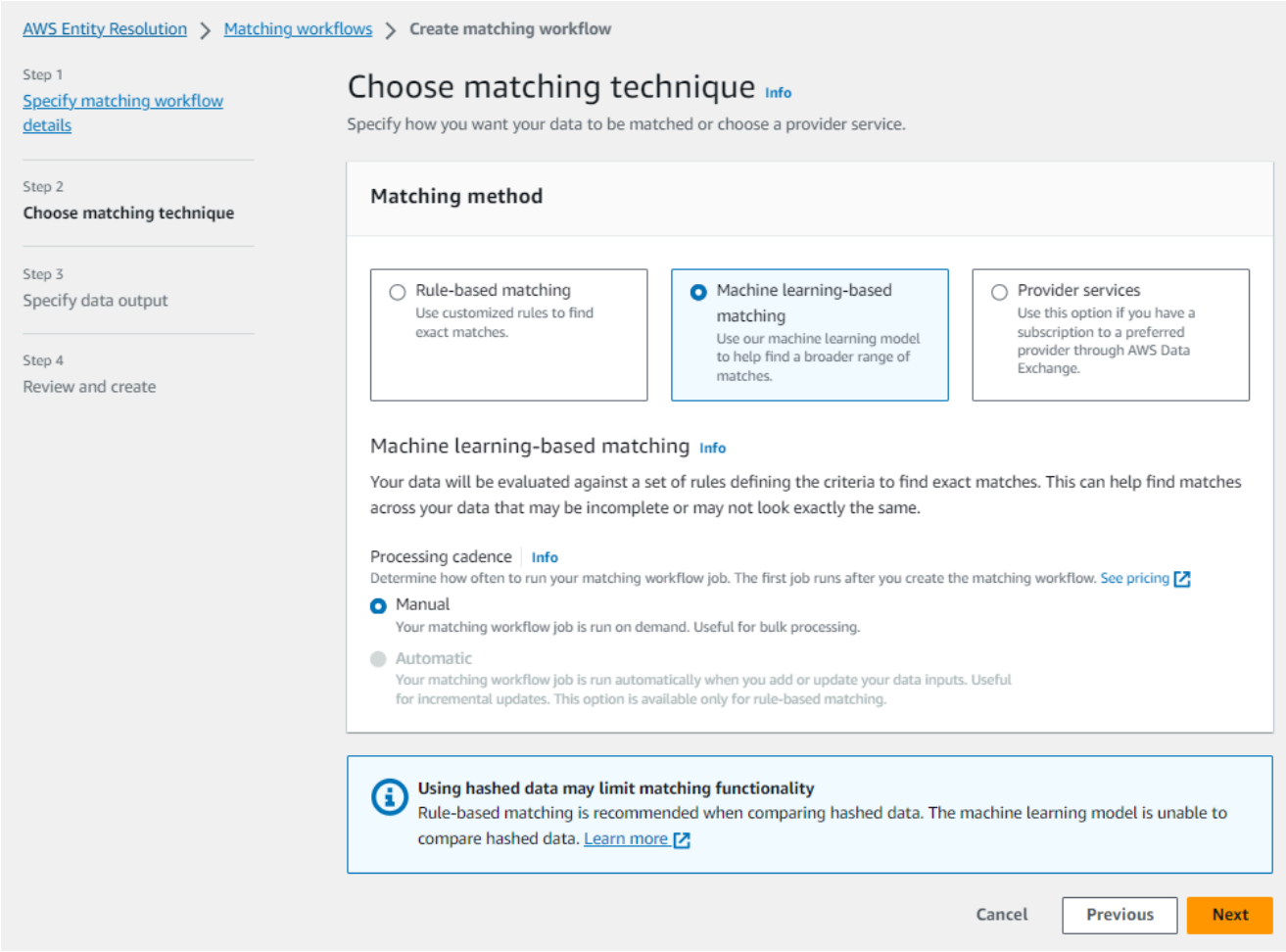
選択した場合	THEN
既存のサービスロールを使用	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. IAM 外部リンクで表示を選択して、サービスロールを表示します。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必要なアクセス許可を追加しようとしません。

e. （オプション) リソースのタグを有効にするには、新しいタグを追加 を選択し、キーと値のペアを入力します。

f. [次へ] をクリックします。

5. ステップ 2: 一致する手法を選択する：

   a. マッチング方法 で、機械学習ベースのマッチング を選択します。



b. 処理ケイデンス では、手動 オプションが選択されています。

このオプションを使用すると、一括更新のワークフローをオンデマンドで実行できます。

c. [次へ] をクリックします。

6. ステップ 3: データ出力と形式を指定する :

a. データ出力の送信先と形式 で、データ出力の Amazon S3 の場所と、データ形式を正規化データまたは元のデータのどちらにするかを選択します。

b. 暗号化 で、暗号化設定 をカスタマイズする場合は、AWS KMS キー ARN を入力します。

c. システム生成の出力 を表示します。

d. データ出力 には、含まれているすべてのフィールドを表示します。

e. フィールドを含めるか、非表示にするか、マスクするかを決定します。

目的	選択内容
フィールドを含める	出力状態は「Included」のままにします。
フィールドを非表示にする (出力から除外)	出力フィールド を選択し、 を非表示 を選択します。
マスクフィールド	出力フィールド を選択し、ハッシュ出力 を選択します。
以前の設定をリセットする	[リセット] を選択します。

f. [次へ] をクリックします。

7. ステップ 4: を確認して作成する：

a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

b. Create and run を選択します。

一致するワークフローが作成され、ジョブが開始されたことを示すメッセージが表示されます。

8. 一致するワークフローの詳細ページのメトリクスタブで、「最後のジョブメトリクス」で以下を表示します。

- ジョブ ID 。
- 一致するワークフロージョブのステータス: Queued 、In progress 、Completed 、Failed
- ワークフロージョブの完了時刻。
- 処理されたレコードの数。
- 処理されなかったレコードの数。
- 生成された一意の一致 IDs。
- 入力レコードの数。

ジョブ履歴 で以前に実行されたワークフロージョブを照合するためのジョブメトリクスを表示することもできます。

9. 一致するワークフロージョブが完了した後 (ステータスは完了) 、データ出力タブに移動し、Amazon S3 の場所を選択して結果を表示できます。

これで次の作業に進むことができます。

- 一致するワークフローを編集する
- 一致するワークフローを削除する
- 一致するワークフローを実行する

プロバイダーのサービスベースのマッチングワークフローを作成する

を通じてプロバイダーサービスのサブスクリプションをお持ちの場合は AWS Data Exchange、既知の識別子を優先プロバイダーと照合できます。 AWS Entity Resolution は現在、次のデータプロバイダーサービスをサポートしています。

- LiveRamp
- TransUnion
- 統合 ID 2.0

新しいサブスクリプションの作成またはプロバイダーサービスへの既存のサブスクリプションの再利用の詳細については、「」を参照してくださいでプロバイダーサービスをサブスクライブする AWS Data Exchange。

以下のセクションでは、プロバイダーベースのマッチングワークフローを作成する方法について説明します。

トピック

- を使用した一致するワークフローの作成 LiveRamp
- を使用した一致するワークフローの作成 TransUnion
- UID 2.0 を使用したマッチングワークフローの作成

を使用した一致するワークフローの作成 LiveRamp

LiveRamp サービスにサブスクリプションしている場合は、 サービスで一致するワークフローを作成して ID LiveRamp解決を実行できます。

この LiveRamp サービスは、RampID と呼ばれる識別子を提供します。RampID は、広告キャンペーンのオーディエンスを作成するために需要側プラットフォームで最も一般的に使用される IDs の 1 つです。で一致するワークフローを使用すると LiveRamp、ハッシュ化された E メールアドレスを RAMPIDsに解決できます。

> **Note**
>
> AWS Entity Resolution は PII ベースの RampID 割り当てをサポートします。

このワークフローには、一致するワークフロー出力を一時的に書き込む Amazon S3 データステージングバケットが必要です。を使用して ID マッピングワークフローを作成する前に LiveRamp、データステージングバケットに次のアクセス許可を追加します。

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

各 ################ を独自の情報に置き換えます。

##########	プロバイダーのサービスベースのワークフローの実行中にデータを一時的に保存する Amazon S3 バケット。

を使用して一致するワークフローを作成するには LiveRamp :

1. にサインイン AWS Management Console し、 でAWS Entity Resolution コンソールを開きますAWS アカウント （ まだ開いていない場合 ）。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. マッチングワークフローページの右上隅で、マッチングワークフローの作成を選択します。
4. ステップ 1: 一致するワークフローの詳細を指定するには、次の手順を実行します。

    a. 一致するワークフロー名とオプションの説明 を入力します。

    b. データ入力 で、ドロップダウンからAWS Glue データベースを選択し、AWS Glue テーブル を選択し、対応するスキーママッピング を選択します。

    最大 20 個のデータ入力を追加できます。

    c. データの正規化オプションはデフォルトで選択され、一致する前にデータ入力が正規化されます。

E メールのみの解決プロセスを使用している場合は、データの正規化オプションの選択を解除します。これは、ハッシュ化された E メールのみが入力データに使用されるためです。

d. [新しいサービスロールを作成して使用] または [既存のサービスロールを使用] を選択して、[サービスアクセス] 許可を指定します。

選択した場合	THEN
新しいサービスロールを作成して使用	• AWS Entity Resolution は、このテーブルに必要なポリシーを持つサービスロールを作成します。 • デフォルトの [サービスロール名] は `entityresolution-matching-workflow-<timestamp>` です。 • ロールを作成してポリシーをアタッチするアクセス許可が必要です。 • 入力データが暗号化されている場合は、KMS キーオプションで暗号化されたデータを選択し、データ入力の復号に使用される AWS KMS キーを入力できます。

選択した場合	THEN
既存のサービスロールを使用	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. IAM 外部リンクで表示を選択して、サービスロールを表示します。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必要なアクセス許可を追加しようとしません。

e. （オプション) リソースのタグを有効にするには、新しいタグの追加 を選択し、キーと値のペアを入力します。

f. [次へ] をクリックします。

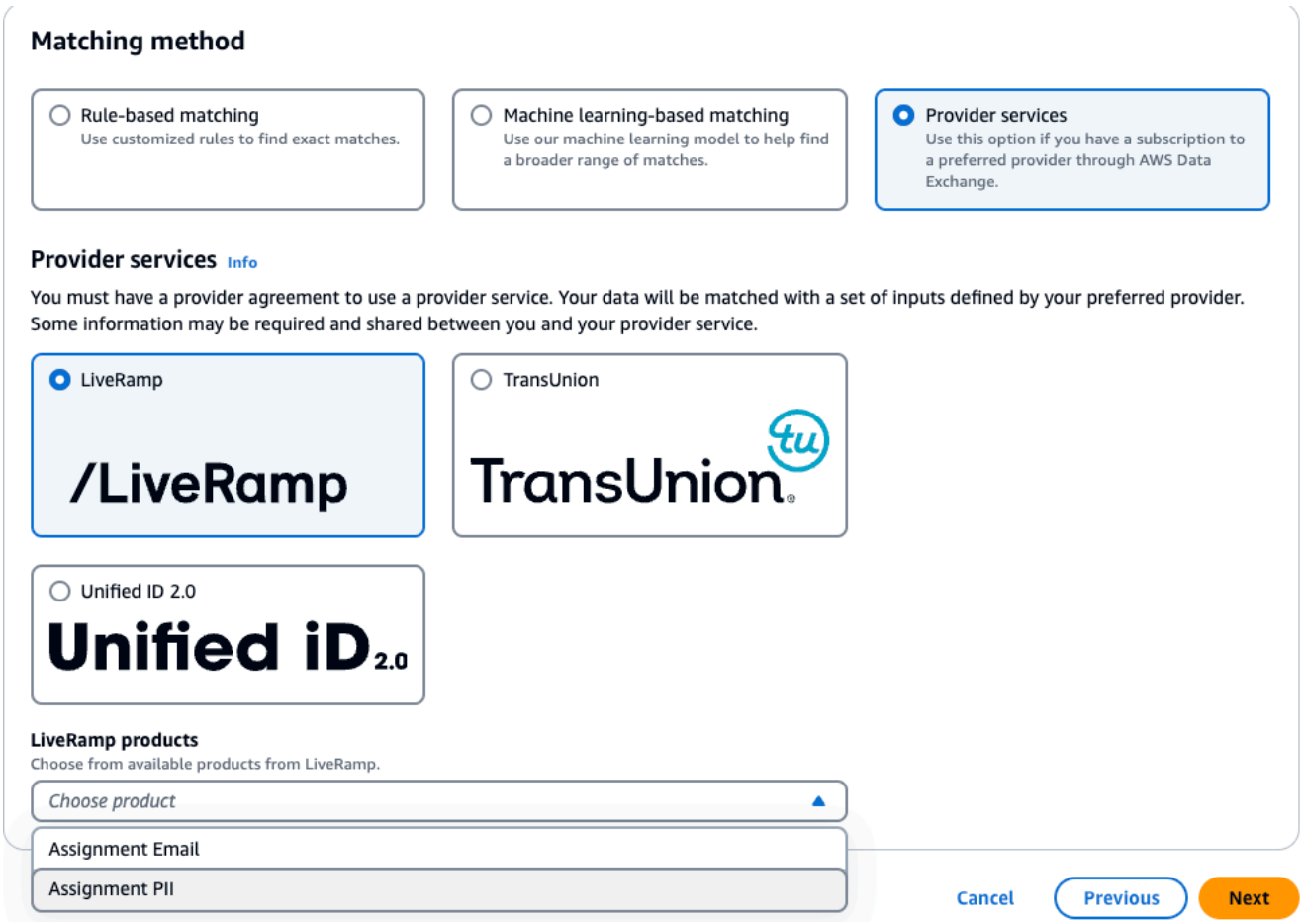
5. ステップ 2: 一致する手法を選択する：

a. マッチング方法 で、プロバイダーサービス を選択します。

b. プロバイダーサービス で、 を選択しますLiveRamp。

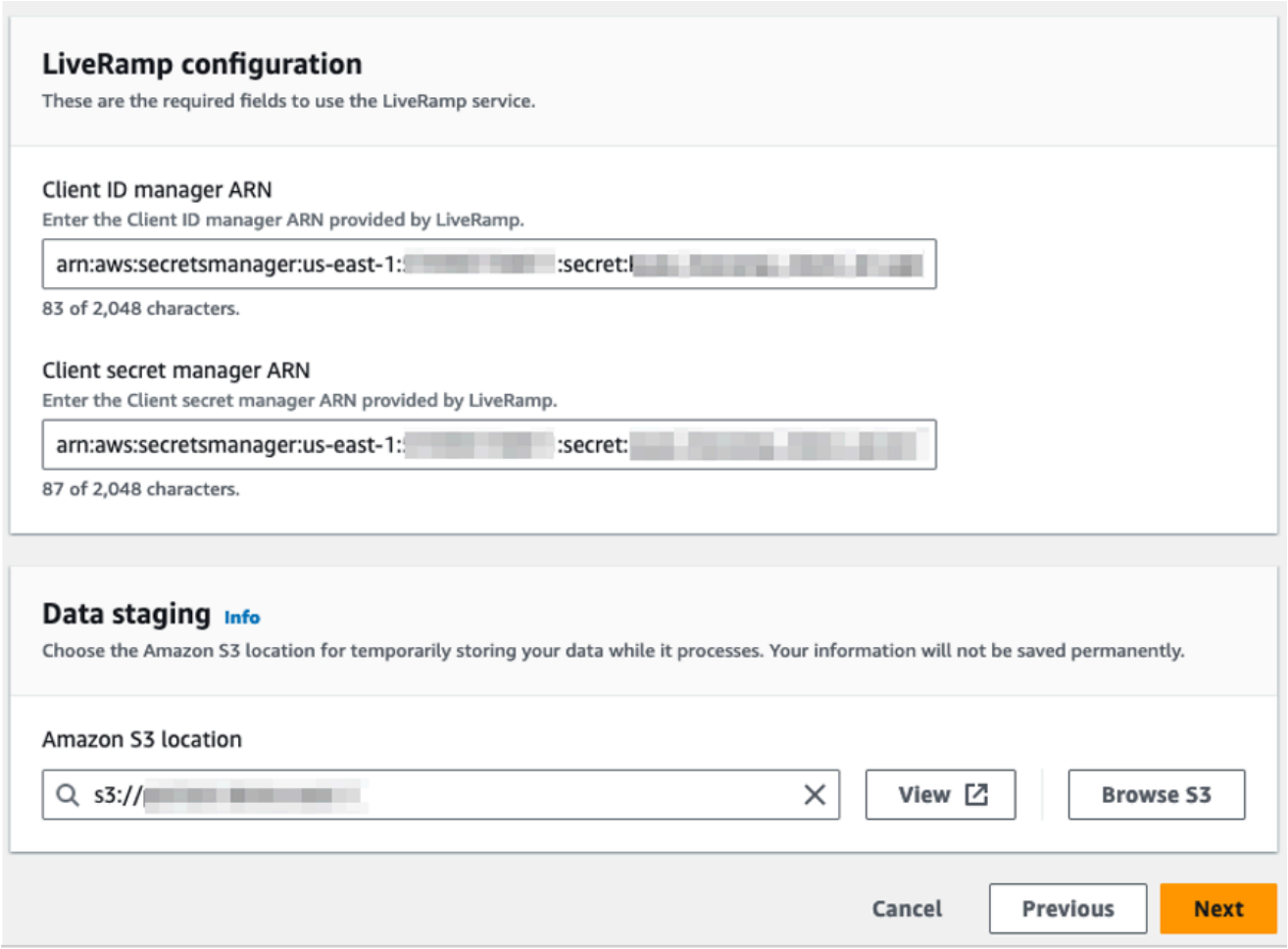
> **Note**
>
> データ入力ファイルの形式と正規化がプロバイダーサービスのガイドラインと一致していることを確認します。
> マッチングワークフローの入力ファイルフォーマットガイドラインの詳細については、 LiveRamp ドキュメントの「ADX によるアイデンティティ解決の実行」を参照してください。

c. LiveRamp 製品 の場合、ドロップダウンリストから製品を選択します。



> **Note**
>
> PII の割り当てを選択した場合は、エンティティ解決を実行するときに、少なくとも 1 つの非識別子列を指定する必要があります。例えば、GENDER などです。

d. LiveRamp 設定 には、クライアント ID マネージャー ARN とクライアントシークレットマネージャー ARN を入力します。



e. データステージング では、処理中のデータの一時ストレージ用の Amazon S3 の場所を選択します。

データステージング Amazon S3 の場所 に対するアクセス許可が必要です。詳細については、「the section called “のワークフロージョブロールを作成する AWS Entity Resolution”」を参照してください。

f. [Next] (次へ) を選択します。

6. ステップ 3: データ出力 を指定します。

a. データ出力の送信先と形式 で、データ出力の Amazon S3 の場所と、データ形式を正規化されたデータか元のデータかを選択します。

b. 暗号化 で、暗号化設定 をカスタマイズする場合は、AWS KMS キー ARN を入力します。

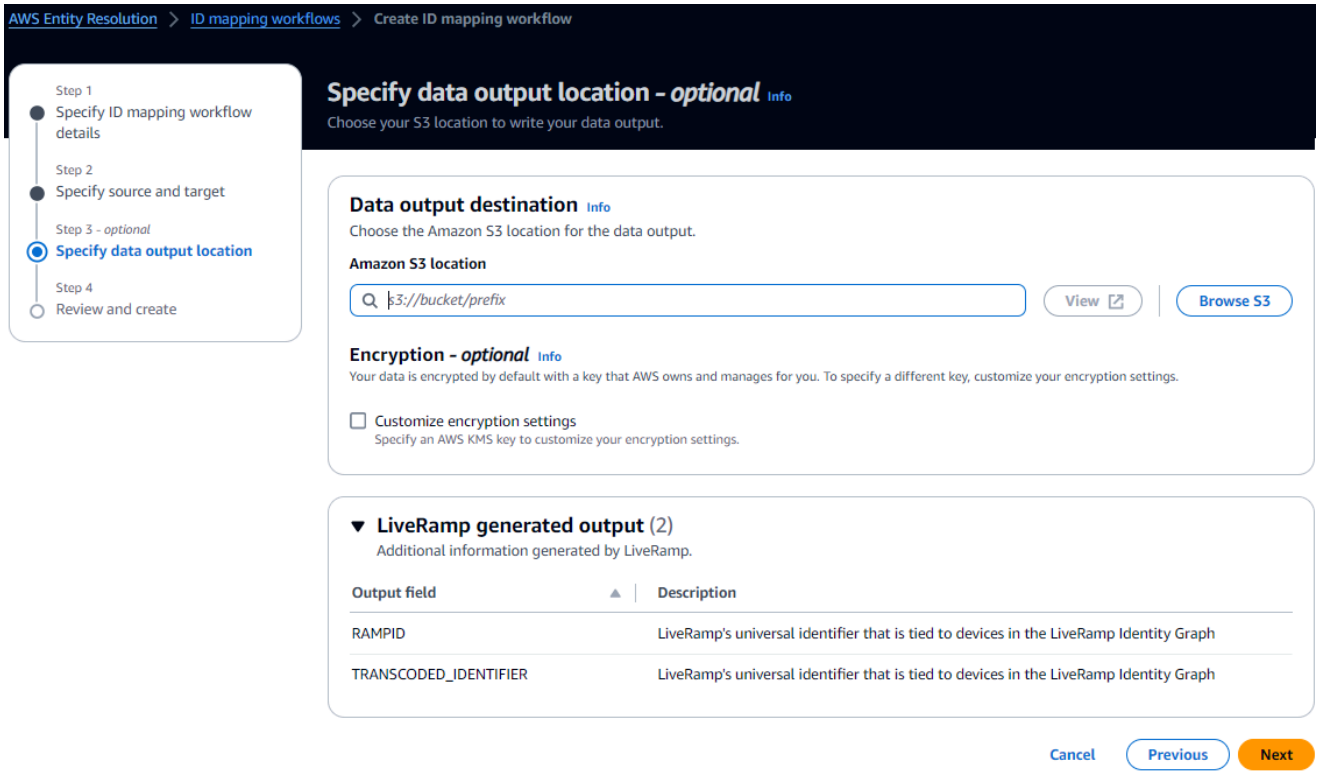
c. LiveRamp 生成された出力 を表示します。

これは、 によって生成された追加情報です LiveRamp。

d. データ出力 では、含まれているすべてのフィールドを表示し、フィールドを含めるか、非表示にするか、マスクするかを決定します。

> **Note**
>
> を選択した場合LiveRamp、個人を特定できる情報 (PII) を削除する LiveRamp プライバシーフィルターにより、一部のフィールドには出力状態が利用不可 と表示されます。

目的	選択内容
フィールドを含める	出力状態は、Included のままにします。
フィールドを非表示にする (出力から除外)	出力フィールド を選択し、 を非表示 を選択します。
マスクフィールド	出力フィールド を選択し、ハッシュ出力 を選択します。
以前の設定をリセットする	[リセット] を選択します。



e. [次へ] をクリックします。

7. ステップ 4: を確認して作成する :

   a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

   b. Create and run を選択します。

      一致するワークフローが作成され、ジョブが開始されたことを示すメッセージが表示されます。

8. 一致するワークフローの詳細ページのメトリクスタブで、「最後のジョブメトリクス」で以下を表示します。

   - ジョブ ID 。
   - 一致するワークフロージョブのステータス: キューに入れられた 、進行中 、完了した 、失敗
   - ワークフロージョブの完了時刻。
   - 処理されたレコードの数。
   - 処理されなかったレコードの数。
   - 生成された一意の一致 IDs。
   - 入力レコードの数。

ジョブ履歴 で以前に実行されたワークフロージョブを照合するためのジョブメトリクスを表示することもできます。

9. 一致するワークフロージョブが完了した後 (ステータスが完了) 、データ出力タブに移動し、Amazon S3 の場所を選択して結果を表示できます。

これで次の作業に進むことができます。

- 一致するワークフローを編集する
- 一致するワークフローを削除する

を使用した一致するワークフローの作成 TransUnion

TransUnion サービスのサブスクリプションをお持ちの場合は、さまざまなチャネルに保存された顧客関連レコードを TransUnion Person and Familyhold E Keys と 200 を超えるデータ属性とリンク、マッチング、強化することで、顧客の理解を向上させることができます。

この TransUnion サービスは、 TransUnion 個人 ID および世帯 IDs。 TransUnion は、名前、住所、電話番号、E メールアドレスなどの既知の識別子の ID 割り当て (エンコードとも呼ばれます) を提供します。

このワークフローには、一致するワークフロー出力を一時的に書き込む Amazon S3 データステージングバケットが必要です。で一致するワークフローを作成する前に TransUnion、データステージングバケットに次のアクセス許可を追加します。

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

各 ################ を独自の情報に置き換えます。

##########	プロバイダーのサービスベースのワークフローの実行中にデータを一時的に保存する Amazon S3 バケット。

を使用して一致するワークフローを作成するには TransUnion：

1. にサインイン AWS Management Console し、 でAWS Entity Resolution コンソールを開きますAWS アカウント（まだ開いていない場合）。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. マッチングワークフローページの右上隅で、マッチングワークフローの作成 を選択します。
4. ステップ 1: 一致するワークフローの詳細を指定するには、次の手順を実行します。

a. 一致するワークフロー名とオプションの説明を入力します。

b. データ入力 で、ドロップダウンからAWS Glue データベースを選択し、AWS Glue テーブル を選択し、対応するスキーママッピング を選択します。

   最大 20 個のデータ入力を追加できます。

c. データの正規化オプションはデフォルトで選択され、一致する前にデータ入力が正規化されます。データを正規化しない場合は、データの正規化オプションの選択を解除します。

d. [新しいサービスロールを作成して使用] または [既存のサービスロールを使用] を選択して、[サービスアクセス] 許可を指定します。

選択した場合	THEN
新しいサービスロールを作成して使用	• AWS Entity Resolution は、このテーブルに必要なポリシーを持つサービスロールを作成します。 • デフォルトの [サービスロール名] は `entityresolution-matching-workflow-<timestamp>` です。 • ロールを作成してポリシーをアタッチするアクセス許可が必要です。 • 入力データが暗号化されている場合は、KMS キーオプションで暗号化されたデータを選択し、データ入力の復号に使用される AWS KMS キーを入力できます。

選択した場合	THEN
既存のサービスロールを使用	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. IAM 外部リンクで表示を選択して、サービスロールを表示します。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必要なアクセス許可を追加しようとしません。

e. （オプション) リソースのタグを有効にするには、新しいタグの追加 を選択し、キーと値のペアを入力します。

f. [次へ] をクリックします。

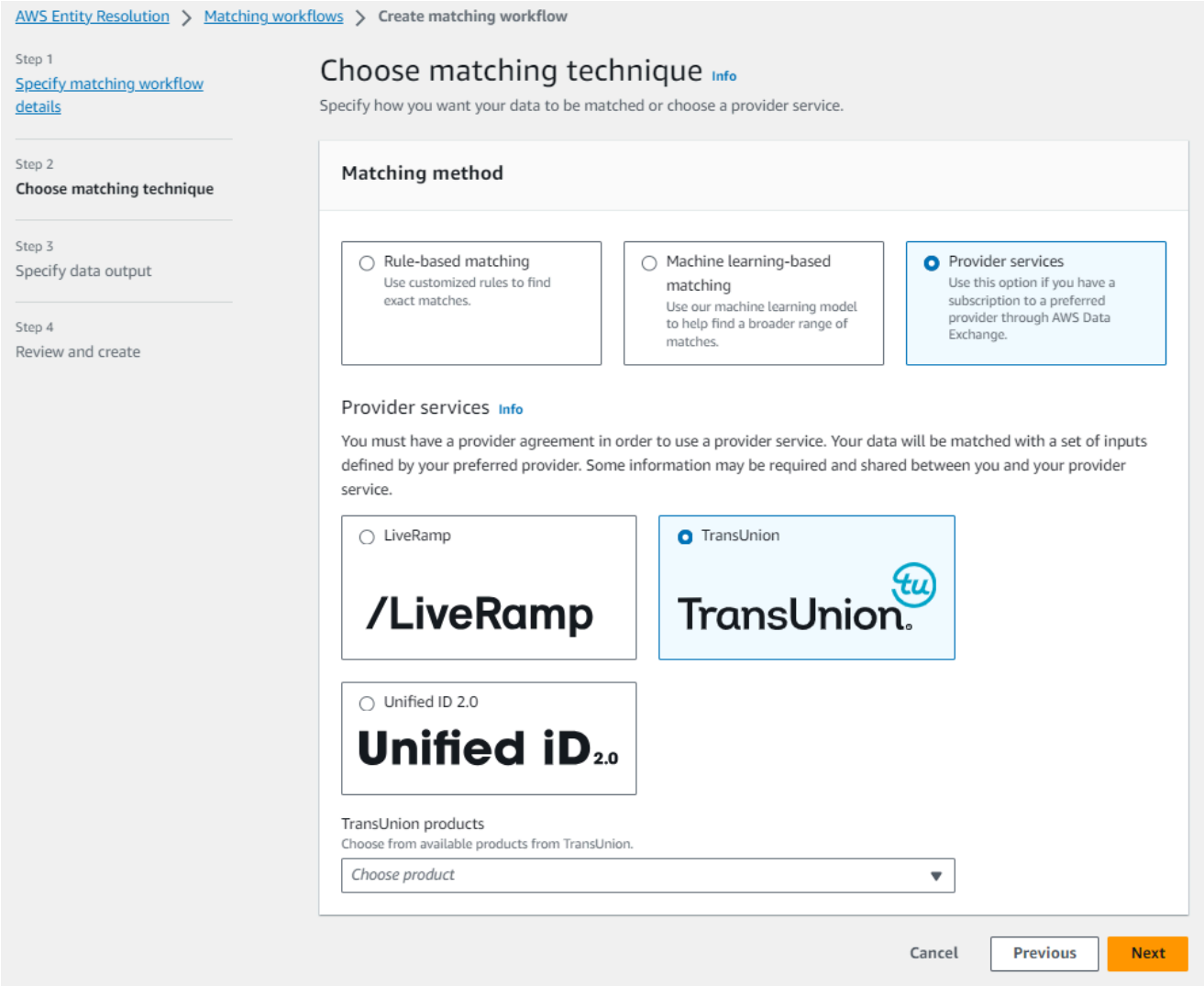
5. ステップ 2: 一致する手法を選択する：

a. マッチング方法 で、プロバイダーサービス を選択します。

b. プロバイダーサービス で、 を選択しますTransUnion。

> **Note**
>
> データ入力ファイルの形式と正規化がプロバイダーサービスのガイドラインと一致していることを確認します。

c. TransUnion 製品 の場合、ドロップダウンリストから製品を選択します。



d. データステージング では、処理中のデータの一時ストレージ用の Amazon S3 の場所を選択します。

データステージング Amazon S3 の場所 に対するアクセス許可が必要です。詳細については、「the section called “のワークフロージョブロールを作成する AWS Entity Resolution”」を参照してください。

6. [Next] (次へ) を選択します。
7. ステップ 3: データ出力 を指定します。

   a. データ出力の送信先と形式 で、データ出力の Amazon S3 の場所と、データ形式を正規化データまたは元のデータのどちらにするかを選択します。

   b. 暗号化 で、暗号化設定 をカスタマイズする場合は、AWS KMS キー ARN を入力します。

   c. TransUnion 生成された出力 を表示します。

      これは、 によって生成された追加情報です TransUnion。

   d. データ出力 では、含まれているすべてのフィールドを表示し、フィールドを含めるか、非表示にするか、マスクするかを決定します。

目的	選択内容
フィールドを含める	出力状態は「Included」のままにします。
フィールドを非表示 (出力から除外)	出力フィールド を選択し、 を非表示 を選択します。
マスクフィールド	出力フィールド を選択し、ハッシュ出力 を選択します。
以前の設定をリセットする	[リセット] を選択します。

   e. システム生成出力 には、含まれているすべてのフィールドを表示します。

   f. [次へ] をクリックします。

8. ステップ 4: を確認して作成する :

   a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

   b. Create and run を選択します。

      一致するワークフローが作成され、ジョブが開始されたことを示すメッセージが表示されます。

9. 一致するワークフローの詳細ページのメトリクスタブで、「最後のジョブメトリクス」で以下を表示します。

   • ジョブ ID 。

- 一致するワークフロージョブのステータス: Queued 、In progress 、Completed 、Failed
- ワークフロージョブの完了時刻。
- 処理されたレコードの数。
- 処理されなかったレコードの数。
- 生成された一意の一致 IDs。
- 入力レコードの数。

ジョブ履歴 で以前に実行されたワークフロージョブを照合するためのジョブメトリクスを表示することもできます。

10. 一致するワークフロージョブが完了した後 (ステータスは完了) 、データ出力タブに移動し、Amazon S3 の場所を選択して結果を表示できます。

これで次の作業に進むことができます。

- 一致するワークフローを編集する
- 一致するワークフローを削除する

UID 2.0 を使用したマッチングワークフローの作成

Unified ID 2.0 サービスのサブスクリプションをお持ちの場合は、決定論的アイデンティティを持つ広告キャンペーンをアクティブ化し、広告エコシステム全体で多くの UID2-enabled参加者との相互運用性に頼ることができます。詳細については、「Unified ID 2.0 Overview」を参照してください。

統合 ID 2.0 サービスは未加工の UID 2 を提供します。これは、トレードデスクプラットフォームでの広告キャンペーンの構築に使用されます。UID 2.0 はオープンソースフレームワークを使用して生成されます。

1 つのワークフローでは、未加工の UID2 生成**Phone number**に **Email Address**または を使用できますが、両方を使用することはできません。両方がスキーママッピングに存在する場合、ワークフローは を選択し**Email Address**、 はパススルーフィールド**Phone number**になります。両方をサポートするには、 がマッピングされているが**Phone number**、 **Email Address**がマッピングされていない新しいスキーママッピングを作成します。次に、この新しいスキーママッピングを使用して 2 番目のワークフローを作成します。

> **Note**
>
> Raw UID2sは、ソルトバケットからソルトを 1 年に約 1 回ローテーションすることで作成され、それに伴って raw UID2 もローテーションされるため、raw UID2sを毎日更新することをお勧めします。詳細については、https://unifiedid.com/docs/getting-started/gs-faqs#how-often-should-uid2s-be-refreshed-for-incremental-updates」を参照してください。

UID 2.0 で一致するワークフローを作成するには：

1. にサインイン AWS Management Console し、 でAWS Entity Resolution コンソールを開きますAWS アカウント（まだ開いていない場合）。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. 一致ワークフロー ページの右上隅で、一致ワークフローの作成 を選択します。
4. ステップ 1: 一致するワークフローの詳細を指定するには、次の手順を実行します。

   a. 一致するワークフロー名とオプションの 説明を入力します。

   b. データ入力 で、ドロップダウンからAWS Glue データベースを選択し、AWS Glue テーブル を選択し、対応するスキーママッピング を選択します。

      最大 20 個のデータ入力を追加できます。

   c. データ正規化オプションを選択したままにして、一致する前にデータ入力 (**`Email Address`** または **`Phone number`**) を正規化します。

      `Email Address` 正規化の詳細については、UID 2.0 ドキュメントの「E メールアドレスの正規化」を参照してください。

      `Phone number` 正規化の詳細については、UID 2.0 ドキュメントの「電話番号の正規化」を参照してください。

   d. [新しいサービスロールを作成して使用] または [既存のサービスロールを使用] を選択して、[サービスアクセス] 許可を指定します。

選択した場合	THEN
新しいサービスロールを作成して使用	• AWS Entity Resolution は、このテーブルに必要なポリシーを

選択した場合	THEN
	持つサービスロールを作成します。 • デフォルトの [サービスロール名] は `entityresolution-matching-workflow-<timestamp>` です。 • ロールを作成してポリシーをアタッチするアクセス許可が必要です。 • 入力データが暗号化されている場合は、KMS キーオプションで暗号化されたデータを選択し、データ入力の復号に使用される AWS KMS キーを入力できます。

選択した場合	THEN
既存のサービスロールを使用	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. IAM 外部リンクで表示を選択して、サービスロールを表示します。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必要なアクセス許可を追加しようとしません。

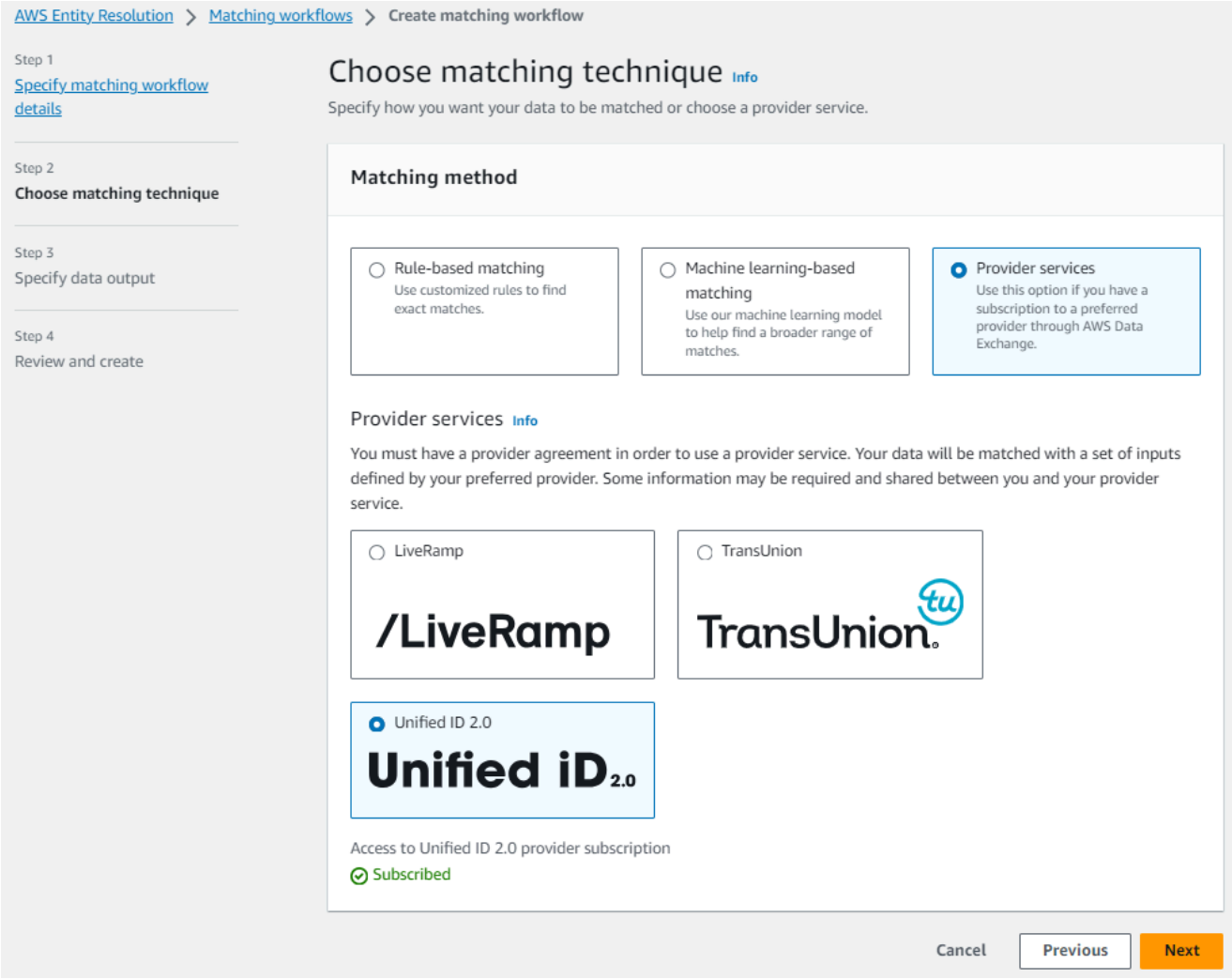
e. （オプション) リソースのタグを有効にするには、新しいタグを追加 を選択し、キーと値のペアを入力します。

f. [次へ] をクリックします。

5. ステップ 2: 一致する手法を選択する：

a. マッチング方法 で、プロバイダーサービス を選択します。

b. プロバイダーサービス で、統合 ID 2.0 を選択します。



c. [次へ] をクリックします。

6. ステップ 3: データ出力 を指定します。

a. データ出力の送信先と形式 で、データ出力の Amazon S3 の場所と、データ形式を正規化データまたは元のデータのどちらにするかを選択します。

b. 暗号化 で、暗号化設定 をカスタマイズする場合は、AWS KMS キー ARN を入力します。

c. Unified ID 2.0 で生成された出力 を表示します。

これは UID 2.0 によって生成されたすべての追加情報のリストです。

d. データ出力 では、含まれているすべてのフィールドを表示し、フィールドを含めるか、非表示にするか、マスクするかを決定します。

目的	選択内容
フィールドを含める	出力状態は「Included」のままにします。
フィールドを非表示 (出力から除外)	出力フィールド を選択し、 を非表示 を選択します。
マスクフィールド	出力フィールド を選択し、ハッシュ出力 を選択します。
以前の設定をリセットする	[リセット] を選択します。

e. システム生成の出力 には、含まれているすべてのフィールドを表示します。

f. [次へ] をクリックします。

7. ステップ 4: を確認して作成する :

a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

b. Create and run を選択します。

一致するワークフローが作成され、ジョブが開始されたことを示すメッセージが表示されます。

8. 一致するワークフローの詳細ページのメトリクスタブで、「最終ジョブメトリクス」で以下を表示します。

- ジョブ ID 。
- 一致するワークフロージョブのステータス: Queued 、In progress 、Completed 、Failed
- ワークフロージョブの完了時刻。
- 処理されたレコードの数。
- 処理されていないレコードの数。
- 生成された一意の一致 IDs。
- 入力レコードの数。

ジョブ履歴 で以前に実行されたワークフロージョブを照合するためのジョブメトリクスを表示することもできます。

9. 一致するワークフロージョブが完了した後 (ステータスは完了) 、データ出力タブに移動し、Amazon S3 の場所を選択して結果を表示できます。

これで次の作業に進むことができます。

- 一致するワークフローを編集する
- 一致するワークフローを削除する

一致するワークフローを実行する

手動処理タイプでルールベースのマッチングまたは機械学習ベースのマッチングワークフローを作成したら、一致するワークフロージョブを実行できます。

> **Note**
>
> 自動処理タイプを使用して一致するワークフローを作成すると、データ入力が更新されるたびに一致するワークフロージョブが実行されます。

AWS Entity Resolution は、指定した場所からデータを読み取り、データ内の 2 つ以上のレコード間の一致を検出します。次に、一致したデータセットのレコードに一致 ID を割り当てます。

- ルールベースのマッチング手法を指定した場合、 AWS Entity Resolution は一致を生成した適用されたルール番号も割り当てます。
- 機械学習ベースのマッチング手法を指定した場合、 AWS Entity Resolution は一致信頼度の割合も割り当てます。

AWS Entity Resolution 次に、 は選択した場所にデータ出力ファイルを書き込みます。

ワークフローは複数の実行を行うことができ、結果 (成功またはエラー) は を名前`jobId`とするフォルダに書き込まれます。

データ出力には、一致が成功したファイルとエラーのファイルの両方が含まれます。データ出力には複数のフィールドを含めることができます。成功した結果は`success`フォルダに書き込まれ、フォルダには複数のファイルが含まれ、それぞれに成功したレコードのサブセットが含まれます。同様に、エラーは複数のフィールドを持つ`error`フォルダに書き込まれ、それぞれにエラーレコードのサ

ブセットが含まれます。エラーのトラブルシューティングの詳細については、「」を参照してくださいワークフローのトラブルシューティング。

一致するワークフローを実行するには：

1. にサインイン AWS Management Console し、 でAWS Entity Resolution コンソールを開きますAWS アカウント（まだ開いていない場合）。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. 一致するワークフローを選択します。
4. 一致するワークフローの詳細ページの右上隅にあるワークフローの実行 を選択します。

   ジョブが開始されたことを示すメッセージが表示されます。
5. 「メトリクス」タブの「ジョブ履歴」で、以下を表示します。

   - 一致するワークフロージョブのステータス: 進行中、完了、失敗
   - 処理されたレコードの数。
   - 見つかった一致の数。
   - 一意のレコードの数。
   - ジョブの所要時間。
   - ジョブ ID 。
6. 一致するワークフロージョブが完了した後 (ステータスが完了)、データ出力タブに移動し、Amazon S3 の場所を選択して結果を表示できます。

次のステップ

これで次の作業に進むことができます。

- 一致するワークフローを編集する
- 一致するワークフローを削除する

ID 名前空間の作成

ID 名前空間は、データとマッチング手法、およびそれらを ID マッピングワークフロー で使用する方法を説明するメタデータを提供するために使用するデータテーブルのラッパーです。

ID 名前空間には、ソース とターゲット の 2 種類があります。

- ソースには、ID マッピングワークフローで AWS Entity Resolution 処理するソースデータの設定が含まれています。
- ターゲットには、すべてのソースが解決するターゲットデータの設定が含まれています。

ID マッピングワークフローで 2 AWS アカウント つの 間で解決する入力データを定義できます。1 人の参加者が ID 名前空間ソースを作成し、別の参加者が ID 名前空間ターゲットを作成します。参加者がソースとターゲットを作成したら、ID マッピングワークフローを実行して、ソースからターゲットにデータを変換できます。

以下のトピックでは、ソース ID とターゲット ID の名前空間を作成し、Amazon Simple Storage Service (Amazon S3) でデータ出力を指定する一連の手順について説明します。

> **Note**
>
> AWS Entity Resolution は現在、ID 名前空間の作成時に ID 名前空間メソッドの LiveRamp トランスコードを提供しています。

トピック

ID 名前空間ソースを作成する

このトピックでは、コンソール で ID AWS Entity Resolution名前空間ソースを作成するプロセスについて説明します。これは、ID マッピングワークフロー 内のデータのソースです。

> **Note**
>
> 入力データがソースである場合は、スキーママッピングと関連付けられた AWS Glue データベースが必要です。

ID 名前空間ソースを作成するには

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのデータ準備 で、ID 名前空間 を選択します。
3. ID 名前空間 ページの右上隅で、ID 名前空間の作成 を選択します。
4. 詳細 で、次の操作を行います。
   a. ID 名前空間名 には、一意の名前を入力します。
   b. (オプション) 説明 に、オプションの説明を入力します。
   c. ID 名前空間タイプ で、ソース を選択します。
5. ID 名前空間メソッド を表示します。

   > **Note**
   >
   > AWS Entity Resolution は現在、ID 名前空間メソッドとして LiveRamp プロバイダーサービスを提供しています。へのサブスクリプションがある場合 LiveRamp、ステータスは Subscribed と表示されます。をサブスクライブする方法の詳細については、LiveRamp「」を参照してくださいでプロバイダーサービスをサブスクライブする AWS Data Exchange。

6. データ入力 で、ドロップダウンリストからAWS Glue データベース 、AWS Glue テーブル 、スキーママッピングを選択します。

   最大 20 個のデータ入力を追加できます。
7. サービスアクセス許可を指定するには、新しいサービスロールを作成して使用するか、既存のサービスロールを使用するを選択します。

選択した場合	THEN
新しいサービスロールを作成して使用	AWS Entity Resolution は、このテーブルに必要なポリシーを持つサービスロールを作成します。 デフォルトのサービスロール名は ですentityresolution-id-mapping-workflow-<timestamp> 。 ロールを作成してポリシーをアタッチするアクセス許可が必要です。 入力データが暗号化されている場合は、「このデータは KMS キーで暗号化されます」オプションを選択します。次に、データ入力の復号に使用される AWS KMS キーを入力します。

選択した場合	THEN
既存のサービスロールを使用	ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、既存のサービスロールを使用するオプションは使用できません。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必要なアクセス許可を追加しようとしません。

8. (オプション) リソースのタグを有効にするには、新しいタグを追加 を選択し、キーと値のペアを入力します。
9. ID 名前空間の作成 を選択します。

ID 名前空間ターゲットを作成する

このトピックでは、コンソール で ID AWS Entity Resolution名前空間ターゲットを作成するプロセスについて説明します。これは、ID マッピングワークフロー 内のデータのターゲットです。すべてのソースがターゲットに解決されます。

ID 名前空間ターゲットを作成するには

1. にサインイン AWS Management Console し AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのデータ準備 で、ID 名前空間 を選択します。
3. ID 名前空間 ページの右上隅で、ID 名前空間の作成 を選択します。
4. 詳細 で、次の操作を行います。

   a. ID 名前空間名 には、一意の名前を入力します。

   b. （オプション) 説明 に、オプションの説明を入力します。

   c. ID 名前空間タイプ で、ターゲット を選択します。
5. ID 名前空間メソッド を表示します。

> **Note**
>
> AWS Entity Resolution は現在、ID 名前空間メソッドとして LiveRamp プロバイダーサービスを提供しています。
> へのサブスクリプションがある場合 LiveRamp、ステータスは Subscribed と表示されます。
> をサブスクライブする方法の詳細については、 LiveRamp「」を参照してくださいでプロバイダーサービスをサブスクライブする AWS Data Exchange。

6. ターゲットドメイン には、 LiveRamp が提供するトランスコードの対象となる LiveRamp クライアントドメイン識別子を入力します。
7. （オプション) リソースのタグを有効にするには、新しいタグを追加 を選択し、キーと値のペアを入力します。
8. ID 名前空間の作成 を選択します。

2 つの にわたる ID マッピングワークフローに必要な ID 名前空間を作成したら AWS アカウント、ID マッピングワークフロー を作成する準備が整います。

ID マッピングワークフローの作成

の ID マッピングワークフロー AWS Entity Resolution は現在、 と統合されています LiveRamp。LiveRamp サービスのサブスクリプションがある場合は、 を使用して LiveRamp ID マッピングワークフローを作成して、トランスコードを実行できます。 LiveRamp トランスコードを使用すると、ソース RampIDs のセットを任意のターゲット先 RampID に変換できます。RampID をトークンとして使用して顧客を表すことで、顧客データを広告プラットフォームと直接共有することを回避できます。

2 つのデータセット間で ID マッピングを自分で実行 AWS アカウント することも、2 つの異なる 間で実行することもできます AWS アカウント。データ入力ソースとターゲットは、実行する ID マッピングのタイプによって異なります。

詳細については、 LiveRamp ドキュメントウェブサイトの「ADX による翻訳の実行」を参照してください。

トピック

- 前提条件
- 1 つの ID マッピングワークフローの作成 AWS アカウント
- 2 つの にわたる ID マッピングワークフローの作成 AWS アカウント
- ID マッピングワークフローの実行
- 新しい出力先で ID マッピングワークフローを実行する

前提条件

この ID マッピングワークフローには、ID マッピングワークフロー出力を一時的に書き込む Amazon Simple Storage Service (Amazon S3) データステージングバケットが必要です。を使用して ID マッピングワークフローを作成する前に LiveRamp、次のアクセス許可ポリシーを追加します。これにより、データステージングバケットにアクセスできます。

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

上記のアクセス許可ポリシーで、各 ################ をユーザー自身の情報に置き換えます。

##########	プロバイダーのサービスベースのワークフローの実行中にデータを一時的に保存する Amazon S3 バケット。

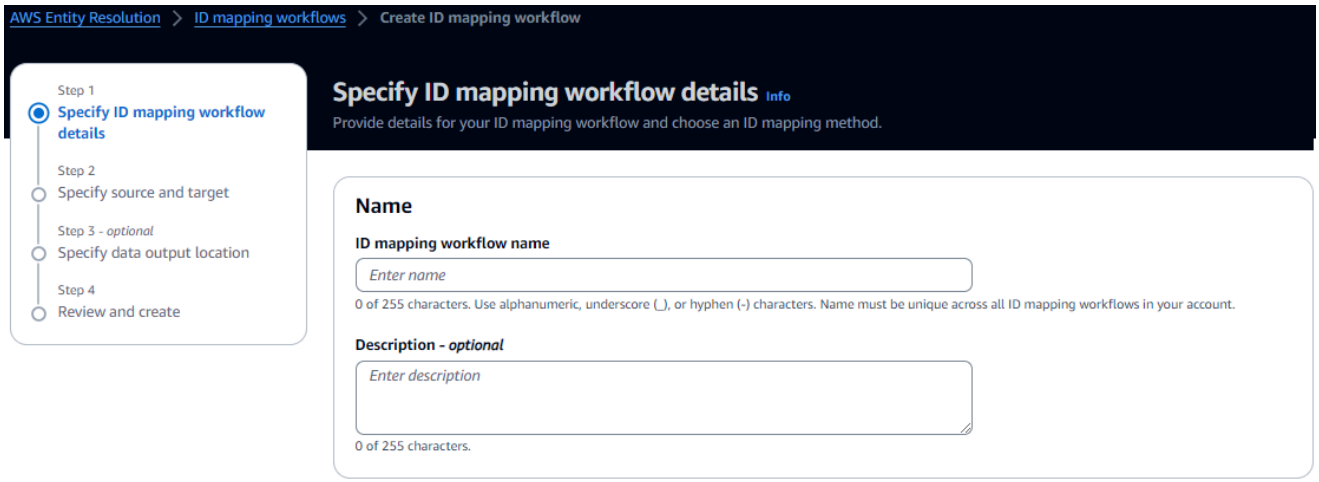
1 つの ID マッピングワークフローの作成 AWS アカウント

セットアップステップを完了し、スキーママッピング を作成したら、1 つ以上の ID マッピングワークフローを作成して、維持されている RampIDs または派生した RampID のいずれかを使用して、ソース RampIDsのセットを別の に変換できます。

1 つの ID マッピングワークフローを作成するには AWS アカウント

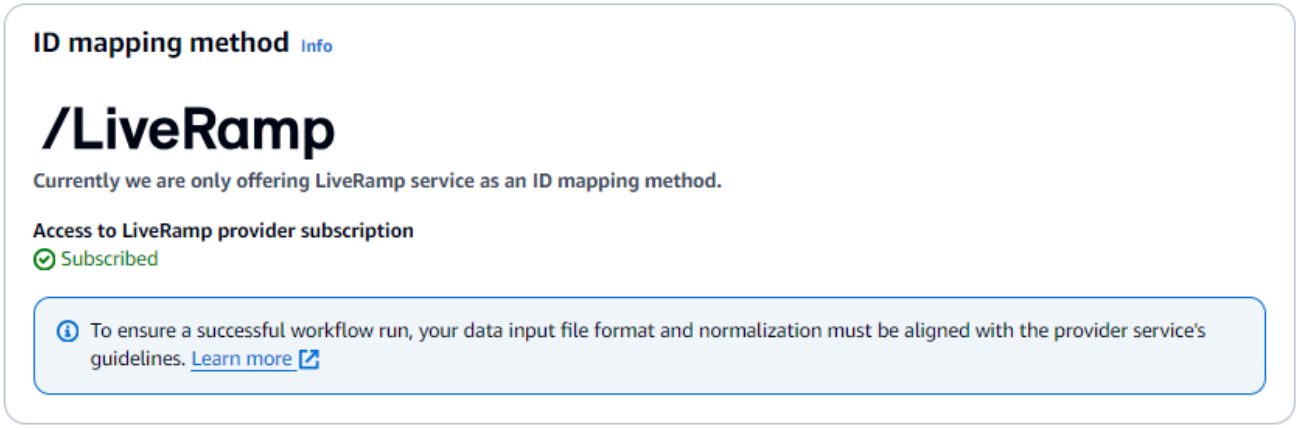
1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、ID マッピング を選択します。
3. ID マッピングワークフローページの右上隅で、ID マッピングワークフローの作成 を選択します。
4. ステップ 1: ID マッピングワークフローの詳細を指定するには、次の手順を実行します。

    a. ID マッピングワークフロー名とオプションの説明 を入力します。



    b. ID マッピング方法を表示します。

    AWS Entity Resolution は現在、ID マッピング方法として LiveRamp プロバイダーサービスを提供しています。へのサブスクリプションがある場合 LiveRamp、ステータスは Subscribed と表示されます。をサブスクライブする方法の詳細については、LiveRamp「」を参照してくださいでプロバイダーサービスをサブスクライブする AWS Data Exchange。



> **Note**
>
> データ入力ファイルの形式がプロバイダーサービスのガイドラインと一致していることを確認します。の入力ファイルフォーマットガイドラインの詳細については、LiveRamp ドキュメントウェブサイト LiveRampの「ADX による翻訳の実行」を参照してください。

c. LiveRamp 設定 には、 LiveRamp が提供する次の値を入力します。

- クライアント ID マネージャー ARN
- クライアントシークレットマネージャー ARN

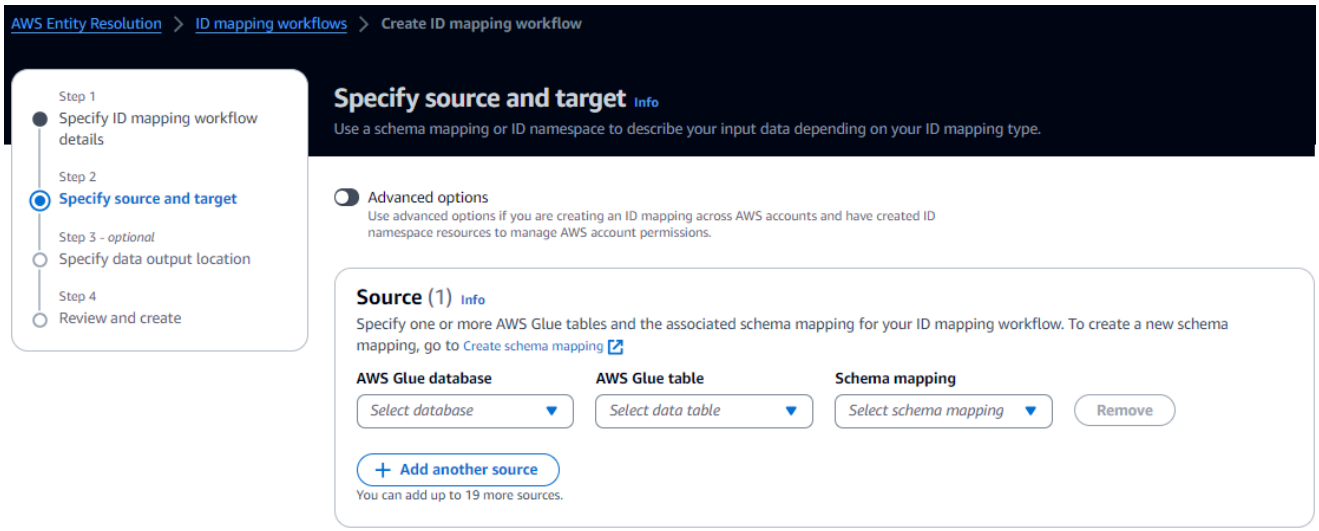
d. (オプション) リソースのタグを有効にするには、新しいタグの追加 を選択し、キーと値のペアを入力します。

e. [次へ] をクリックします。

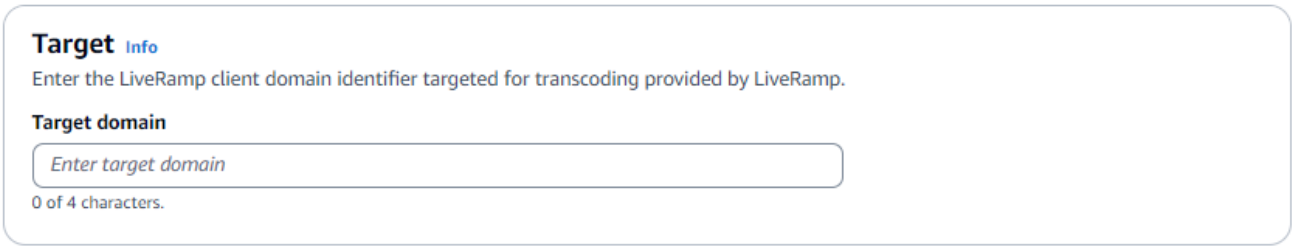
5. ステップ 2: ソース とターゲット を指定するには、次の手順を実行します。

a. ソース で、ドロップダウンからAWS Glueデータベースを選択し、AWS Glue テーブル を選択し、対応するスキーママッピング を選択します。

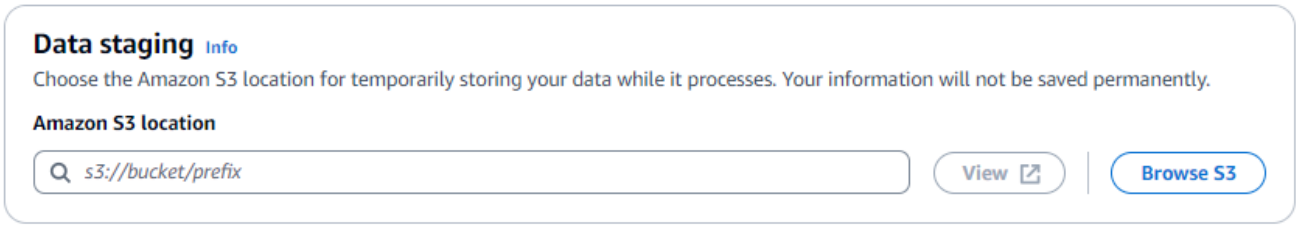
最大 19 個のデータ入力を追加できます。



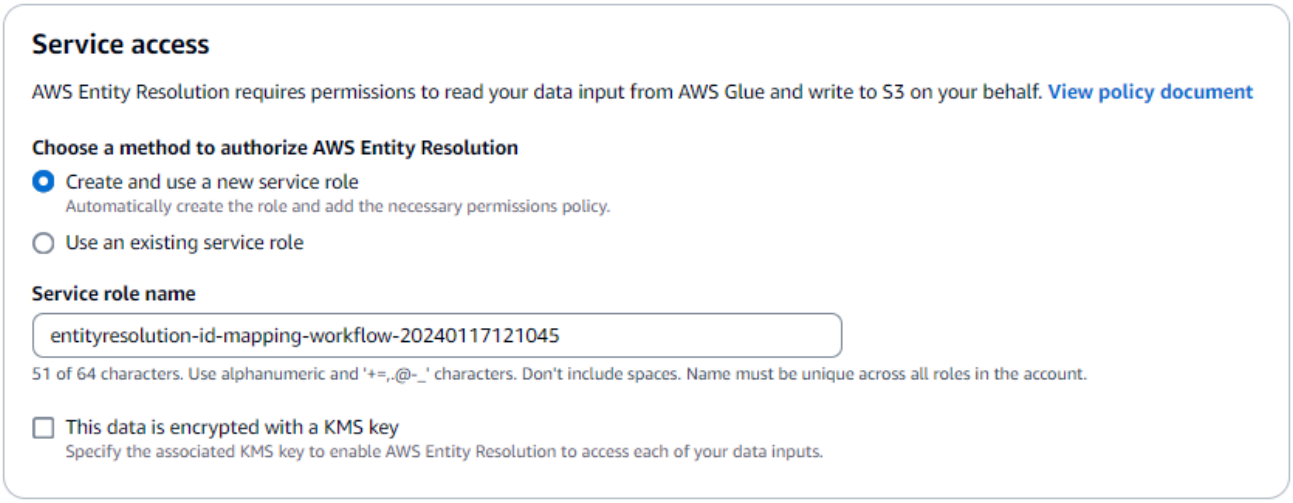
b. ターゲット には、 LiveRamp が提供するトランスコードの対象となる LiveRamp クライアントドメイン識別子を入力します。



c. データステージング で、ID マッピングワークフロー出力を一時的に書き込む Amazon S3 の場所を選択します。



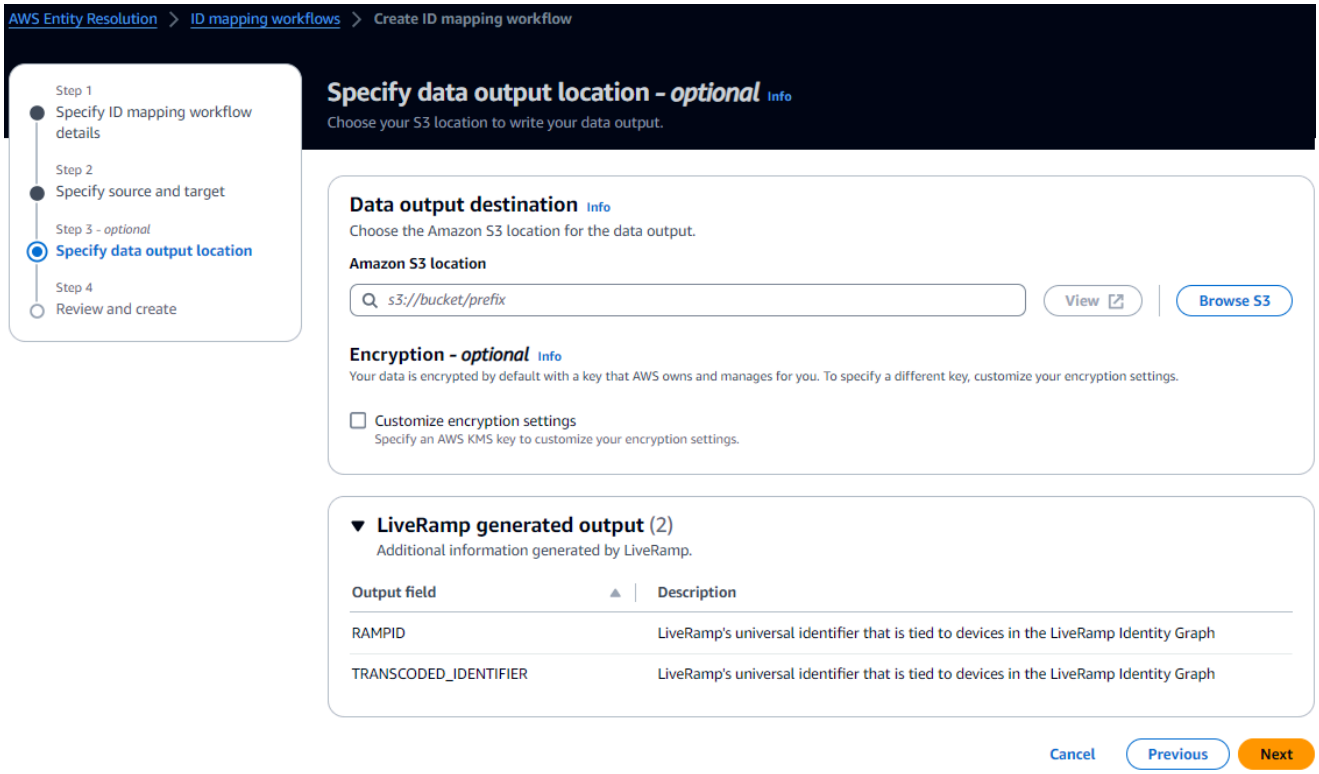
d. サービスアクセス許可を指定するには、新しいサービスロールを作成して使用するか、既存のサービスロールを使用するを選択します。



選択した場合	THEN
新しいサービスロールを作成して使用	AWS Entity Resolution は、このテーブルに必要なポリシーを持つサービスロールを作成します。 デフォルトのサービスロール名は ですentityresolution-id-mapping-workflow-<timestamp> 。 ロールを作成してポリシーをアタッチするアクセス許可が必要です。 入力データが暗号化されている場合は、「このデータは KMS キーで暗号化されます」オプションを選択します。次に、データ入力の復号に使用される AWS KMS キーを入力します。

選択した場合	THEN
既存のサービスロールを使用	ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、既存のサービスロールを使用するオプションは使用できません。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必要なアクセス許可を追加しようとしません。

6. [次へ] をクリックします。
7. ステップ 3: データ出力場所を指定する – オプション で、次の操作を行います。
   a. データ出力先 の場合、次の操作を行います。
      i. データ出力の Amazon S3 の場所を選択します。
      ii. 暗号化 で、暗号化設定 をカスタマイズする場合は、AWS KMS キー ARN を入力するか、 AWS KMS キーの作成 を選択します。
   b. LiveRamp 生成された出力 を表示します。
   c. [次へ] をクリックします。



8. ステップ 4: を確認して作成するには、次の手順を実行します。

   a. 前のステップで選択した内容を確認し、必要に応じて編集します。

   b. [作成] を選択します。

      ID マッピングワークフローが作成されたことを示すメッセージが表示されます。

ID マッピングワークフローを作成したら、ID マッピングワークフローを実行する準備が整います。

2 つの にわたる ID マッピングワークフローの作成 AWS アカウント

前提条件

2 つの にまたがる ID マッピングワークフローを作成するには、 が S3 バケットと AWS Key Management Service （ AWS KMS) カスタマーマネージドキーにアクセス LiveRamp するためのアクセス許可 AWS アカウント が必要です。 AWS アカウント を使用して 2 つの にまたがる ID マッピングワークフローを作成する前に LiveRamp、次のアクセス許可ポリシーを追加します。これにより、 は S3 バケットとカスタマーマネージドキー LiveRamp にアクセスできます。

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

上記のアクセス許可ポリシーで、各 ################ をユーザー自身の情報に置き換えます。

<KMSKeyARN >	AWS KMS カスタマーマネージドキーの ARN。

ID マッピングワークフローを作成する

2 つの にまたがる ID マッピングワークフローを作成する前に AWS アカウント、まず以下を実行する必要があります。

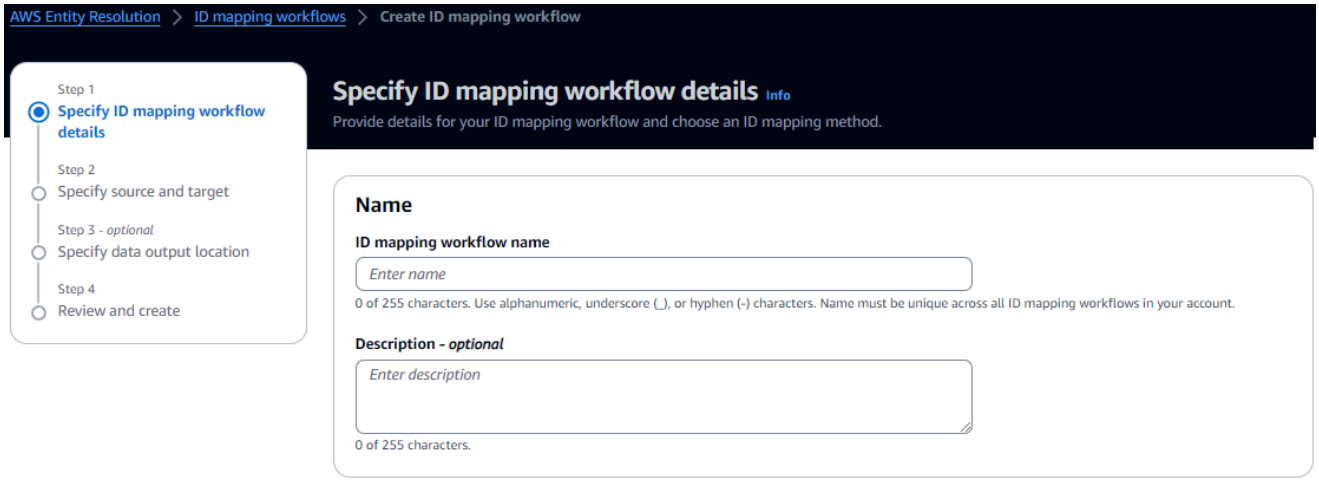
- カスタマーマネージドキーにアクセス許可を追加するには、前提条件を完了します。
- セットアップ AWS Entity Resolution の各タスクを完了する。
- ID 名前空間ソース を作成します。
- ID 名前空間ターゲット を作成します。

前述のタスクを完了したら、1 つ以上の ID マッピングワークフローを作成して、維持されている RampIDs または派生した RampID を使用して、ソース RampID のセットを別の RampIDs に変換できます。

2 つの にまたがる ID マッピングワークフローを作成するには AWS アカウント

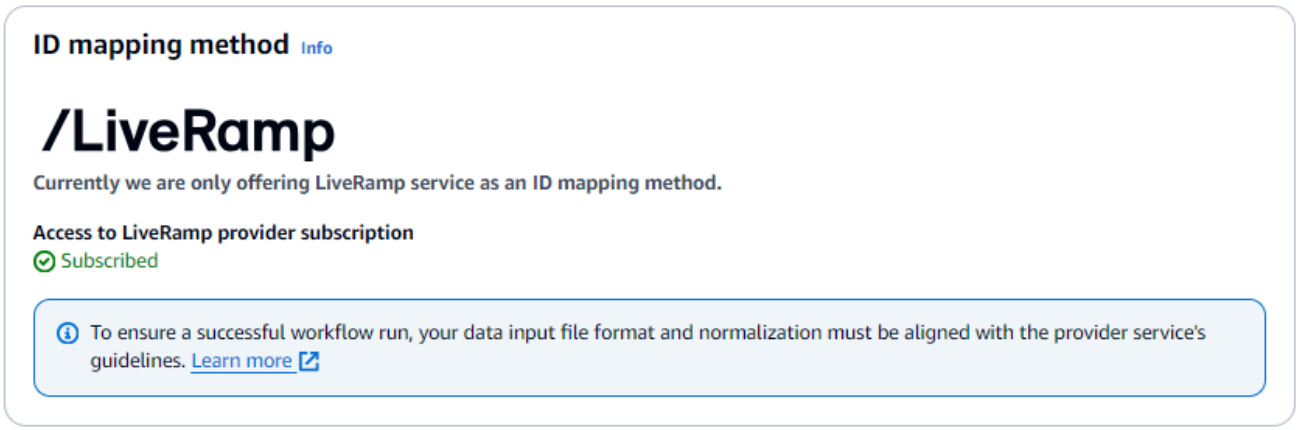
1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、ID マッピング を選択します。
3. ID マッピングワークフローページの右上隅で、ID マッピングワークフローの作成 を選択します。
4. ステップ 1: ID マッピングワークフローの詳細を指定するには、次の手順を実行します。

   a. ID マッピングワークフロー名とオプションの説明 を入力します。



   b. ID マッピング方法を表示します。

      AWS Entity Resolution は現在、ID マッピング方法として LiveRamp プロバイダーサービスを提供しています。へのサブスクリプションがある場合 LiveRamp、ステータスは Subscribed と表示されます。をサブスクライブする方法の詳細については、LiveRamp「」を参照してくださいでプロバイダーサービスをサブスクライブする AWS Data Exchange。



> **Note**
>
> データ入力ファイルの形式がプロバイダーサービスのガイドラインと一致していることを確認します。の入力ファイルフォーマットガイドラインの詳細については、LiveRamp ドキュメントウェブサイト LiveRampの「ADX による翻訳の実行」を参照してください。

c. LiveRamp 設定 には、 LiveRamp が提供する次の値を入力します。

- クライアント ID マネージャー ARN
- クライアントシークレットマネージャー ARN

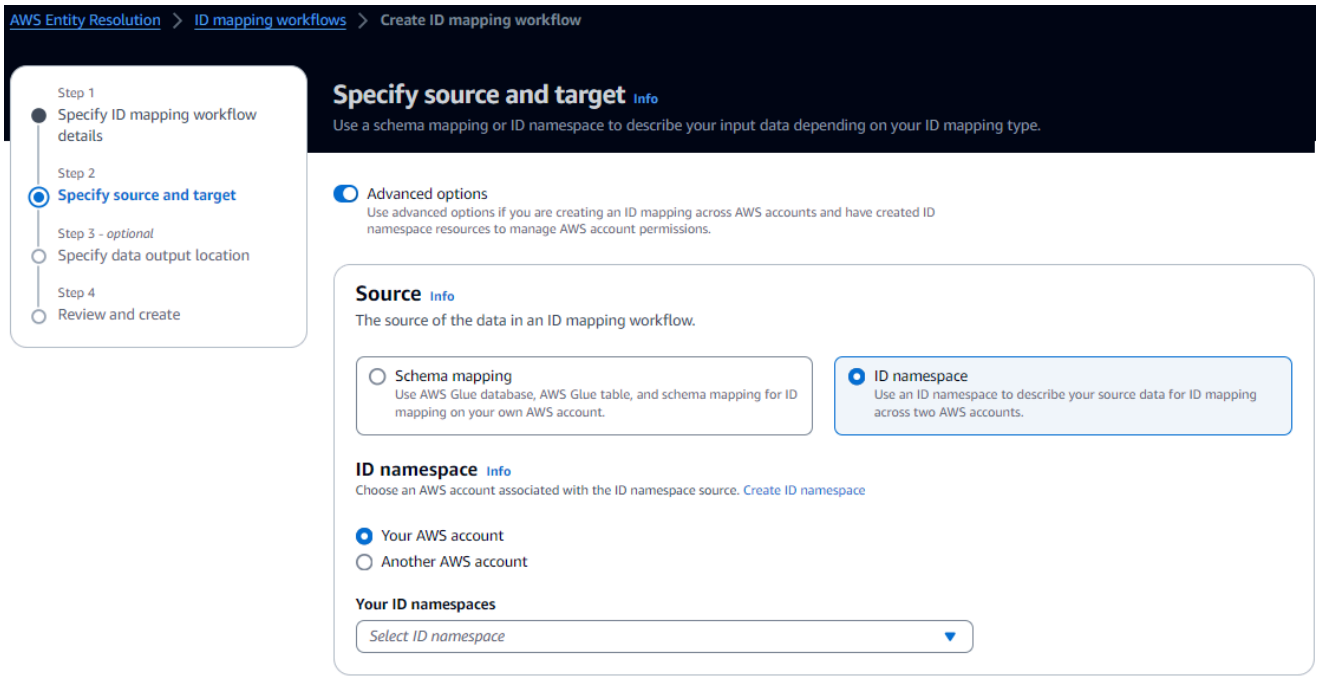
d. (オプション) リソースのタグを有効にするには、新しいタグを追加 を選択し、キーと値のペアを入力します。

e. [次へ] をクリックします。

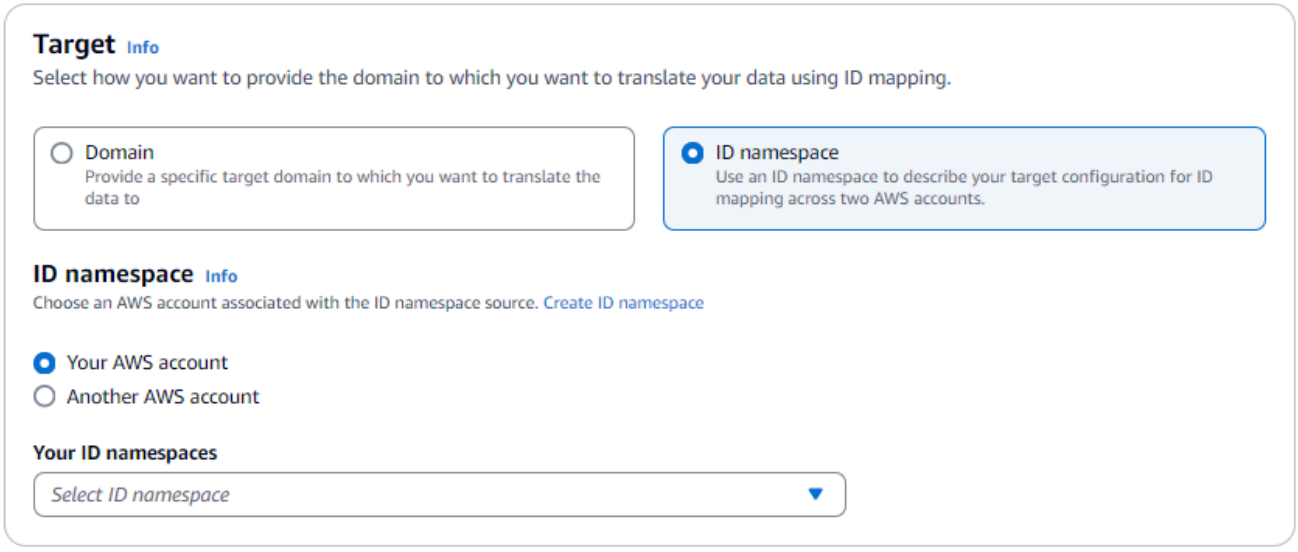
5. ステップ 2: ソース とターゲット を指定するには、次の手順を実行します。

a. 詳細オプション をオンにします。

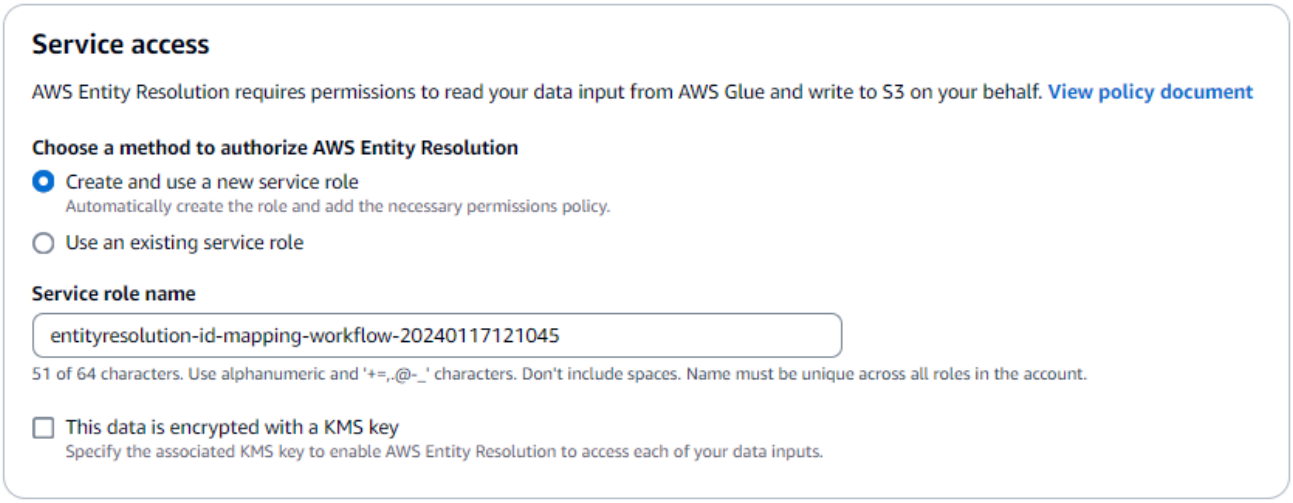
b. ソース で、ID 名前空間 を選択します。



c. ターゲット で、ID 名前空間 を選択します。



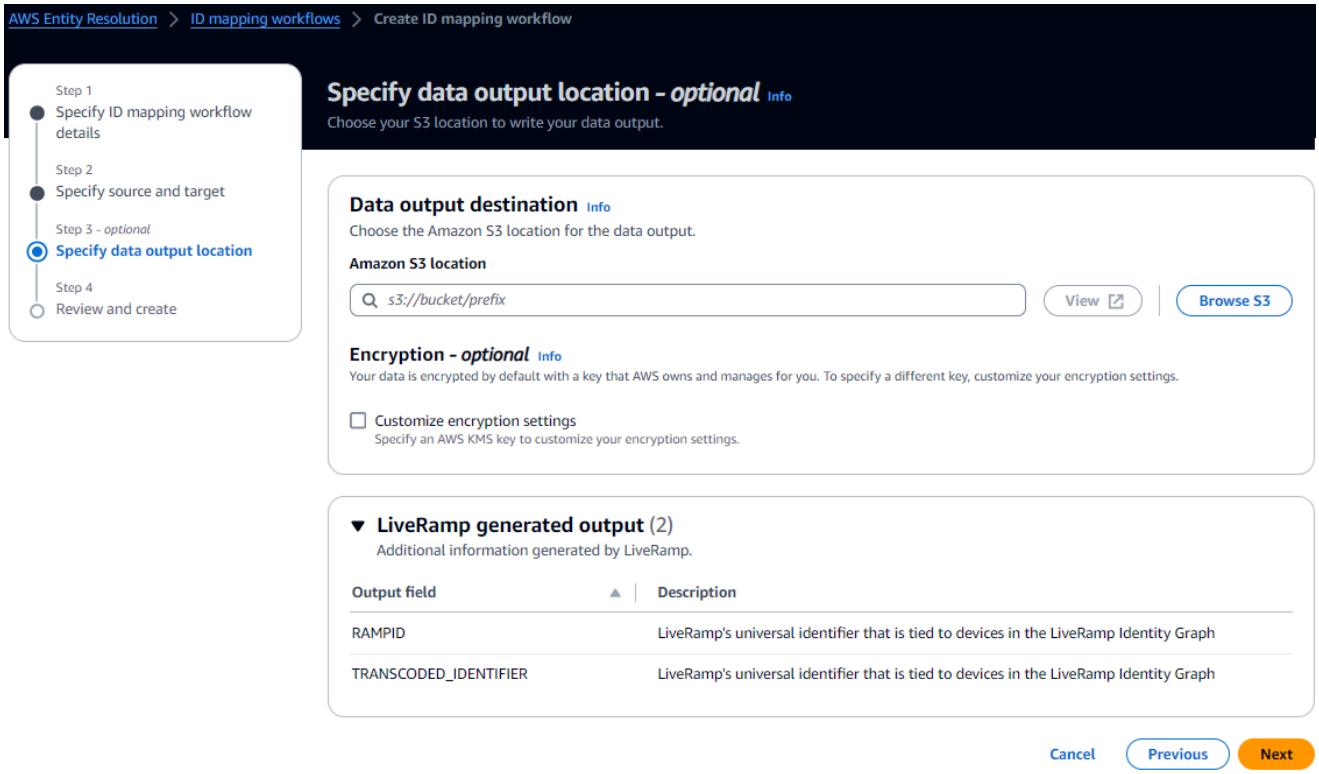
d. サービスアクセス許可を指定するには、新しいサービスロールを作成して使用するか、既存のサービスロールを使用するを選択します。



選択した場合	THEN
新しいサービスロールを作成して使用	AWS Entity Resolution は、このテーブルに必要なポリシーを持つサービスロールを作成します。 デフォルトのサービスロール名は ですentityresolution-id-mapping-workflow-<timestamp> 。 ロールを作成してポリシーをアタッチするアクセス許可が必要です。 入力データが暗号化されている場合は、「このデータは KMS キーで暗号化されます」オプションを選択します。次に、データ入力の復号に使用される AWS KMS キーを入力します。

選択した場合	THEN
既存のサービスロールを使用	ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、既存のサービスロールを使用するオプションは使用できません。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必要なアクセス許可を追加しようとしません。

6. [次へ] をクリックします。
7. ステップ 3: データ出力場所を指定する – オプション で、次の操作を行います。
   a. データ出力先 の場合、次の操作を行います。
      i. データ出力の Amazon S3 の場所を選択します。
      ii. 暗号化 で、暗号化設定 をカスタマイズする場合は、AWS KMS キー ARN を入力するか、 AWS KMS キーの作成 を選択します。
   b. LiveRamp 生成された出力 を表示します。
   c. [次へ] をクリックします。



8. ステップ 4: を確認して作成するには、次の手順を実行します。

   a. 前のステップで選択した内容を確認し、必要に応じて編集します。

   b. [作成] を選択します。

      ID マッピングワークフローが作成されたことを示すメッセージが表示されます。

ID マッピングワークフローを作成したら、ID マッピングワークフロー を実行する準備が整います。

ID マッピングワークフローの実行

1 つの の ID マッピングワークフロー AWS アカウントを作成するか、2 つの にまたがる ID マッピングワークフロー AWS アカウントを作成したら、ID マッピングワークフローを実行できます。

ID マッピングワークフローを実行するには

1. にサインイン AWS Management Console し AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、ID マッピング を選択します。

3. ID マッピングワークフローを選択します。
4. ID マッピングワークフローの詳細ページの右上隅にある「 の実行」を選択します。
5. 一致するワークフローの詳細ページのメトリクスタブで、「最後のジョブメトリクス」で以下を表示します。

   - ジョブ ID
   - ワークフロージョブの完了時刻
   - 一致するワークフロージョブのステータス: Queued 、In progress 、Completed 、Failed
   - 処理されたレコードの数
   - 処理されなかったレコードの数
   - 入力レコードの数

   ジョブ履歴 では、以前に実行した ID マッピングワークフロージョブのジョブメトリクスを表示することもできます。
6. ID マッピングワークフロージョブが完了したら (ステータスは完了) 、データ出力 を選択し、Amazon S3 の場所を選択して結果を表示します。

   CSV ファイルを取得したら、 `RAMPID`と を結合できます`TRANSCODED_ID`。

新しい出力先で ID マッピングワークフローを実行する

1 つの の ID マッピングワークフロー AWS アカウントを作成するか、2 つの にまたがる ID マッピングワークフローを作成 AWS アカウントしたら、別の S3 ロケーションを選択してデータ出力を書き込むことができます。

新しい出力先で ID マッピングワークフローを実行するには

1. にサインイン AWS Management Console し AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、ID マッピング を選択します。
3. ID マッピングワークフローを選択します。
4. ID マッピングワークフローの詳細ページの右上隅にある「ワークフローの実行」ドロップダウンリストから「新しい出力先で実行」を選択します。
5. データ出力先 の場合、次の操作を行います。

a. データ出力の Amazon S3 の場所を選択します。

b. 暗号化 で、暗号化設定 をカスタマイズする場合は、AWS KMS キー ARN を入力するか、AWS KMS キーの作成 を選択します。

6. サービスアクセス許可を指定するには、新しいサービスロールを作成して使用するか、既存のサービスロールを使用するを選択します。

選択した場合	THEN
新しいサービスロールを作成して使用	AWS Entity Resolution は、このテーブルに必要なポリシーを持つサービスロールを作成します。 デフォルトのサービスロール名は ですentityresolution-id-mapping-workflow-<timestamp> 。 ロールを作成してポリシーをアタッチするアクセス許可が必要です。 入力データが暗号化されている場合は、「このデータは KMS キーで暗号化されます」オプションを選択します。次に、データ入力の復号に使用される AWS KMS キーを入力します。
既存のサービスロールを使用	ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。

選択した場合	THEN
	ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、既存のサービスロールを使用するオプションは使用できません。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必要なアクセス許可を追加しようとしません。

7. [実行] を選択します。
8. 一致するワークフローの詳細ページのメトリクスタブで、「最後のジョブメトリクス」で以下を表示します。

   - ジョブ ID
   - ワークフロージョブの完了時刻
   - 一致するワークフロージョブのステータス: Queued 、In progress 、Completed 、Failed
   - 処理されたレコードの数
   - 処理されなかったレコードの数
   - 入力レコードの数

   ジョブ履歴 では、以前に実行した ID マッピングワークフロージョブのジョブメトリクスを表示することもできます。
9. ID マッピングワークフロージョブが完了したら (ステータスは完了) 、データ出力 を選択し、Amazon S3 の場所を選択して結果を表示します。

   CSV ファイルを取得したら、 `RAMPID`と を結合できます`TRANSCODED_ID`。

の管理 AWS Entity Resolution

以下のトピックでは、 AWS Entity Resolution コンソールを使用してワークフローを管理する方法について説明します。

SDK AWS Entity Resolution を使用して を管理する方法については、 AWS Entity Resolution API リファレンス を参照してください。 AWS SDKs

トピック

スキーママッピングの管理

以下のトピックでは、 AWS Entity Resolution コンソールを使用してスキーママッピングを管理する方法について説明します。

トピック

スキーママッピングのクローンを作成する

既存の設定を使用して新しいスキーママッピングを作成する場合は、スキーママッピングのクローンを作成できます。

スキーママッピングのクローンを作成するには：

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。

2. 左側のナビゲーションペインのデータ準備 で、スキーママッピング を選択します。
3. スキーママッピングを選択します。
4. [クローンを作成] を選択します。
5. 「スキーマの詳細を指定」ページで、必要な変更を加え、「次へ」を選択します。
6. 「一致する手法を選択」ページで、必要な変更を加え、次へを選択します。
7. 「入力フィールドのマッピング」ページで、必要な変更を加え、「次へ」を選択します。
8. グループデータページで、必要な変更を加え、次へ を選択します。
9. 確認と保存ページで、必要な変更を加え、スキーママッピングのクローン を選択します。

スキーママッピングを編集する

スキーママッピングは、ワークフローに関連付ける前にのみ編集できます。スキーママッピングをワークフローに関連付けた後は、編集できません。既存の設定を使用して新しいスキーママッピングを作成する場合は、スキーママッピングのクローンを作成できます。

スキーママッピングを編集するには：

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのデータ準備 で、スキーママッピング を選択します。
3. スキーママッピングを選択します。
4. [編集] を選択します。
5. 「スキーマの詳細を指定」ページで、必要な変更を加え、「次へ」を選択します。
6. 「一致する手法を選択」ページで、必要な変更を加え、次へを選択します。
7. 「入力フィールドのマッピング」ページで、必要な変更を加え、「次へ」を選択します。
8. グループデータページで、必要な変更を加え、次へ を選択します。
9. 確認と保存ページで、必要な変更を加え、スキーママッピングの編集を選択します。

スキーママッピングを削除する

一致するワークフローに関連付けられているスキーママッピングは削除できません。スキーママッピングを削除する前に、まず関連するすべての一致ワークフローからスキーママッピングを削除する必要があります。

スキーママッピングを削除するには：

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのデータ準備 で、スキーママッピング を選択します。
3. スキーママッピングを選択します。
4. [削除] を選択します。
5. 削除を確定し、[削除] を選択します。

マッチングワークフローの管理

ルールベースのマッチング 、機械学習ベースのマッチング 、またはプロバイダーのサービスベースのマッチングワークフローを作成したら、次の方法でマッチングワークフローを管理できます。

トピック

- 一致するワークフローを編集する
- 一致するワークフローを削除する
- ルールベースの一致ワークフローの一致 ID を検索する
- ルールベースまたは ML ベースのマッチングワークフローからレコードを削除する

一致するワークフローを編集する

一致するワークフローを編集するには：

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. 一致するワークフローを選択します。
4. 一致するワークフローの詳細ページの右上隅にある 編集 を選択します。
5. 一致するワークフローの詳細を指定ページで、必要な変更を加え、次へ を選択します。
6. 「一致する手法を選択」ページで、必要な変更を加え、次へを選択します。
7. データ出力を指定ページで、必要な変更を加え、次へ を選択します。
8. 確認と保存ページで、必要な変更を加え、保存 を選択します。

一致するワークフローを削除する

一致するワークフローを削除するには：

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. 一致するワークフローを選択します。
4. 一致するワークフローの詳細ページの右上隅にある「削除」を選択します。
5. 削除を確定し、[削除] を選択します。

ルールベースの一致ワークフローの一致 ID を検索する

ルールベースのマッチングワークフローを実行すると、処理されたレコードに対応する一致 ID と関連するルールを見つけることができます。

ルールベースの一致ワークフローの一致 ID を検索するには：

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. 処理されたルールベースのマッチングワークフローを選択します (ジョブステータスは完了) 。
4. 一致するワークフローの詳細ページで、一致 ID の検索タブを選択します。
5. 次のいずれかを行います。

... の場合	結果
このワークフローに関連付けられているスキーママッピングは 1 つだけです。	デフォルトでは選択されているスキーママッピングを表示します。
このワークフローには複数のスキーママッピングが関連付けられています。	ドロップダウンリストからスキーママッピングを選択します。

6. 一致ルール を展開します。
7. 各一致キー の値を入力します。

データの正規化オプションはデフォルトで選択され、一致する前にデータ入力が正規化されます。データを正規化しない場合は、データの正規化オプションの選択を解除します。

> **Tip**
>
> 一致 ID を見つけるために、できるだけ多くの値を入力します。

8. [検索] を選択します。
9. 対応する一致 ID と、一致に使用された関連ルールを表示します。

ルールベースまたは ML ベースのマッチングワークフローからレコードを削除する

データ管理規制に準拠する必要がある場合は、ルールベースまたは ML ベースのマッチングワークフローからレコードを削除できます。

ルールベースまたは ML ベースのマッチングワークフローからレコードを削除するには

1. にサインイン AWS Management Console し AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、一致 を選択します。
3. ルールベースまたは ML ベースのマッチングワークフローを選択します。
4. 一致するワークフローの詳細ページで、アクションドロップダウンリストから一意の IDs の削除を選択します。
5. 「一意の IDIDs を入力します。

   最大 10 IDsを入力できます。
6. 一意の IDsを削除する入力ソースを指定します。

   ワークフローの入力ソースが 1 つだけの場合、入力ソースはデフォルトで一覧表示されます。

   1 つの入力ソース のみを指定した場合、他の入力ソースIDs は影響を受けません。
7. 一意の IDs の削除 を選択します。

ID 名前空間の管理

ID 名前空間は、次の方法で管理できます。

トピック

ID 名前空間を編集する

ID 名前空間は、ID マッピングワークフローに関連付ける前にのみ編集できます。ID 名前空間を ID マッピングワークフローに関連付けた後は、編集できません。

ID 名前空間を編集するには：

1. にサインイン AWS Management Console し、 でAWS Entity Resolution コンソールを開きます AWS アカウント （まだ開いていない場合）。
2. 左側のナビゲーションペインのデータ準備 で、ID 名前空間 を選択します。
3. ID 名前空間を選択します。
4. [編集] を選択します。
5. ID 名前空間の編集ページで、必要な変更を加え、保存を選択します。

ID 名前空間を削除する

ID マッピングワークフローに関連付けられている ID 名前空間は削除できません。スキーママッピングを削除する前に、まず関連付けられているすべての ID マッピングワークフローからスキーママッピングを削除する必要があります。

ID 名前空間を削除するには：

1. にサインイン AWS Management Console し、 でAWS Entity Resolution コンソールを開きます AWS アカウント （まだ開いていない場合）。
2. 左側のナビゲーションペインのデータ準備 で、ID 名前空間 を選択します。
3. ID 名前空間を選択します。

4. [削除] を選択します。
5. 削除を確定し、[削除] を選択します。

リソースポリシーの追加または更新

リソースポリシーは、ID マッピングリソースの作成者が ID 名前空間リソースにアクセスすることを許可します。

リソースポリシーを追加または更新するには

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、ID 名前空間 を選択します。
3. ID 名前空間を選択します。
4. ID 名前空間の詳細ページで、アクセス許可タブを選択します。
5. リソースポリシー セクションで、編集 を選択します。
6. JSON エディタでポリシーを追加または更新します。
7. [変更を保存] を選択します。

ID マッピングワークフローの管理

ID マッピングワークフローは、次の方法で管理できます。

トピック

- ID マッピングワークフローを編集する
- ID マッピングワークフローを削除する
- リソースポリシーの追加または更新

ID マッピングワークフローを編集する

ID マッピングワークフローを編集するには：

1. にサインイン AWS Management Console し AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。

2. 左側のナビゲーションペインのワークフロー で、ID マッピング を選択します。
3. ID マッピングワークフローを選択します。
4. ID マッピングワークフローの詳細ページの右上隅にある 編集 を選択します。
5. 「ID マッピングワークフローの詳細を指定」ページで、必要な変更を加え、次へ を選択します。
6. データ出力の指定ページで、必要な変更を加え、次へ を選択します。
7. 確認と保存ページで、必要な変更を加え、保存を選択します。

ID マッピングワークフローを削除する

ID マッピングワークフローを削除するには：

1. にサインイン AWS Management Console し AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、ID マッピング を選択します。
3. ID マッピングワークフローを選択します。
4. ID マッピングワークフローの詳細ページの右上隅にある「削除」を選択します。
5. 削除を確定し、[削除] を選択します。

リソースポリシーの追加または更新

リソースポリシーは、ID マッピングリソースの作成者が ID 名前空間リソースにアクセスすることを許可します。

リソースポリシーを追加または更新するには

1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、ID マッピング を選択します。
3. ID マッピングワークフローを選択します。
4. ID マッピングワークフローの詳細ページで、アクセス許可タブを選択します。
5. リソースポリシー で、セクション 編集 を選択します。
6. JSON エディタでポリシーを追加または更新します。
7. [変更を保存] を選択します。

ワークフローのトラブルシューティング

次の情報は、ワークフローの実行時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

エラーファイルを受信しました。

エラーファイルのレコードは、次の理由で作成できます。

- 一意の ID は次のとおりです。
  - null
  - データ行に がない
  - データテーブルのレコードに がない
  - データテーブル内の別の行のデータで繰り返される
  - 指定されていません
  - 同じソース内で一意ではない
  - 複数のソース間で一意ではない
  - ソース間で重複する
- スキーママッピングのフィールドの 1 つに予約名が含まれています。
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - MatchID
  - HashingProtocol
  - ConfidenceLevel
  - ソース

前述の理由でエラーファイルのレコードが作成された場合、サービスの処理コストが発生するため、料金が発生します。エラーファイルのレコードが内部サーバーエラーによるものである場合、料金は発生しません。

AWS Entity Resolution でのセキュリティ

AWS では、クラウドセキュリティを最優先事項としています。AWS のユーザーは、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを利用できます。

セキュリティは、AWS とユーザーの間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — AWS は、AWS クラウド で AWS のサービス を実行するインフラストラクチャを保護する責任を負います。また AWS は、お客様が使用するサービスを安全に提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Entity Resolution に適用するコンプライアンスプログラムの詳細については、コンプライアンスプログラムによる対象範囲内の AWS のサービスをご参照ください。
- クラウド内のセキュリティ — お客様の責任は、使用する AWS のサービス に応じて異なります。また、お客様は、データの機密性、お客様の会社の要件、および適用される法律および規制など、その他の要因についても責任を負います。

このドキュメントは、AWS Entity Resolution を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。次のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために AWS Entity Resolution を設定する方法を示します。また、AWS Entity Resolution リソースのモニタリングや保護に役立つ、他の AWS のサービスの使用方法についても説明します。

トピック

- でのデータ保護 AWS Entity Resolution
- の Identity and Access Management AWS Entity Resolution
- のコンプライアンス検証 AWS Entity Resolution
- AWS Entity Resolution での耐障害性

でのデータ保護 AWS Entity Resolution

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Entity Resolution。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに

対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された記事「AWS 責任共有モデルおよび GDPR」を参照してください。

データ保護の目的で、 認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、AWS Entity Resolution または SDK を使用して AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

の保管中のデータ暗号化 AWS Entity Resolution

AWS Entity Resolution はデフォルトで暗号化を提供し、 AWS 所有の暗号化キーを使用して保管中の顧客の機密データを保護します。

AWS 所有キー – デフォルトでこれらのキー AWS Entity Resolution を使用して、個人を特定できるデータを自動的に暗号化します。 AWS が所有するキーを表示、管理、使用したり、その使用を監査したりすることはできません。ただし、データを暗号化するキーを保護するためにアクションを実

行する必要はありません。詳細については、AWS Key Management Service デベロッパーガイド の「AWS 所有キー」を参照してください。

保管中のデータをデフォルトで暗号化して、機密データの保護に伴う運用のオーバーヘッドと複雑な作業を軽減できます。同時に、これを使用して、厳格な暗号化コンプライアンスと規制要件を満たす安全なアプリケーションを構築できます。

または、一致するワークフローリソースを作成するときに、暗号化用のカスタマーマネージド KMS キーを指定することもできます。

カスタマーマネージドキー — 機密データの暗号化を可能にするために作成、所有、管理する対称カスタマーマネージド KMS キーの使用 AWS Entity Resolution をサポートします。この暗号化層はユーザーが完全に制御できるため、次のようなタスクを実行できます。

- キーポリシーの策定と維持
- IAM ポリシーとグラントの策定と維持
- キーポリシーの有効化と無効化
- 暗号化素材のローテーション
- タグの追加
- キーエイリアスの作成
- キー削除のスケジュール設定

詳細については、「 AWS Key Management Service デベロッパーガイド」の「カスタマーマネージドキー」を参照してください。

の詳細については AWS KMS、AWS Key Management Service とは」を参照してください。

キー管理

で 許可 AWS Entity Resolution を使用する方法 AWS KMS

AWS Entity Resolution には、カスタマーマネージドキーを使用するための許可が必要です。カスタマーマネージドキーで暗号化された一致するワークフローを作成すると、 は にCreateGrantリクエストを送信して、ユーザーに代わってグラント AWS Entity Resolution を作成します AWS KMS。の許可 AWS KMS は、顧客アカウントの KMS キー AWS Entity Resolution へのアクセスを許可するために使用されます。 AWS Entity Resolution では、以下の内部オペレーションでカスタマーマネージドキーを使用するには許可が必要です。

- カスタマーマネージドキーで暗号化されたデータキーを生成する AWS KMS には、にGenerateDataKeyリクエストを送信します。
- Decrypt リクエストを AWS KMS に送信して、暗号化されたデータキーを復号し、データの暗号化に使用できます。

任意のタイミングで、許可に対するアクセス権を取り消したり、カスタマーマネージドキーに対するサービスからのアクセス権を削除したりできます。これを行う AWS Entity Resolution と、カスタマーマネージドキーによって暗号化されたデータにアクセスできなくなり、そのデータに依存するオペレーションに影響します。例えば、グラントを通じてキーへのサービスアクセスを削除し、カスタマーキーで暗号化された一致するワークフローのジョブを開始しようとすると、オペレーションはAccessDeniedException工ラーを返します。

カスタマーマネージドキーの作成

対称カスタマーマネージドキーを作成するには AWS Management Console、、、または AWS KMS APIsを使用します。

対称カスタマーマネージドキーを作成するには

AWS Entity Resolution は、対称暗号化 KMS キー を使用した暗号化をサポートします。AWS Key Management Service デベロッパーガイドにある対称カスタマーマネージドキーの作成ステップを実行します。

キーポリシーステートメント

キーポリシーは、カスタマーマネージドキーへのアクセスを制御します。すべてのカスタマーマネージドキーには、キーポリシーが 1 つだけ必要です。このポリシーには、そのキーを使用できるユーザーとその使用方法を決定するステートメントが含まれています。カスタマーマネージドキーを作成する際に、キーポリシーを指定することができます。詳細については、「 AWS Key Management Service デベロッパーガイド」の「カスタマーマネージドキーへのアクセスの管理」を参照してください。

AWS Entity Resolution リソースでカスタマーマネージドキーを使用するには、キーポリシーで次の API オペレーションを許可する必要があります。

- kms:DescribeKey – キー ARN、作成日 (および該当する場合は削除日) 、キーの状態、キーマテリアルのオリジンと有効期限 (存在する場合) などの情報を提供します。これには、さまざまなタイプの KMS キーを区別KeySpecするのに役立つ などのフィールドが含まれています。ま

た、キーの使用状況 (暗号化、署名、または MACs) と、KMS キーがサポートするアルゴリズムも表示されます。 AWS Entity Resolution KeySpec は SYMMETRIC_DEFAULT、 KeyUsage は ですENCRYPT_DECRYPT。

- kms:CreateGrant - カスタマーマネージドキーに許可を追加します。指定された KMS キーへのアクセスを制御する権限。これにより、必要な権限付与オペレーション AWS Entity Resolution へのアクセスが可能になります。詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS でのグラント」を参照してください。

これにより、 AWS Entity Resolution は以下を実行できます。

- GenerateDataKey を呼び出して、暗号化されたデータキーを生成して保存します。データキーは暗号化にすぐには使用されないからです。
- Decrypt を呼び出して、保存されている暗号化データキーを使用して暗号化されたデータにアクセスします。
- RetireGrant へのサービスを許可するために、削除プリンシパルを設定します。

に追加できるポリシーステートメントの例を次に示します 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"
        }
      }
}
```

ユーザーのアクセス許可

暗号化のデフォルトキーとして KMS キーを設定すると、デフォルトの KMS キーポリシーにより、必要な KMS アクションにアクセスできるすべてのユーザーがこの KMS キーを使用してリソースを

暗号化または復号できるようになります。カスタマーマネージド KMS キー暗号化を使用するには、次のアクションを呼び出すアクセス許可をユーザーに付与する必要があります。

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

CreateMatchingWorkflow リクエスト中、 AWS Entity Resolution はユーザーに代わって DescribeKeyおよび CreateGrantリクエストを AWS KMS に送信します。これには、カスタマー管理の KMS キーを使用してCreateMatchingWorkflowリクエストを行う IAM エンティティが KMS キーポリシーに対するkms:DescribeKeyアクセス許可を持っている必要があります。

CreateIdMappingWorkflow および StartIdMappingJobリクエスト中、 AWS Entity Resolution はユーザーに代わって DescribeKeyおよび CreateGrantリクエストを AWS KMS に送信します。これには、 と を行う IAM エンティティがCreateIdMappingWorkflow、カスタマーマネージド KMS キーを使用して KMS キーポリシーに対するkms:DescribeKeyアクセス許可を持っていることをStartIdMappingJobリクエストする必要があります。プロバイダーは、カスタマーマネージドキーにアクセスして AWS Entity Resolution Amazon S3 バケット内のデータを復号化できます。

プロバイダーが AWS Entity Resolution Amazon S3 バケット内のデータを復号化するために追加できるポリシーステートメントの例を次に示します。

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

```
}
```

各 ################ を独自の情報に置き換えます。

<KMSKeyARN >	AWS KMS Amazon リソースネーム。

同様に、StartMatchingJobAPI を呼び出す IAM エンティティには、一致するワークフローで提供されるカスタマーマネージド KMS キーに対する kms:Decryptおよび アクセスkms:GenerateDataKey許可が必要です。

ポリシー でのアクセス許可の指定の詳細については、「AWS Key Management Service デベロッパーガイド」を参照してください。

キーアクセスのトラブルシューティングの詳細については、「AWS Key Management Service デベロッパーガイド」を参照してください。

のカスタマーマネージドキーの指定 AWS Entity Resolution

カスタマーマネージドキーは、以下のリソースの第 2 レイヤー暗号化として指定できます。

ワークフローの一致 — 一致するワークフローリソースを作成するときに、KMSArn KMSArnは、AWS Entity Resolution を使用して、リソースに保存されている識別可能な個人データを暗号化します。

KMSArn – AWS KMS カスタマーマネージドキーのキー識別子であるキー ARN を入力します。

2 つの で ID マッピングワークフローを作成または実行している場合、カスタマーマネージドキーを次のリソースの 2 番目のレイヤー暗号化として指定できます AWS アカウント。

ID マッピングワークフローまたは ID マッピングワークフローの開始 – ID マッピングワークフローリソースを作成するか、ID マッピングワークフロージョブを開始するときに、KMSArnは、 AWS Entity Resolution を使用して、リソースに保存されている識別可能な個人データを暗号化します。

KMSArn – AWS KMS カスタマーマネージドキーのキー識別子であるキー ARN を入力します。

Service の AWS Entity Resolution 暗号化キーのモニタリング

AWS Entity Resolution サービスリソースで AWS KMS カスタマーマネージドキーを使用する場合、AWS CloudTrail または Amazon CloudWatch Logs を使用して、 AWS Entity Resolution が に送信するリクエストを追跡できます AWS KMS。

次の例はCreateGrant、カスタマーマネージドキーによって暗号化されたデータにアクセスDescribeKeyするために によって呼び出される AWS KMS オペレーションをモニタリング AWS Entity Resolution するための Decrypt、、、および GenerateDataKeyの AWS CloudTrail イベントです。

トピック

- CreateGrant
- DescribeKey
- GenerateDataKey
- Decrypt

CreateGrant

AWS KMS カスタマーマネージドキーを使用して一致するワークフローリソースを暗号化すると、はユーザーに代わって の KMS キーにアクセスするCreateGrantリクエスト AWS Entity Resolution を送信します AWS アカウント。が AWS Entity Resolution 作成する許可は、 AWS KMS カスタマーマネージドキーに関連付けられたリソースに固有です。さらに、 RetireGrantオペレーション AWS Entity Resolution を使用して、リソースを削除するときにグラントを削除します。

以下のイベント例では CreateGrant オペレーションを記録しています。

```
{
    "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 は DescribeKeyオペレーションを使用して、一致するリソースに関連付けられた AWS KMS カスタマーマネージドキーがアカウントとリージョンに存在するかどうかを確認します。

次のイベント例では、 DescribeKeyオペレーションを記録します。

```
{
    "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

一致するワークフローリソースの AWS KMS カスタマーマネージドキーを有効にすると、 は Amazon Simple Storage Service (Amazon S3) を介して、リソースの AWS KMS カスタマーマネージドキーを指定する にGenerateDataKeyリクエスト AWS Entity Resolution を送信します。 AWS KMS

次のイベント例では、 GenerateDataKeyオペレーションを記録します。

```
{
    "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

一致するワークフローリソースの AWS KMS カスタマーマネージドキーを有効にすると、 は Amazon Simple Storage Service (Amazon S3) を介して、リソースの AWS KMS カスタマーマネージドキー AWS KMS を指定する にDecryptリクエスト AWS Entity Resolution を送信します。

次のイベント例では、 Decryptオペレーションを記録します。

```
{
    "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"
}
```


考慮事項

AWS Entity Resolution は、新しいカスタマーマネージド KMS キーを使用したマッチングワークフローの更新をサポートしていません。このような場合は、カスタマーマネージド KMS キーを使用して新しいワークフローを作成できます。

詳細はこちら

次のリソースは、保管時のデータ暗号化についての詳細を説明しています。

AWS Key Management Service の基本概念 の詳細については、「 AWS Key Management Service デベロッパーガイド」を参照してください。

AWS Key Management Service のセキュリティのベストプラクティスの詳細については、「 デベロッパーガイド」を参照してください。 AWS Key Management Service

インターフェイスエンドポイント (AWS PrivateLink) AWS Entity Resolution を使用した へのアクセス

を使用して AWS PrivateLink 、VPC と の間にプライベート接続を作成できます AWS Entity Resolution。インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect

接続を使用せずに、VPC 内にある AWS Entity Resolution かのように にアクセスできます。VPC のインスタンスは、パブリック IP アドレスがなくても AWS Entity Resolutionにアクセスできます。

このプライベート接続を確立するには、 AWS PrivateLinkを利用したインターフェイスエンドポイントを作成します。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらは、 AWS Entity Resolution宛てのトラフィックのエントリポイントとして機能するリクエスタ管理型ネットワークインターフェイスです。

詳細については、「 AWS PrivateLink ガイド」の「 AWS のサービス によるアクセス AWS PrivateLink」を参照してください。

に関する考慮事項 AWS Entity Resolution

のインターフェイスエンドポイントを設定する前に AWS Entity Resolution、「 AWS PrivateLink ガイド」の「考慮事項」を参照してください。

AWS Entity Resolution は、インターフェイスエンドポイントを介したすべての API アクションの呼び出しをサポートします。

VPC エンドポイントポリシーは、 ではサポートされていません AWS Entity Resolution。デフォルトでは、インターフェイスエンドポイント経由での AWS Entity Resolution への完全なアクセスが許可されます。または、セキュリティグループをエンドポイントのネットワークインターフェイスに関連付けて、インターフェイスエンドポイント経由での AWS Entity Resolution へのトラフィックを制御することもできます。

のインターフェイスエンドポイントを作成する AWS Entity Resolution

Amazon VPC コンソールまたは AWS Command Line Interface () AWS Entity Resolution を使用して、 のインターフェイスエンドポイントを作成できますAWS CLI。詳細については、「AWS PrivateLink ガイド」の「インターフェイスエンドポイントを作成」を参照してください。

次のサービス名 AWS Entity Resolution を使用して、 用のインターフェイスエンドポイントを作成します。

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

インターフェイスエンドポイントのプライベート DNS を有効にすると、リージョンのデフォルト DNS 名を使用して、 AWS Entity Resolution への API リクエストを実行できます。例えば `entityresolution.us-east-1.amazonaws.com` です。

インターフェイスエンドポイントのエンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイスエンドポイント AWS Entity Resolution を介した へのフルアクセスが許可されます。VPC AWS Entity Resolution から に許可されるアクセスを制御するには、カスタムエンドポイントポリシーをインターフェイスエンドポイントにアタッチします。

エンドポイントポリシーは、以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)。
- 実行可能なアクション。
- このアクションを実行できるリソース。

詳細については、AWS PrivateLink ガイドのControl access to services using endpoint policies (エンドポイントポリシーを使用してサービスへのアクセスをコントロールする)を参照してください。

例: AWS Entity Resolution アクションの VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。このポリシーをインターフェイスエンドポイントにアタッチすると、すべてのリソースのすべてのプリンシパルに対して、リストされている AWS Entity Resolution アクションへのアクセスが許可されます。

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

の Identity and Access Management AWS Entity Resolution

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Entity Resolution リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

> **Note**
>
> AWS Entity Resolution はクロスアカウントポリシーをサポートしています。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、 で行う作業によって異なります AWS Entity Resolution。

サービスユーザー – AWS Entity Resolution サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの AWS Entity Resolution 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者から適切な権限をリクエストするのに役に立ちます。 AWS Entity Resolution機能にアクセスできない場合は、「AWS Entity Resolution ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内の AWS Entity Resolution リソースを担当している場合は、通常、 へのフルアクセスがあります AWS Entity Resolution。サービスユーザーがどの AWS Entity Resolution 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で IAM を で使用する方法の詳細については、 AWS Entity Resolution「」を参照してくださいと IAM の AWS Entity Resolution 連携方法。

IAM 管理者 - 管理者は、 AWS Entity Resolutionへのアクセスを管理するポリシーの書き込み方法の詳細について確認する場合があります。IAM で使用できる AWS Entity Resolution アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Entity Resolutionのアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証（ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 にサインインする方法 AWS アカウントAWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用することをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての AWS のサービス およびリソースへの完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリのユーザー、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「IAM Identity Center とは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイド の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。

クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「IAM ユーザーガイド」の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、『Amazon Simple Storage Service デベロッパーガイド』の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS

アカウント ビジネスが所有する複数の をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、AWS Organizations ユーザーガイドの「SCP の仕組み」を参照してください。

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

と IAM の AWS Entity Resolution 連携方法

IAM を使用して へのアクセスを管理する前に AWS Entity Resolution、 で使用できる IAM 機能について学びます AWS Entity Resolution。

で使用できる IAM の機能 AWS Entity Resolution

IAM 機能	AWS Entity Resolution サポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	はい
ポリシーアクション	Yes
ポリシーリソース	Yes
ポリシー条件キー	Yes

IAM 機能	AWS Entity Resolution サポート
ACL	No
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	はい
転送アクセスセッション (FAS)	はい
サービスロール	あり
サービスリンクロール	いいえ

AWS Entity Resolution およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

のアイデンティティベースのポリシー AWS Entity Resolution

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

のアイデンティティベースのポリシーの例 AWS Entity Resolution

AWS Entity Resolution アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Entity Resolutionのアイデンティティベースのポリシーの例。

内のリソースベースのポリシー AWS Entity Resolution

リソースベースのポリシーのサポート	はい

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

のポリシーアクション AWS Entity Resolution

ポリシーアクションに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーのAction要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレー

ションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

AWS Entity Resolution アクションのリストを確認するには、「サービス認証リファレンス」の「 で定義されるアクション AWS Entity Resolution」を参照してください。

のポリシーアクションは、アクションの前に次のプレフィックス AWS Entity Resolution を使用します。

```
entityresolution
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

AWS Entity Resolution アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Entity Resolutionのアイデンティティベースのポリシーの例。

のポリシーリソース AWS Entity Resolution

ポリシーリソースに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

AWS Entity Resolution リソースタイプとその ARNs」の「 で定義されるリソース AWS Entity Resolution」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、「AWS Entity Resolutionで定義されるアクション」を参照してください。

AWS Entity Resolution アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Entity Resolutionのアイデンティティベースのポリシーの例。

のポリシー条件キー AWS Entity Resolution

サービス固有のポリシー条件キーのサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

AWS Entity Resolution 条件キーのリストを確認するには、「サービス認証リファレンス」の「 の条件キー AWS Entity Resolution」を参照してください。条件キーを使用できるアクションとリソースについては、「 で定義されるアクション AWS Entity Resolution」を参照してください。

AWS Entity Resolution アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Entity Resolutionのアイデンティティベースのポリシーの例。

ACLs AWS Entity Resolution

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

での ABAC AWS Entity Resolution

ABAC (ポリシー内のタグ) のサポート	部分的

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。ではAWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、IAM ユーザーガイド の「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセス制御 (ABAC) を使用する」を参照してください。

での一時的な認証情報の使用 AWS Entity Resolution

一時的な認証情報のサポート	はい

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

の転送アクセスセッション AWS Entity Resolution

転送アクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FASリクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS Entity Resolutionのサービスロール

サービスロールに対するサポート	あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 AWS Entity Resolution 機能が破損する可能性があります。が指示する場合以外 AWS Entity Resolution は、サービスロールを編集しないでください。

のサービスにリンクされたロール AWS Entity Resolution

サービスにリンクされたロールのサポート	いいえ

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の中から、Service-linked role (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、「はい」 リンクを選択します。

AWS Entity Resolutionのアイデンティティベースのポリシーの例

デフォルトでは、 ユーザーおよびロールには、 AWS Entity Resolution リソースを作成または変更する権限はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

各リソースタイプの ARN の形式など AWS Entity Resolution、 で定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンス」の「 のアクション、リソース、および条件キー AWS Entity Resolution」を参照してください。 ARNs

トピック

- ポリシーのベストプラクティス
- AWS Entity Resolution コンソールを使用する
- 自分の権限の表示をユーザーに許可する

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが AWS Entity Resolution リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素: 条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは

100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。

- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

AWS Entity Resolution コンソールを使用する

AWS Entity Resolution コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の AWS Entity Resolution リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが AWS Entity Resolution 引き続きコンソールを使用できるようにするには、エンティティに AWS Entity Resolution *ConsoleAccess*または *ReadOnly* AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "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 の マネージドポリシー AWS Entity Resolution

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケース別にカスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) が更新されます。 は、新しい AWS のサービス が起動されたとき、または既存のサービスで新しい API AWS オペレーションが使用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS 管理ポリシー: AWSEntityResolutionConsoleFullAccess

`AWSEntityResolutionConsoleFullAccess` ポリシーは IAM ID にアタッチできます。

このポリシーは、 AWS Entity Resolution エンドポイントとリソースへのフルアクセスを許可します。

このポリシーでは、S3、タグ付け、 AWS のサービス などの関連 への特定の読み取りアクセスも許可 AWS KMS されるため AWS Glue、コンソールは選択肢を表示し、選択したものを使用してエンティティ解決アクションを実行できます。一部のリソースは、サービス名 を含むように絞り込まれます`entityresolution`。

AWS Entity Resolution は、渡されたロールに依存して関連 AWS リソースに対してアクションを実行するため、このポリシーは、目的のロールを選択して渡すアクセス許可も付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `EntityResolutionAccess` — プリンシパルに AWS Entity Resolution エンドポイントとリソースへのフルアクセスを許可します。
- `GlueSourcesConsoleDisplay` – ユーザーエクスペリエンスのために、データソースオプションとして AWS Glue テーブルを一覧表示し、データソースのテーブルスキーマをインポートするアクセス許可を付与します。
- `S3BucketsConsoleDisplay` – すべての S3 バケットをデータソースオプションとして一覧表示するアクセス許可を付与します。
- `S3SourcesConsoleDisplay` – S3 バケットをデータソースオプションとして表示するためのアクセス許可を付与します。
- `TaggingConsoleDisplay` – タグ付けのキーと値を読み取るアクセス許可を付与します。
- `KMSConsoleDisplay` – データソースを復号化および暗号化するために、 でキーを記述し、エイリアスを一覧表示 AWS Key Management Service するアクセス許可を付与します。

- ListRolesToPickForPassing – すべてのロールを一覧表示するアクセス許可を付与し、ユーザーが渡すロールを選択できるようにします。
- PassRoleToEntityResolutionService – 絞り込まれたロールを AWS Entity Resolution サービスに渡すためのアクセス許可を付与します。
- ManageEventBridgeRules – S3 通知を取得するための Amazon EventBridge ルールを作成、更新、削除するアクセス許可を付与します。
- ADXReadAccess – 顧客がエンタイトルメントまたはサブスクリプションを持っているかどうかを確認する AWS Data Exchange ための へのアクセスを許可します。

```
{
    "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 マネージドポリシー: AWSEntityResolutionConsoleReadOnlyAccess

IAM エンティティに `AWSEntityResolutionConsoleReadOnlyAccess` をアタッチできます。

このポリシーは AWS Entity Resolution 、エンドポイントとリソースへの読み取り専用アクセスを許可します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- EntityResolutionRead — プリンシパルに AWS Entity Resolution エンドポイントとリソースへの読み取り専用アクセスを許可します。

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

AWS Entity ResolutionAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した AWS Entity Resolution 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートを受け取るには、AWS Entity Resolution ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSEntityResolutionConsoleFullAccess – 既存のポリシーの更新	ADXReadAccess および ManageEventBridgeRules を追加して、一致するワークフローでプロバイダーサービスオプションを有効にします。	2023 年 10 月 16 日

変更	説明	日付
AWS Entity Resolution が変更の追跡を開始しました	AWS Entity Resolution が AWS マネージドポリシーの変更の追跡を開始しました。	2023 年 8 月 18 日

AWS Entity Resolution ID とアクセスのトラブルシューティング

次の情報は、 と IAM の使用時に発生する可能性がある一般的な問題の診断 AWS Entity Resolution と修正に役立ちます。

トピック

- でアクションを実行する権限がない AWS Entity Resolution
- iam を実行する権限がありません。PassRole
- 自分の 以外のユーザーに自分の AWS Entity Resolution リソース AWS アカウント へのアクセスを許可したい

でアクションを実行する権限がない AWS Entity Resolution

がアクションを実行する権限がないと AWS Management Console 通知した場合は、管理者に連絡してサポートを依頼する必要があります。管理者とは、ユーザーにユーザー名とパスワードを提供した人です。

以下のエラー例は、mateojackson IAM ユーザーがコンソールを使用して架空の *my-example-widget* リソースに関する詳細情報を表示しようとしているが、架空の entityresolution:*GetWidget* アクセス許可がないという場合に発生します。

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

この場合、Mateo は、entityresolution:*GetWidget* アクションを使用して *my-example-widget* リソースにアクセスできるように、ポリシーの更新を管理者に依頼します。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して AWS Entity Resolutionにロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して AWS Entity Resolutionでアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーに自分の AWS Entity Resolution リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- がこれらの機能 AWS Entity Resolution をサポートしているかどうかを確認するには、「」を参照してくださいと IAM の AWS Entity Resolution 連携方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部認証されたユーザーへのアクセスの提供 (ID フェデレーション) を参照してください。

- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

のコンプライアンス検証 AWS Entity Resolution

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。

- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

AWS Entity Resolution での耐障害性

AWS グローバルインフラストラクチャは AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。AWS リージョン には、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている物理的に独立・隔離された複数のアベイラビリティーゾーンがあります。アベイラビリティーゾーンを使用すると、中断することなくゾーン間で自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用できます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン とアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS では、AWS Entity Resolution グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズに対応できるように複数の機能を提供しています。

モニタリング AWS Entity Resolution

モニタリングは、 AWS Entity Resolution およびその他の AWS ソリューションの信頼性、可用性、およびパフォーマンスを維持する上で重要な部分です。 は、 をモニタリングし AWS Entity Resolution、問題が発生したときに報告し、必要に応じて自動アクションを実行するために、以下のモニタリングツール AWS を提供します。

- AWS CloudTrail は、 によって、または に代わって行われた API コールおよび関連イベントをキャプチャ AWS アカウント し、指定した Amazon S3 バケットにログファイルを配信します。を呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しが発生した日時を特定できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

トピック

- を使用した AWS Entity Resolution API コールのログ記録 AWS CloudTrail

を使用した AWS Entity Resolution API コールのログ記録 AWS CloudTrail

AWS Entity Resolution は と統合されています。これは AWS CloudTrail、ユーザー、ロール、またはのサービスによって実行されたアクションを記録する AWS サービスです AWS Entity Resolution。は、 のすべての API コールをイベント AWS Entity Resolution として CloudTrail キャプチャします。キャプチャされた呼び出しには、 AWS Entity Resolution コンソールからの呼び出しと AWS Entity Resolution API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、 の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます AWS Entity Resolution。証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、 に対するリクエスト AWS Entity Resolution、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については CloudTrail、「 AWS CloudTrail ユーザーガイド」を参照してください。

AWS Entity Resolution の情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 で が有効になります。でアクティビティが発生すると AWS Entity Resolution、そのアクティビティは CloudTrail イベント履歴 の他の AWS

サービスイベントとともにイベントに記録されます。最近のイベントは、 AWS アカウントで表示、検索、ダウンロードできます。詳細については、「イベント履歴 を使用した CloudTrail イベントの表示」を参照してください。

のイベントなど AWS アカウント、 のイベントの継続的な記録については AWS Entity Resolution、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 「証跡作成の概要」
- CloudTrail がサポートするサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

すべての AWS Entity Resolution アクションは によってログに記録 CloudTrail され、 AWS Entity Resolution API リファレンス に記載されています。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して行われたか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、CloudTrail userIdentity 要素」を参照してください。

AWS Entity Resolution ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパ

ラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

を使用した AWS エンティティ解決リソースの作成 AWS CloudFormation

AWS Entity Resolution は AWS CloudFormation、 AWS リソースとインフラストラクチャの作成と管理に費やす時間を短縮できるように、リソースのモデル化とセットアップに役立つサービスであると統合されています。必要なすべての AWS リソース (AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace や など AWS::EntityResolution::PolicyStatement) を記述するテンプレートを作成し、それらのリソースを AWS CloudFormation プロビジョニングして設定します。

を使用すると AWS CloudFormation、テンプレートを再利用して AWS エンティティ解決リソースを一貫して繰り返しセットアップできます。リソースを一度記述し、複数の AWS アカウント およびリージョンで同じリソースを何度もプロビジョニングします。

AWS エンティティ解決と AWS CloudFormation テンプレート

AWS エンティティ解決および関連サービスのリソースをプロビジョニングおよび設定するには、AWS CloudFormation テンプレート を理解する必要があります。テンプレートは、JSON や YAML でフォーマットされたテキストファイルです。これらのテンプレートは、 AWS CloudFormation スタックでプロビジョニングするリソースを記述します。JSON または YAML に慣れていない場合は、 AWS CloudFormation デザイナー を使用して AWS CloudFormation テンプレートの使用を開始できます。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation Designer とは」を参照してください。

AWS Entity Resolution は、 AWS::EntityResolution::PolicyStatement での AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace およびび の作成をサポートしています AWS CloudFormation。および の JSON テンプレートと YAML テンプレートの例を含む詳細については、 AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace 「 ユーザーガイド」の「AWS エンティティ解決リソースタイプのリファレンスAWS CloudFormation AWS::EntityResolution::PolicyStatement」を参照してください。

次のテンプレートを使用できます。

- マッチングワークフロー

  実行するデータ処理ジョブの設定を保存する `MatchingWorkflow` オブジェクトを作成します。

  詳細については、次のトピックを参照してください。

  「AWS CloudFormation ユーザーガイド」の「AWS::EntityResolution::MatchingWorkflow」

  「CreateMatchingWorkflow API リファレンス」の「AWS Entity Resolution 」
- スキーママッピング

  入力カスタマーレコードテーブルのスキーマを定義するスキーママッピングを作成します。

  詳細については、次のトピックを参照してください。

  「AWS CloudFormation ユーザーガイド」の「AWS::EntityResolution::SchemaMapping」

  「CreateSchemaMapping API リファレンス」の「AWS Entity Resolution 」
- ID マッピングワークフロー

  実行するデータ処理ジョブの設定を保存する `IdMappingWorkflow` オブジェクトを作成します。

  詳細については、次のトピックを参照してください。

  「AWS CloudFormation ユーザーガイド」の「AWS::EntityResolution::IdMappingWorkflow」

  「CreateIdMappingWorkflow API リファレンス」の「AWS Entity Resolution 」
- ID 名前空間

  オブジェクトを作成します。オブジェクトには`IdNamespace`、データセットとその使用方法を説明するメタデータが保存されます。

  詳細については、次のトピックを参照してください。

  「AWS CloudFormation ユーザーガイド」の「AWS::EntityResolution::IdNamespace」

  「CreateIdNamespace API リファレンス」の「AWS Entity Resolution 」
- PolicyStatement

  `PolicyStatement` オブジェクトを作成します。

  詳細については、次のトピックを参照してください。

「AWS CloudFormation ユーザーガイド」の「AWS::EntityResolution::PolicyStatement」

「AddPolicyStatement API リファレンス」の「AWS Entity Resolution 」

の詳細 AWS CloudFormation

の詳細については AWS CloudFormation、以下のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド
- AWS CloudFormation API リファレンス
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

のクォータ AWS Entity Resolution

には、 ごとに、以前 AWS アカウント は制限と呼ばれていたデフォルトのクォータがあります AWS のサービス。特に明記されていない限り、クォータは地域固有です。一部のクォータの引き上げをリクエストできますが、他のクォータは引き上げできません。

のクォータを表示するには AWS Entity Resolution、Service Quotas コンソール を開きます。ナビゲーションペインで、[AWS のサービス] を選択し、[AWS Entity Resolution] を選択します。

クォータの引き上げをリクエストするには、Service Quotas ユーザーガイド の「クォータ引き上げリクエスト」を参照してください。Service Quotas でクォータがまだ利用できない場合は、制限の引き上げ フォームを使用します。

には、 に関連する次のクォータ AWS アカウント があります AWS Entity Resolution。

名前	デフォルト	引き上げ可能	説明
同時 ID マッピングジョブ	1	いいえ	現在の で同時に処理できる ID マッピングジョブの最大数 AWS リージョン。
同時マッチングジョブ	1	いいえ	現在の で同時に処理できるマッチングジョブの最大数 AWS リージョン。
同時プロバイダーサービスマッチングジョブ	1	いいえ	現在の で同時に処理できるプロバイダーサービスマッチングジョブの最大数 AWS リージョン。
データ入力	20	いいえ	これは、マッチングワークフローで使用する入力テーブルのリストです。各入力は、 AWS Glue 入力データテーブルの列に対応します。このテーブルには、列名と、 がマッチングの目的で AWS Entity Resolution 使用する追加情報が含まれています。入力には、一意の ID と少なくとも 1 つの追加入力フィールドが含まれている必要があります。

名前	デフォルト	引き上げ可能	説明
データ出力	750	いいえ	これは`OutputAttribute` オブジェクトのリストで、それぞれに名前とハッシュ化された というフィールドがあります。これらの各オブジェクトは、 AWS Glue 出力テーブルに含める列と、列内の値をハッシュするかどうかを表します。
データスキーマ	25	いいえ	データスキーマ入力フィールドの最大数。
ID マッピングワークフロー	10	はい	現在の AWS アカウント でこの で作成できる ID マッピングワークフローの最大数 AWS リージョン。
ID 名前空間	10	[Yes (はい)]	現在の AWS アカウント でこの で作成できる ID 名前空間の最大数 AWS リージョン。
IDs一致	500	いいえ	ワークロードごとに 1 つの MatchID で統合できるレコードの最大数。
一致ルール	15	いいえ	ルールベースのマッチングの場合、これは、一致したレコードセットを生成するために適用されたルール番号です。これは、出力に含まれるワークフローメタデータのマッチングの一部です。
ワークフローのマッチング	10	はい	マッチングワークフローの最大数。
ワークフローあたりのルールの数	15	いいえ	マッチングワークフローあたりのルールの最大数。

名前	デフォルト	引き上げ可能	説明
GetMatchId API リクエストのレート	50	はい	1 秒あたりの GetCustomerID API リクエストの最大数。
スキーママッピング	50	はい	このアカウントで現在の AWS リージョンに作成できるスキーママッピングの最大数。
ルールセットあたりの一意の一致キー	15	いいえ	ルールセットあたりの一意の一致キーの最大数。一致キーは AWS Entity Resolution 、類似データと見なされる入力フィールドと異なるデータと見なされる入力フィールドを指示します。これにより、ルールベースのマッチングルール AWS Entity Resolution を自動的に設定し、さまざまな入力フィールドに保存されている同様のデータを比較できます。

API スロットリングのクォータ

リソース	デフォルト	[Description] (説明)
GetMatchId リクエストのレート	50 TPS	1 秒あたりの GetMatchId API コールの最大数。

AWS Entity Resolution ユーザーガイドのドキュメント履歴

次の表に、 のドキュメントリリースを示します AWS Entity Resolution。

このドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。RSS の更新をサブスクリプションするには、使用しているブラウザで RSS プラグインを有効にする必要があります。

変更	説明	日付
マッチングワークフロー – 更新	顧客は、データ管理規制への準拠に役立つように、ルールベースまたは ML ベースのマッチングワークフローからレコードを削除できるようになりました。	2024 年 4 月 8 日
ID マッピングワークフロー – 更新	お客様は、複数の で ID マッピングワークフローを使用できるようになりました AWS アカウント。	2024 年 4 月 2 日
AWS CloudFormation リソース - 新規および更新されたリソース	AWS Entity Resolution に次のリソースが追加されました: `AWS::EntityResolution::IdNamespace` `AWS::EntityResolution::PolicyStatement` および は次のリソースを更新しました: `AWS::EntityResolution::IdMappingWorkflow` 。	2024 年 4 月 2 日
一致 ID の検索	お客様は、処理されたルールベースのワークフローに対応する一致 ID と関連するルール	2024 年 3 月 25 日

	を見つけることができるようになりました。	
マッチングワークフロー – 更新	AWS Entity Resolution は、LiveRamp プロバイダーのサービスベースのマッチングワークフローで PII ベースの RAMPID 割り当てをサポートするようになりました。	2024 年 2 月 12 日
AWS PrivateLink	AWS Entity Resolution は、 でホスト AWS PrivateLink されている のサービスにお客様がプライベートにアクセスできるように、 で追加のデータセキュリティをサポートするようになりました AWS。	2023 年 10 月 20 日
AWS CloudFormation リソース — 新規および更新されたリソース	AWS Entity Resolution では、次のリソースが追加されました。 `AWS::EntityResolution:IdMappingWorkflow` および のリソースが更新され`AWS::EntityResolution::MatchingWorkflow` ましたAWS::EntityResolution::Schemamapping 。	2023 年 10 月 19 日
既存のポリシーの更新	`AWSEntityResolutionConsoleFullAccess` 管理ポリシーに次の新しいアクセス許可が追加されました: `ADXReadAccess` および `ManageEventBridgeRules` 。	2023 年 10 月 16 日

スキーママッピング – 更新	お客様は、既存のデータスキーマを編集および更新できるようになりました。	2023 年 10 月 16 日
マッチングワークフロー – 更新	お客様は、データの照合とリンクに役立つ任意のデータプロバイダーサービスを選択できるようになりました。	2023 年 10 月 16 日
ID マッピングワークフロー	お客様はこの新しいワークフローを使用して、ID マッピングの詳細を指定し、目的の ID マッピング方法を選択し、データ入力フィールドと出力フィールドを指定できます。	2023 年 10 月 16 日
AWS CloudFormation 統合	AWS Entity Resolution が と統合されるようになりました AWS CloudFormation。	2023 年 8 月 24 日
AWS マネージドポリシーの更新 - 新しいポリシー	AWS Entity Resolution は 2 つの新しい マネージドポリシーを追加しました。	2023 年 8 月 18 日
初回リリース	AWS Entity Resolution ユーザーガイドの初回リリース	2023 年 7 月 26 日

AWS Entity Resolution 用語集

Amazon リソースネーム (ARN)

AWS リソースの一意の識別子。ARNs は、 AWS Entity Resolution ポリシー、Amazon Relational Database Service (Amazon RDS) タグ AWS Entity Resolution、API コールなど、すべての でリソースを明確に指定する必要がある場合に必要です。 Amazon Relational Database Service

自動処理

一致するワークフロージョブの処理頻度オプション。データ入力が変更されると自動的に で実行できます。

このオプションは、ルールベースのマッチングでのみ使用できます。

デフォルトでは、一致するワークフロージョブの処理頻度は手動に設定され、オンデマンドで実行できます。データ入力が変更されると、一致するワークフロージョブを自動的に実行するように自動処理を設定できます。これにより、一致するワークフロー出力が維持されます up-to-date。

AWS KMS key ARN

これは、保管時の暗号化用の AWS KMS Amazon リソースネーム (ARN) です。指定しない場合、システムは AWS Entity Resolution マネージド KMS キーを使用します。

クリアテキスト

暗号化で保護されていないデータ。

信頼度 (ConfidenceLevel)

ML マッチングの場合、ML が一致レコードセットを識別する AWS Entity Resolution ときに によって適用される信頼レベルです。これは、出力に含まれる一致するワークフローメタデータの一部です。

復号

暗号化されたデータを元の形式に戻すプロセスです。復号化は、シークレットキーにアクセスできる場合にのみ実行できます。

暗号化

キーと呼ばれる秘密の値を使用して、データをランダムに見える形式にエンコードするプロセスです。キーにアクセスしない限り、元のプレーンテキストを特定することはできません。

グループ名

グループ名は入力フィールドのグループ全体を参照し、解析されたデータをグループ化して照合するのに役立ちます。

例えば、、**first_name**、および の 3 つの入力フィールドがある場合**last_name**、グループ名に一致と出力**full_name**の **middle_name**と入力することで、それらをグループ化できます。

ハッシュ

ハッシュとは、固定サイズの不可逆的で一意の文字列を生成する暗号化アルゴリズムを適用することを意味します。これは hash. AWS Entity Resolution uses Secure Hash Algorithm 256-bit (SHA256) ハッシュプロトコルと呼ばれ、32 バイトの文字列を出力します。では AWS Entity Resolution、出力でデータ値をハッシュするかどうかを選択できます。

ハッシュプロトコル (HashingProtocol)

AWS Entity Resolution は Secure Hash Algorithm 256 ビット (SHA256) ハッシュプロトコルを使用し、32 バイトの文字列を出力します。これは、出力に含まれる一致するワークフローメタデータの一部です。

ID マッピングワークフロー

ID を変換する入力データと IDsマッピングの実行方法を指定するように設定したプロセス。

AWS Entity Resolution は現在、ID マッピングメソッド LiveRamp として をサポートしています。ID マッピングワークフロー AWS Data Exchange を使用するには、 LiveRamp から へのサブスクリプションが必要です。

詳細については、「でプロバイダーサービスをサブスクライブする AWS Data Exchange」を参照してください。

ID 名前空間

複数の AWS アカウント にわたるデータセットを説明するメタデータと、ID マッピングワークフロー でこれらのデータセットを使用する方法 AWS Entity Resolution を含む のリソース。

ID 名前空間には、 SOURCEと の 2 種類がありますTARGET。には、ID マッピングワークフローで処理されるソースデータの設定SOURCEが含まれています。には、すべてのソースが解決されるターゲットデータの設定TARGETが含まれています。2 つの で解決する入力データを定義するには AWS アカウント、ID 名前空間ソースと ID 名前空間ターゲットを作成して、データを 1 つのセット (SOURCE) から別のセット () に変換しますTARGET。

自分と別のメンバーが ID 名前空間を作成して ID マッピングワークフローを実行したら、 でコラボレーションに参加 AWS Clean Rooms して ID マッピングテーブルでマルチテーブル結合を実行し、データを分析できます。

詳細については、『AWS Clean Rooms ユーザーガイド』を参照してください。

入力フィールド

入力フィールドは、 AWS Glue 入力データテーブルの列名に対応します。

入力ソース ARN (InputSourceARN)

AWS Glue テーブル入力用に生成された Amazon リソースネーム (ARN)。これは、出力に含まれるワークフローメタデータのマッチングの一部です。

入力タイプ

入力データのタイプ。これは、名前、住所、電話番号、E メールアドレスなどの事前設定された値リストから選択します。入力タイプは、どの種類のデータを表示する AWS Entity Resolution かを指定するため、分類と正規化を適切に行うことができます。

機械学習ベースのマッチング

機械学習ベースのマッチング (ML マッチング) は、データ全体で、不完全であるか、まったく同じように見えない可能性のある一致を検索します。ML マッチングは、入力するすべてのデータのレコー

ドを照合しようとするプリセットプロセスです。ML マッチングは、一致したデータセットごとに一致 ID と信頼度を返します。

手動処理

オンデマンドで実行できるようにする、一致するワークフロージョブの処理頻度オプション。

このオプションはデフォルトで設定され、ルールベースのマッチングと機械学習ベースのマッチングの両方で使用できます。

多対多マッチング

M any-to-many マッチングは、類似データの複数のインスタンスを比較します。同じ一致キーが割り当てられた入力フィールドの値は、同じ入力フィールドにあるか異なる入力フィールドにあるかに関係なく、互いに照合されます。

例えば、「Phone」という同じ一致キーhome_phoneを持つ mobile_phoneや などの複数の電話番号入力フィールドがあるとします。 many-to-many マッチングを使用して、mobile_phone入力フィールドのデータとmobile_phone入力フィールドのデータおよびhome_phone入力フィールドのデータを比較します。

一致ルールは、 (または) オペレーションで同じ一致キーを持つ複数の入力フィールドのデータを評価し、 one-to-many 一致は複数の入力フィールドの値を比較します。つまり、2 つのレコード間で mobile_phoneまたは の組み合わせがhome_phone一致すると、「電話」一致キーは一致を返します。一致を見つけるための一致キー「Phone」の場合は、 `Record One mobile_phone = Record Two mobile_phone OR OR Record One mobile_phone = Record Two home_phone Record One home_phone = Record Two home_phone OR` ですRecord One home_phone = Record Two mobile_phone。

一致 ID (MatchID)

ルールベースのマッチングと ML マッチングの場合、これは によって生成 AWS Entity Resolution され、一致した各レコードセットに適用される ID です。これは、出力に含まれる一致するワークフローメタデータの一部です。

一致キー (MatchKey)

一致キーは、 AWS Entity Resolution どの入力フィールドを類似データと見なし、どの入力フィールドを異なるデータと見なすかを指示します。これにより、ルールベースのマッチングルール AWS Entity Resolution を自動的に設定し、さまざまな入力フィールドに保存されている同様のデータを比較できます。

入力フィールドやmobile_phone入力home_phoneフィールドなど、比較するデータに複数のタイプの電話番号情報がある場合は、両方の一致キー「Phone」を指定できます。その後、ルールベースのマッチングは、すべての入力フィールドの「または」ステートメントと「電話」一致キーを使用してデータを比較するように設定できます (「一致ワークフロー」セクションの「1 対 1 のマッチングと多対多マッチングの定義」を参照してください)。

ルールベースのマッチングで異なるタイプの電話番号情報を個別に考慮する場合は、「Mobile_Phone」や「Home_Phone」などのより具体的なマッチキーを作成できます。次に、マッチングワークフローを設定するときに、各電話一致キーをルールベースのマッチングで使用する方法を指定できます。

特定の入力フィールドに MatchKey が指定されていない場合、マッチングには使用できませんが、マッチングワークフロープロセスを通じて実行でき、必要に応じて出力できます。

一致キー名

一致キー に割り当てられた名前。

一致ルール (MatchRule)

ルールベースのマッチングの場合、これは、一致したレコードセットを生成するために適用されたルール番号です。これは、出力に含まれる一致するワークフローメタデータの一部です。

一致

さまざまな入力フィールド、テーブル、またはデータベースのデータを組み合わせて比較し、特定の一致基準 (例えば、一致するルールやモデル) を満たすことに基づいて、どちらが類似しているか、または「一致」しているかを判断するプロセス。

マッチングワークフロー

一致する入力データとマッチングの実行方法を指定するように設定したプロセス。

一致するワークフローの説明

入力することを選択できる、一致するワークフローのオプションの説明。説明は、複数のワークフローを作成する場合に、一致するワークフローを区別するのに役立ちます。

一致するワークフロー名

指定した一致するワークフローの名前。

> **Note**
>
> 一致するワークフロー名は一意である必要があります。同じ名前にすることはできません。そうしないと、エラーが返されます。

ワークフローメタデータの一致

一致するワークフロージョブ AWS Entity Resolution 中に によって生成および出力される情報。この情報は出力時に必要です。

正規化 (ApplyNormalization)

スキーマで定義されているように入力データを正規化するかどうかを選択します。正規化は、余分なスペースや特殊文字を削除し、小文字の形式に標準化することで、データを標準化します。

例えば、入力フィールドの入力タイプが でPHONE_NUMBER、入力テーブルの値が として フォーマットされている場合(123) 456-7890、 は値を に AWS Entity Resolution 正規化します1234567890。

以下のセクションでは、正規化ルールについて説明します。

トピック

- 名前

- Email(メール)
- 電話
- Address
- ハッシュ
- Source_ID

名前

- TRIM = 先頭と末尾の空白をトリミングする
- LOWERCASE = すべての英字を小文字にします
- CONVERT_ACCENT = アクセント文字を通常の文字にカバー
- REMOVE_ALL_NON_ALPHA = 英数字以外の文字をすべて削除します [a-zA-Z]

Email(メール)

- TRIM = 先頭と末尾の空白をトリミングする
- LOWERCASE = すべての英字を小文字にします
- CONVERT_ACCENT = アクセント文字を通常の文字にカバー
- REMOVE_ALL_NON_EMAIL_CHARS = すべての non-alpha-numeric 文字 [a-zA-Z0-9] と [.@-] を削除します

電話

- TRIM = 先頭と末尾の空白をトリミングする
- REMOVE_ALL_NON_NUMERIC = 数値以外の文字をすべて削除します [0 ~ 9]
- REMOVE_ALL_LEADING_ZEROES = 先頭のゼロをすべて削除します

Address

- TRIM = 先頭と末尾の空白をトリミングする
- LOWERCASE = すべての英字を小文字にします
- CONVERT_ACCENT = アクセント文字を通常の文字にカバー

- REMOVE_ALL_NON_ALPHA = 英数字以外の文字をすべて削除します [a-zA-Z]
- ADDRESS_RENAME_WORD_MAP を使用する RENAME_WORDS = Address 文字列の単語を ADDRESS_RENAME_WORD_MAP の単語に置き換えます
- ADDRESS_RENAME_DELIMITER_MAP を使用する RENAME_DELIMITERS = Address 文字列の区切り文字を ADDRESS_RENAME_DELIMITER_MAP の文字列に置き換えます
- ADDRESS_RENAME_DIRECTION_MAP を使用する RENAME_DIRECTIONS = Address 文字列の区切り文字を ADDRESS_RENAME_DIRECTION_MAP の文字列に置き換えます
- ADDRESS_RENAME_NUMBER_MAP を使用する RENAME_NUMBERS = Address 文字列の数値を ADDRESS_RENAME_NUMBER_MAP の文字列に置き換えます
- ADDRESS_RENAME_"_CHAR_MAP を使用する RENAME_"_CHARS = Address 文字列の特殊文字を ADDRESS_RENAME_"_CHAR_MAP の文字列に置き換えます

ADDRESS_RENAME_WORD_MAP

これらは、アドレス文字列を正規化するときに名前が変更される単語です。

```
"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

これらは、アドレス文字列を正規化するときに名前が変更される区切り文字です。

```
",": " ",
".": " ",
"[": " ",
"]": " ",
"/": " ",
"-": " ",
"#": " number "
```

ADDRESS_RENAME_DIRECTION_MAP

これらは、アドレス文字列を正規化するときに名前が変更される方向識別子です。

```
"east": "e",
"north": "n",
"south": "s",
"west": "w",
"northeast": "ne",
"northwest": "nw",
"southeast": "se",
"southwest": "sw"
```

ADDRESS_RENAME_NUMBER_MAP

これらは、アドレス文字列を正規化するときに名前が変更される数値文字列です。

```
"número": "number",
 "numero": "number",
 "no": "number",
 "núm": "number",
 "num": "number"
```

ADDRESS_RENAME_SPECIAL_CHAR_MAP

これらは、アドレス文字列を正規化するときに名前が変更される特殊文字文字列です。

```
"ß": "ss",
 "ä": "ae",
 "ö": "oe",
 "ü": "ue",
 "ø": "o",
 "æ": "ae"
```

ハッシュ

- TRIM = 先頭と末尾の空白をトリミングする

Source_ID

- TRIM = 先頭と末尾の空白をトリミングする

1 対 1 のマッチング

O ne-to-one マッチングは、類似データの単一インスタンスを比較します。同じ入力フィールド内の同じ一致キーと値を持つ入力フィールドは、互いに照合されます。

例えば、「Phone」という同じ一致キーhome_phoneを持つ mobile_phoneや などの複数の電話番号入力フィールドがあるとします。 one-to-one マッチングを使用して、mobile_phone入力フィールドのデータとmobile_phone入力フィールドのデータを比較し、home_phone入力フィールドのデータとhome_phone入力フィールドのデータを比較します。mobile_phone 入力フィールドのデータは、home_phone入力フィールドのデータと比較されません。

一致ルールは、 (または) オペレーションで同じ一致キーを持つ複数の入力フィールドのデータを評価し、 one-to-many 一致は 1 つの入力フィールド内の値を比較します。つまり、2 つのレコード間で mobile_phoneまたは home_phoneが一致すると、「電話」一致キーは一致を返します。一致を見つけるための一致キー「電話」の場合は、 Record One mobile_phone = Record Two mobile_phone または ですRecord One home_phone = Record Two home_phone。

一致ルールは、 (および) オペレーションで異なる一致キーを持つ入力フィールドのデータを評価します。ルールベースのマッチングで異なるタイプの電話番号情報を個別に考慮する場合は、

「mobile_phone」や「home_phone」などのより具体的なマッチキーを作成できます。ルールで両方の一致キーを使用して一致を検索する場合は、 `Record One mobile_phone = Record Two mobile_phone` AND `Record One home_phone = Record Two home_phone`。

出力

オブジェクトのリスト。各OutputAttributeオブジェクトには、名前 とハッシュされた のフィールドがあります。これらの各オブジェクトは、 AWS Glue 出力テーブルに含める列と、列内の値をハッシュするかどうかを表します。

OutputS3Path

AWS Entity Resolution が出力テーブルを書き込む S3 送信先。

OutputSourceConfig

オブジェクトのリスト。各 OutputSource オブジェクトには OutputS3Path、、ApplyNormalizationおよび Output フィールドがあります。

プロバイダーのサービスベースのマッチング

プロバイダーのサービスベースのマッチングは、レコードを優先データサービスプロバイダーやライセンスデータセットと照合、リンク、強化するプロセスです。このマッチング手法を使用するには、プロバイダーサービス AWS Data Exchange で を通じてサブスクリプションが必要です。

AWS Entity Resolution は現在、以下のデータサービスプロバイダーと統合されています。

- LiveRamp
- TransUnion
- UID 2.0

ルールベースのマッチング

ルールベースのマッチングは、完全一致を見つけるように設計されたプロセスです。ルールベースのマッチングは、入力したデータに基づいて によって提案され AWS Entity Resolution、ユーザーが完全に設定できるウォーターフォールマッチングルールの階層セットです。ルール条件内で提供されるすべての一致キーは、比較データで一致を宣言し、関連するメタデータを出力するために正確に一致

する必要があります。ルールベースの一致は、一致したデータセットごとに一致 ID とルール番号を返します。

エンティティを一意に識別できるルールを定義することをお勧めします。ルールを順序付けして、より正確な一致を最初に見つけます。

例えば、ルール 1 とルール 2 の 2 つのルールがあるとします。

これらのルールには、次の一致キーがあります。

- ルール 1 にはフルネームと住所が含まれます
- ルール 2 にはフルネーム、住所、電話番号が含まれます

ルール 1 が最初に実行されるため、ルール 1 によってすべて見つかったはずであるため、ルール 2 では一致は見つかりません。

電話によって区別される一致を検索するには、次のようにルールの順序を変更します。

- ルール 2 にはフルネーム、住所、電話番号が含まれます
- ルール 1 にはフルネームと住所が含まれます

Schema

一連のデータの編成と接続方法を定義する構造またはレイアウトに使用される用語。

スキーマの説明

入力できるスキーマのオプションの説明。説明は、複数のスキーマを作成する場合にスキーママッピングを区別するのに役立ちます。

スキーマ名

スキーマの名前。

> **Note**
>
> スキーマ名は一意である必要があります。同じ名前にすることはできません。そうしないと、エラーが返されます。

スキーママッピング

のスキーママッピング AWS Entity Resolution は、マッチングのためにデータを解釈 AWS Entity Resolution する方法を指示するプロセスです。一致するワークフローに AWS Entity Resolution 読み込む入力データテーブルのスキーマを定義します。

スキーママッピング ARN

スキーママッピング 用に生成された Amazon リソースネーム (ARN)。

一意の ID

指定した一意の識別子で、 が AWS Entity Resolution 読み取る入力データの各行に割り当てる必要があります。

Example

たとえば、**`Primary_key`**、**`Row_ID`**、または **`Record_ID`** などです。

一意の ID 列は必須です。

一意の ID は、単一のテーブル内の一意の識別子である必要があります。

異なるテーブル間で、一意の ID に重複する値を含めることができます。

一致するワークフローが実行されると、一意の ID が の場合、レコードは拒否されます。

- が指定されていない
- 同じテーブル内で一意ではない
- は、ソース間で属性名の点で重複しています。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。