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 (、 などSKUUPC) 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 AWS Entity Resolution して、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、インタラクティブな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 も提供しています。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、データ入力の照合 AWS Entity Resolution 方法と統合データ出力の書き込み場所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、さまざまなデータ入力を比較し、エンティティ解決や ML エクスペリエンスなしで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。これにより、すべてのデータが再処理され、新しい一致や既存の一致に対する更新が行われます。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 データの変更との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 オペレーションで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。さまざまなソースと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 オペレーションを使用して AWS Entity Resolution 、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一致 ID を確認します。エンティティ一致 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一致 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およびハッシュ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 の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 AWS サービス 、 に関連しています 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 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、「を使用してAWSエンティティ解決リソースを作成する 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。

- の AWS Entity Resolution コンソールから直接https://console.aws.amazon.com/entityresolution/。
- を介してプログラムで AWS Entity Resolution API。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 Runtime で を呼び出す AWS Entity Resolution API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ライブラリを含めます AWS SDK。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、 にサインアップ AWS して管理者ユーザーを作成してロールを作成します。

にサインアップする AWS

が既にある場合は AWS アカウント、このステップをスキップします。

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/サインアップ 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 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、「 ユーザーガイド」の「 のセキュリティのベストプラクティス IAMIAM」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
で IAM (非推奨)	長期認証情報を使用して AWSにアクセスする。	「 ユーザーガイドIAM」の「最初の管理者ユーザーとユーザーグループの作成IAM」の手順に従います。	「 ユーザーガイド」の IAM「ユーザーのアクセスキーを管理する」でプログラムによるアクセスを設定します。 IAM

コンソールユーザーの IAMロールの作成

AWS Entity Resolution コンソールを使用している場合は、次の手順を実行します。

IAM ロールを作成するには

1. 管理者アカウントで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以下の マネージドポリシー 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. [ロールの作成] を選択します。

のワークフロージョブロールの作成 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https://console.aws.amazon.com/iam/を使用して で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. [Next (次へ)] を選択します。
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 を置き換える *{{user input placeholder}}* 自分の情報を入力します。

aws-region	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。
input-buckets	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。
output-buckets	AWS Entity Resolution が出力データを生成する Amazon S3 バケット。
input-databases	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 を置き換える *{{user input placeholder}}* 自分の情報を入力します。

aws-region	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 を置き換える *{{user input placeholder}}* 自分の情報を入力します。

aws-region	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 を置き換える *{{user input placeholder}}* 自分の情報を入力します。

aws-region	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. [ロールの作成] 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。

入力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、他のサードパーティー 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。Amazon S3 にデータをアップロードした後、 AWS Glue クローラーを使用して 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。

以下のセクションでは、ファーストパーティデータとサードパーティーデータを準備する方法について説明します。

トピック

- ファーストパーティー入力データの準備
- サードパーティーの入力データの準備

ファーストパーティー入力データの準備

次の手順では、ルールベースのマッチングワークフロー 、機械学習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 で使用するファーストパーティデータを準備します。 機械学習ベースのマッチングワークフローの作成

ステップ 1: 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

ファーストパーティー入力データをサポートされているデータ形式で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 をサポートします。

- カンマ区切り値 (CSV)
- Parquet

ステップ 2: 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、 で Amazon S3 コンソールを開きますhttps://console.aws.amazon.com/s3/。
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 3: 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、 AWS Glue テーブルとして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ーの操作」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、 で AWS Glue コンソールを開きますhttps://console.aws.amazon.com/glue/。
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ロールの選択」を選択し、「次へ」を選択します。

   必要に応じて、 IAMロールを作成する を選択するか、管理者にIAMロールを作成させることもできます。
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. クローラーの出力を設定する で、 AWS Glue データベースを入力し、次へ を選択します。
9. すべての詳細を確認し、「終了」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。

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

これで、スキーママッピングを作成する準備ができました。詳細については、「スキーママッピングの作成」を参照してください。

サードパーティーの入力データの準備

サードパーティーのデータサービスは、既知の識別子と照合できる識別子を提供します。

AWS Entity Resolution は現在、以下のサードパーティーのデータプロバイダーサービスをサポートしています。

データプロバイダーサービス

会社名	使用可能 AWS リージョン	識別子
LiveRamp	米国東部 (バージニア北部) (us-east-1)、米国東部 (オハイオ) (us-east-2)、米国西部 (オレゴン) (us-west-2)	ランプ ID
TransUnion	米国東部 (バージニア北部) (us-east-1)、米国東部 (オハイオ) (us-east-2)、米国西部 (オレゴン) (us-west-2)	TransUnion 個人と世帯 IDs
統合 ID 2.0	米国東部 (バージニア北部) (us-east-1)、米国東部 (オハイオ) (us-east-2)、米国西部 (オレゴン) (us-west-2)	raw UID 2

次の手順では、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 またはプロバイダーのサービスベースの ID マッピングワークフロー を使用するようにサードパーティーデータを準備する方法について説明します。

トピック

- ステップ 1: でプロバイダーサービスをサブスクライブする AWS Data Exchange
- ステップ 2: サードパーティーのデータテーブルを準備する
- ステップ 3: 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 4: 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 5: テーブルを作成する AWS Glue

ステップ 1: でプロバイダーサービスをサブスクライブする AWS Data Exchange

を通じてプロバイダーサービスにサブスクリプションがある場合は AWS Data Exchange、次のいずれかのプロバイダーサービスでマッチングワークフローを実行して、既知の識別子を優先プロバイダーとマッチングできます。データは、優先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。

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

1. でプロバイダーのリストを表示します AWS Data Exchange。以下のプロバイダーリストが利用可能です。

   - 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
2. オファータイプに応じて、次のいずれかの手順を実行します。

   - 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を使用する – プロバイダーに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) offers」の手順に従って、 でのBYOSオファーを承諾します AWS Data Exchange。
3. 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。

を含むプロバイダー製品にアクセスする方法の詳細についてはAPIs、「 AWS Data Exchange ユーザーガイド」の「 APIの製品へのアクセス」を参照してください。

ステップ 2: サードパーティーのデータテーブルを準備する

各サードパーティーサービスには、マッチングワークフローを確実に成功させるために、さまざまな推奨事項とガイドラインがあります。

サードパーティーのデータテーブルを準備するには、次の表を参照してください。

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	あり	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ています。 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「 によるアイデンティティ解決の実行ADX」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「Perform Transcoding ThroughADX」を参照してください。
TransUnion	あり	以下を確認してください。 • TransUnion Data Enrichment には一意の ID が存在します。

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
		- 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。

> **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、クライアント名前空間に固有です。

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
		• **Last Name** は小文字または大文字、ミドルネームは除外できます。

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	あり	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生成に 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、出力にこのレコードの重複が不要な場合は、それぞれに個別のワークフローを作成し、スキーママッピングを個別に作成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、いつでも同じ 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、1 年に約 1 回ローテーションされるソルトバケットからソルトを追加することで作成され、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します。 AWS Entity Resolution 現在、 はローテーションするソルトバケットと raw を追跡しないためUID2s、raw を UID2s毎日再生成することをお勧めします。詳細については、2.0 ドキュメントの「増分更新のために更新UID2sする頻度UID」を参照してください。

ステップ 3: 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

サードパーティーの入力データを既にサポートされているデータ形式で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 4: 入力データテーブルを Amazon S3 にアップロードする

Amazon S3 にサードパーティーの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、 で Amazon S3 コンソールを開きますhttps://console.aws.amazon.com/s3/。
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 5: テーブルを作成する AWS Glue

Amazon S3 の入力データは、 でカタログ化 AWS Glue され、 AWS Glue テーブルとして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「コンソールでのクローラ AWS Glue 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、 で AWS Glue コンソールを開きますhttps://console.aws.amazon.com/glue/。
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ロールの選択」を選択し、「次へ」を選択します。

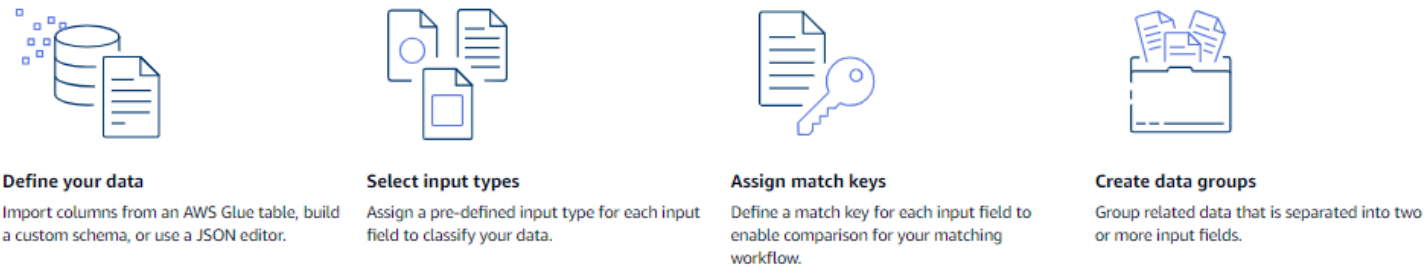
   必要に応じて、ロールの作成IAMを選択するか、管理者にIAMロールを作成させることもできます。
7. [このクローラのスケジュールを設定する] で、[頻度] をデフォルト ([オンデマンドで実行]) のままにして、[次へ] を選択します。
8. クローラーの出力を設定する で、 AWS Glue データベースを入力し、次へ を選択します。
9. 詳細を確認し、[完了] を選択します。
10. [クローラ] ページで、S3 バケットの横にあるチェックボックスをオンにし、[クローラの実行] を選択します。
11. クローラーの実行が完了したら、 AWS Glue ナビゲーションバーでデータベース 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

スキーママッピングを使用して入力データを定義する

スキーママッピングは、解決する入力データを定義します。また、列の属性タイプ (入力タイプ) や一致する列など、入力データに関するメタデータも提供します。

スキーママッピングを作成するときは、まず入力フィールドと入力タイプを定義し、次に一致キーとグループ関連データを定義します。次の図は、スキーママッピングを作成する方法をまとめたものです。



スキーママッピングを作成する前に、まずデータテーブルをセットアップ AWS Entity Resolution して準備する必要があります。詳細については、「セットアップ AWS Entity Resolution」および「入力データテーブルを準備する」を参照してください。

スキーママッピングを作成したら、次のいずれかを実行できます。

- 一致するワークフローを作成して、異なるデータ入力間の一致を検索します。
- ID マッピングワークフローで使用できる ID 名前空間ソースを作成し、ソースからターゲットにデータを変換します。
- スキーママッピングをソースとして使用して、同じ 内に ID マッピングワークフロー AWS アカウントを作成します。

トピック

- スキーママッピングの作成
- スキーママッピングのクローン作成
- スキーママッピングの編集
- スキーママッピングの削除

スキーママッピングの作成

この手順では、AWS Entity Resolution コンソール を使用してスキーママッピングを作成するプロセスについて説明します。

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。

- 「Import from AWS Glue オプション」を使用して既存の入力データをインポートする – この作成方法を使用して、ガイド付きフローを使用して AWS Glue テーブルから事前入力された列で始まる入力フィールドを定義します。
- カスタムスキーマの構築オプションを使用して入力データを手動で定義する – 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。
- JSON エディタの使用オプションを使用して手動で を作成する – JSONエディタを使用して、既存の入力データを手動で作成、サンプルの使用、またはインポートします。

> **Note**
>
> 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。

Import from AWS Glue

から既存の入力データをインポートしてスキーママッピングを作成するには AWS Glue

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 に移動しますhttps://console.aws.amazon.com/glue/。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。ルールベースのマッチングワークフローでこのスキーママッピングを使用している場合、一意の ID は 38 文字を超えることはできません。

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. [Next (次へ)] を選択します。

5. ステップ 2: 入力フィールド をマッピングするには、マッチングに使用する入力フィールドとオプションのパススルーに使用する入力フィールドを定義します。

a. を照合する入力フィールドについては、入力フィールド ごとに、入力タイプ 、一致キー 、ハッシュステータス 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。Hashing ステータスは、その入力フィールドの列値がハッシュ化されているかクリアテキストであるかを示します。

> **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。
> - 住所フィールドは、複数のフィールド (**address1**、 など**address2**) または 1 つのフィールドで指定します。
>
>   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。

> **Note**
>
> 機械学習ベースのマッチングワークフローで使用するスキーママッピングを作成する場合、データセットには、、**phonenumber**、、**fullnameaddresses**、または の少なくとも **emailaddress**1 つの属性が含まれている必要がありますbirthdate。
> これらの属性の入力タイプをカスタム文字列 として指定しないでください。

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と対応するハッシュステータス を追加します。

   Hashing ステータスは、その入力フィールドの列値がハッシュ化されているかクリアテキストであるかを示します。

c. [Next (次へ)] を選択します。

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. [Next (次へ)] を選択します。

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**
>
> ワークフローに関連付けた後で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。

Build custom schema

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、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、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。ルールベースのマッチングワークフローでこのスキーママッピングを使用している場合、一意の ID は 38 文字を超えることはできません。

   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. [Next (次へ)] を選択します。

5. ステップ 2: 入力フィールド をマッピングするには、マッチングに使用する入力フィールドとオプションのパススルーに使用する入力フィールドを定義します。

   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 、および対応する入力タイプ 、一致キー 、ハッシュステータス 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。Hashing ステータスは、その入力フィールドの列値がハッシュ化されているかクリアテキストであるかを示します。

> **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。

> **Note**
>
> 機械学習ベースのマッチングワークフローで使用するスキーママッピングを作成する場合、データセットには、、**phonenumber**、、**fullnameaddresses**、または の少なくとも **emailaddress**1 つの属性が含まれている必要がありますbirthdate。
> これらの属性の入力タイプをカスタム文字列 として指定しないでください。

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と対応するハッシュステータス を追加します。

c. [Next (次へ)] を選択します。

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**、「」というグループ名と**Full name**「」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. [Next (次へ)] を選択します。

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。

JSON Editor

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工ディタ 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. [Next (次へ)] を選択します。

5. ステップ 2: マッピング を指定します。

   a. JSON エディタでスキーマの構築を開始するか、目標に基づいて次のいずれかのオプションを選択します。

目標	推奨オプション
スキーママッピングの構築を開始する	サンプルを挿入JSON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. [Next (次へ)] を選択します。

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。

スキーママッピングのクローン作成

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の編集

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。ワークフローにスキーママッピングを関連付けた後は、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 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の削除

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 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。

ID 名前空間を使用して入力データを定義する

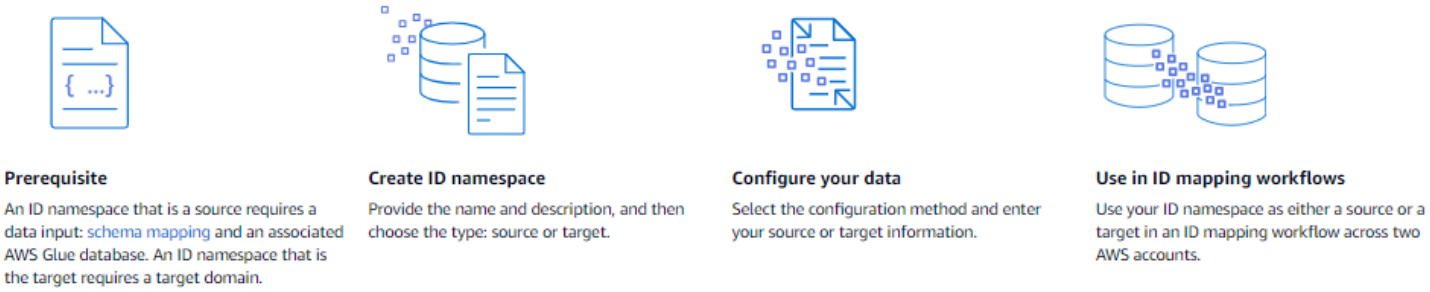
ID 名前空間は、入力データテーブルを囲むラッパーです。ID 名前空間を使用して、入力データとマッチング手法、およびそれらを ID マッピングワークフロー で使用する方法を説明するメタデータを提供します。

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ます。

AWS アカウント ID マッピングワークフローで 2 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。

次の図は、ID マッピングワークフローで使用する ID 名前空間を作成する方法をまとめたものです。



以下のセクションでは、ID 名前空間ソースと ID 名前空間ターゲットを作成する方法について説明します。

トピック

- ID 名前空間ソース
- ID 名前空間ターゲット
- ID 名前空間の編集
- ID 名前空間の削除
- ID 名前空間のリソースポリシーの追加または更新

ID 名前空間ソース

ID 名前空間ソースは、ID マッピングワークフロー 内のデータのソースです。

ID 名前空間ソースを作成する前に、ユースケースに応じて、まずスキーママッピングまたは一致するワークフローを作成する必要があります。詳細については、「スキーママッピングの作成」および「一致するワークフローを使用して入力データを照合する」を参照してください。

ID 名前空間ソースを作成したら、ID マッピングワークフローで ID 名前空間ターゲットと一緒に使用できます。詳細については、「ID マッピングワークフローを使用して入力データをマッピングする」を参照してください。

AWS Entity Resolution コンソールで ID 名前空間ソースを作成するには、ルールベースのメソッドまたはプロバイダーサービスメソッド の 2 つの方法があります。

トピック

- ID 名前空間ソースの作成 (ルールベース)
- ID 名前空間ソースの作成 (プロバイダーサービス)

ID 名前空間ソースの作成 (ルールベース)

このトピックでは、ルールベースの メソッドを使用して ID 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。この方法では、一致するルールを使用して、ID マッピングワークフローでファーストパーティデータをソースからターゲットに変換します。

> **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 (ルールベース)

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、ソース を選択します。

5. ID 名前空間メソッド で、ルールベースの を選択します。

6. データ入力 で、使用する入力タイプを選択し、推奨アクションを実行します。

入力タイプ	推奨されるアクション
既存のスキーママッピング	1. スキーママッピング を選択します。 2. 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。
既存のマッチングワークフロー	1. マッチングワークフロー を選択します。 2. ID 名前空間に関連付けられているアカウントを選択します。自分 AWS アカウントまたは別の AWS アカウントのいずれかです。 3. アカウントのタイプに応じて、一致するワークフロー名を選択するか、一致するワークフローを入力しますARN。

7. ルールパラメータ で、次の操作を行います。

   a. 目標に基づいて次のいずれかのオプションを選択して、ルールコントロールを指定します。

目標	推奨オプション
ソースとターゲットの両方からのルールを許可する	設定なし

目標	推奨オプション
ソース、ターゲット、またはその両方が ID マッピングワークフローでルールを提供できるかどうかを選択します。	制限されたルール

ルールコントロールは、ID マッピングワークフローで使用するソースとターゲットの間で互換性がある必要があります。例えば、ソース ID 名前空間がルールをターゲットに制限し、ターゲット ID 名前空間がルールをソースに制限する場合、エラーが発生します。

b. データ入力タイプに基づいて次のいずれかのオプションを選択して、一致ルールを指定します。

データ入力タイプ	推奨されるアクション
スキーママッピング	別のルールを追加 を選択して、一致するルールを追加します。 最大 25 個の一致ルールを適用して、一致条件を定義できます。
マッチングワークフロー	一致するワークフローからルールを使用するか、新しいルールを指定して一致するルールを定義します。

8. 比較および一致するパラメータ については、以下を実行します。

a. 目標に基づいて次のいずれかのオプションを選択して、比較タイプを指定します。

目標	推奨オプション
ID マッピングワークフローを作成するときに、任意の比較タイプの使用を許可します。	設定なし
データが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	複数の入力フィールド

目標	推奨オプション
、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します。	
複数の入力フィールドに保存されている類似データを一致させない場合、1 つの入力フィールド内の比較を制限します。	単一入力フィールド

b. 目標に基づいて次のいずれかのオプションを選択して、レコードマッチングタイプを指定します。

目標	推奨オプション
ID マッピングワークフローを作成するときに、任意の比較タイプの使用を許可します。	設定なし
ID マッピングワークフローを作成するときに、ターゲット内の一致したレコードごとにソースに一致レコードを 1 つだけ保存するようにレコード一致タイプを制限します。	レコードマッチングの制限 また、 1 つのソースから 1 つのターゲットへ
ID マッピングワークフローを作成するときに、レコード一致タイプを制限して、ターゲット内の一致した各レコードのソースにすべての一致レコードを保存します。	レコードマッチングの制限 また、 1 つのターゲットへの多くのソース

> **Note**
>
> ソース ID 名前空間とターゲット ID 名前空間に互換性のある制限を指定する必要があります。例えば、ソース ID 名前空間がルールをターゲットに制限し、ターゲット ID 名前空間がルールをソースに制限する場合、エラーが発生します。

9. 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て、サービスアクセス許可を指定します。
10. (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。
11. ID 名前空間の作成 を選択します。

ID 名前空間ソースが作成されます。これで、ID 名前空間ターゲット を作成する準備ができました。

ID 名前空間ソースの作成 (プロバイダーサービス)

このトピックでは、プロバイダーサービスメソッドを使用して ID 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。このメソッドは、ID マッピングワークフロー中に LiveRamp LiveRamp 、サードパーティーでエンコードされたデータをソースからターゲットに変換する というプロバイダーサービスを使用します。

> **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 (プロバイダーサービス)

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 で、プロバイダーサービス を選択します。

> **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ステップ 1: 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、 オプションを選択し、推奨アクションを実行します。

オプション	推奨されるアクション
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キーオプションで暗号化されます」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。

オプション	推奨されるアクション
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 名前空間ソースが作成されます。これで、ID 名前空間ターゲット を作成する準備ができました。

ID 名前空間ターゲット

ID 名前空間ターゲットは、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前に、ユースケースに応じて、まず一致するワークフローを作成するか、プロバイダーサービス (LiveRamp) へのサブスクリプションが必要です。詳細については、

「一致するワークフローを使用して入力データを照合する」および「ステップ 1: 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 名前空間ターゲットを作成したら、ID マッピングワークフローで ID 名前空間ソースと一緒に使用できます。詳細については、「ID マッピングワークフローを使用して入力データをマッピングする」を参照してください。

AWS Entity Resolution コンソールで ID 名前空間ターゲットを作成するには、ルールベースのメソッド またはプロバイダーサービスメソッド の 2 つの方法があります。

トピック

- ID 名前空間ターゲットの作成 (ルールベースのメソッド)
- ID 名前空間ターゲットの作成 (プロバイダーサービスメソッド)

ID 名前空間ターゲットの作成 (ルールベースのメソッド)

このトピックでは、ルールベースの メソッドを使用して ID 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。このメソッドは、ID マッピングワークフロー中に、一致するルールを使用してファーストパーティデータをソースからターゲットに変換します。

ID 名前空間ターゲットを作成するには (ルールベース)

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、ターゲット を選択します。
5. ID 名前空間メソッド で、ルールベースの を選択します。
6. データ入力 の場合、ワークフロー の一致で、次の操作を行います。
    a. ID 名前空間に関連付けられているアカウントを選択します。自分 AWS アカウントまたは別の AWS アカウントのいずれかです。

b. アカウントのタイプに応じて、一致するワークフロー名を選択するか、一致するワークフローを入力しますARN。

7. ルールパラメータ で、次の操作を行います。

a. 目標に基づいて次のいずれかのオプションを選択して、ルールコントロールを指定します。

目標	推奨オプション
ソースとターゲットの両方からのルールを許可する	設定なし
ソース、ターゲット、またはその両方が ID マッピングワークフローでルールを提供できるかどうかを選択します。	制限されたルール

ルールコントロールは、ID マッピングワークフローで使用するソースとターゲットの間で互換性がある必要があります。例えば、ソース ID 名前空間がルールをターゲットに制限し、ターゲット ID 名前空間がルールをソースに制限する場合、エラーが発生します。

b. 一致ルール の場合、 は一致するワークフローからルール AWS Entity Resolution を自動的に追加します。

8. 比較および一致するパラメータ については、以下を実行します。

a. 目標に基づいて次のいずれかのオプションを選択して、比較タイプを指定します。

目標	推奨オプション
ID マッピングワークフローを作成するときに、任意の比較タイプの使用を許可します。	設定なし
データが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、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します。	複数の入力フィールド

目標	推奨オプション
複数の入力フィールドに保存されている類似データを一致させない場合、単一の入力フィールド内で比較を制限します。	単一入力フィールド

b. 目標に基づいて次のいずれかのオプションを選択して、レコードマッチングタイプを指定します。

目標	推奨オプション
ID マッピングワークフローを作成するときに、任意の比較タイプの使用を許可します。	設定なし
ID マッピングワークフローを作成するときに、ターゲット内の一致したレコードごとにソースに一致レコードを 1 つだけ保存するようにレコード一致タイプを制限します。	レコードマッチングの制限 また、 1 つのソースから 1 つのターゲットへ
ID マッピングワークフローを作成するときに、レコード一致タイプを制限して、ターゲット内の一致した各レコードについて、一致するすべてのレコードをソースに保存します。	レコードマッチングの制限 また、 1 つのターゲットへの多くのソース

> **Note**
>
> ソース ID 名前空間とターゲット ID 名前空間に互換性のある制限を指定する必要があります。例えば、ソース ID 名前空間がルールをターゲットに制限し、ターゲット ID 名前空間がルールをソースに制限する場合、エラーが発生します。

9. 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て、サービスアクセス許可を指定します。
10. (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。

11. ID 名前空間の作成 を選択します。

ID 名前空間ターゲットが作成されます。ID マッピングワークフローに必要な ID 名前空間 (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 を作成する準備が整います。

ID 名前空間ターゲットの作成 (プロバイダーサービスメソッド)

このトピックでは、プロバイダーサービスメソッドを使用して ID 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。この方法では、ID マッピングワークフロー中に LiveRamp LiveRamp 、サードパーティーでエンコードされたデータをソースからターゲットに変換する というプロバイダーサービスを使用します。

ID 名前空間ターゲットを作成するには (プロバイダーサービス)

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 で、プロバイダーサービス を選択します。

> **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ステップ 1: 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、新しいタグの追加 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。

ID 名前空間ターゲットが作成されます。ID マッピングワークフローに必要な ID 名前空間 (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 を作成する準備が整います。

ID 名前空間の編集

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 名前空間の削除

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、まず関連するすべての 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。

ID 名前空間の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 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. [Save changes] (変更の保存) をクリックします。

一致するワークフローを使用して入力データを照合する

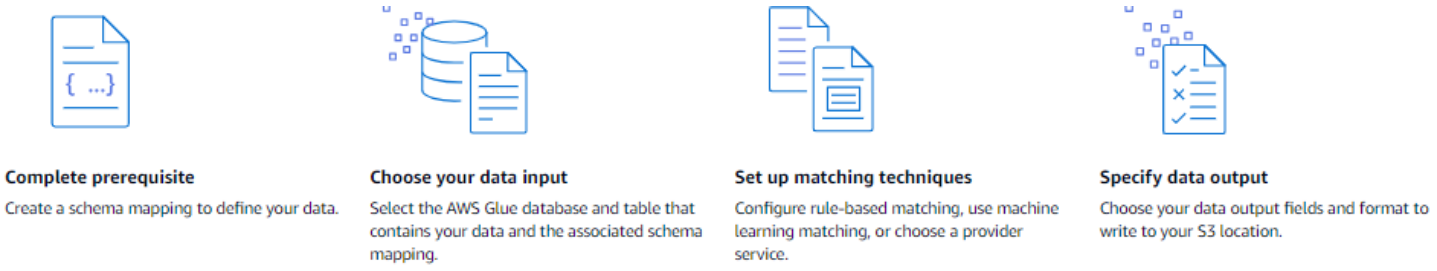
マッチングワークフローは、さまざまな入力ソースのデータを組み合わせて比較し、さまざまなマッチング手法に基づいて一致するものを決定するデータ処理ジョブです。データ出力テーブルを生成します。

一致するワークフローを作成するときは、まずデータ入力、正規化ステップを指定し、次に目的のマッチング手法とデータ出力を選択します。 は、指定した場所からデータを AWS Entity Resolution 読み取り、データ内の 2 つ以上のレコード間の一致を見つけます。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。 AWS Entity Resolution その後、 は選択した場所にデータ出力ファイルを書き込みます。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。

一致する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、複数のファイルを含む`success`フォルダに書き込まれ、各ファイルには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マッチングワークフローのトラブルシューティング。

次の図は、一致するワークフローを作成する方法をまとめたものです。



一致するワークフローを作成する前に、まずスキーママッピングを作成する必要があります。詳細については、「スキーママッピングの作成」を参照してください。

マッチング手法に基づいてマッチングワークフローを作成するには、ルールベースの 、機械学習ベースの 、またはプロバイダーサービスベースの の 3 つの方法があります。 プロバイダーのサービスベースのマッチングワークフローの作成

一致するワークフローを作成して実行したら、以下を実行できます。

- 指定した S3 ロケーションで結果を表示します。一致するワークフローは、データのインデックス作成IDs後に を生成します。
- ビジネスニーズを満たすために、ルールベースのマッチングまたは機械学習 (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ます。

  Example

  例えば、プロバイダーのサブスクリプションコストを節約するには、まず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見つけることができます。その後、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の作成
- 機械学習ベースのマッチングワークフローの作成
- 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の作成
- 一致するワークフローの編集
- 一致するワークフローの削除
- ルールベースの一致ワークフローの一致 ID の検索
- 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のレコードの削除
- マッチングワークフローのトラブルシューティング

ルールベースのマッチングワークフローの作成

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 が提案す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。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、以下が割り当てられます。

- 一致したデータセット内のレコードへの一致 ID
- 一致を生成した一致ルール。

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、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 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. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。

オプション	推奨されるアクション
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、「このデータはKMSキーオプションで暗号化され」を選択し、データ入力の復号に

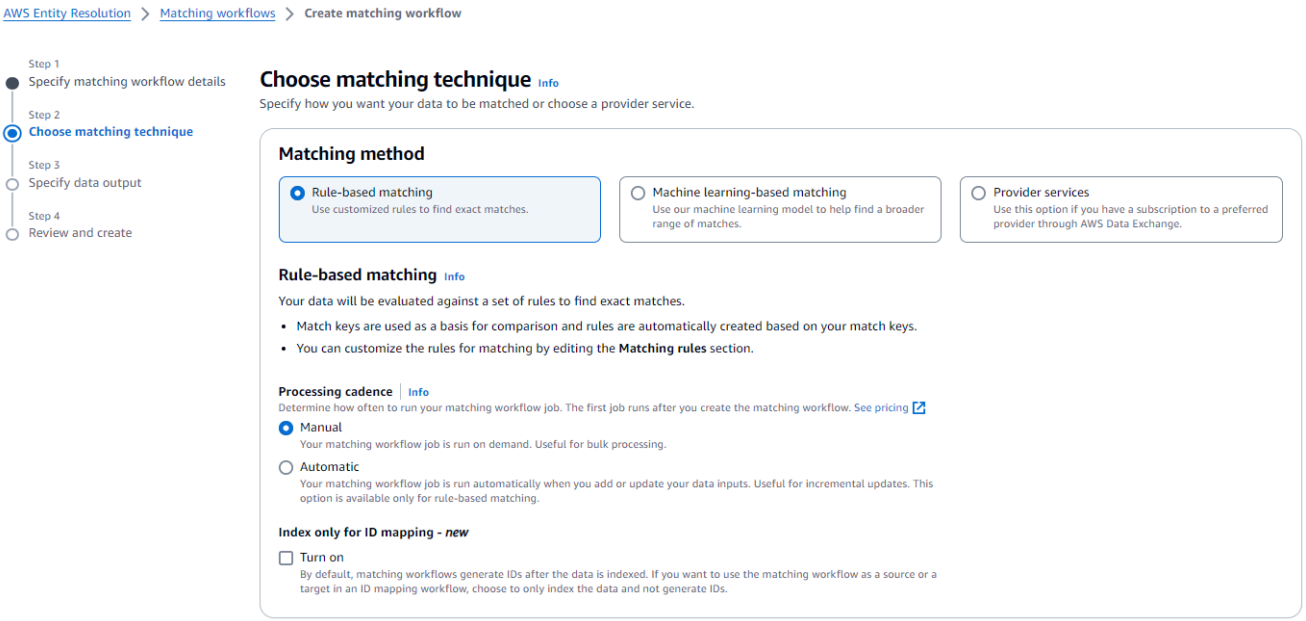
オプション	推奨されるアクション
	使用される AWS KMS キーを入力できます。
既存のサービスロールを使用	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. 外部リンクで表示IAMを選択して、サービスロールを表示します。 デフォルトでは、 AWS Entity Resolution 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. [Next (次へ)] を選択します。

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。



ルールベースおよび機械学習オプションで一致するテクニック画面を選択します。

b. 処理ケイデンス では、目標に基づいて次のいずれかのオプションを選択します。

目標	推奨オプション
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

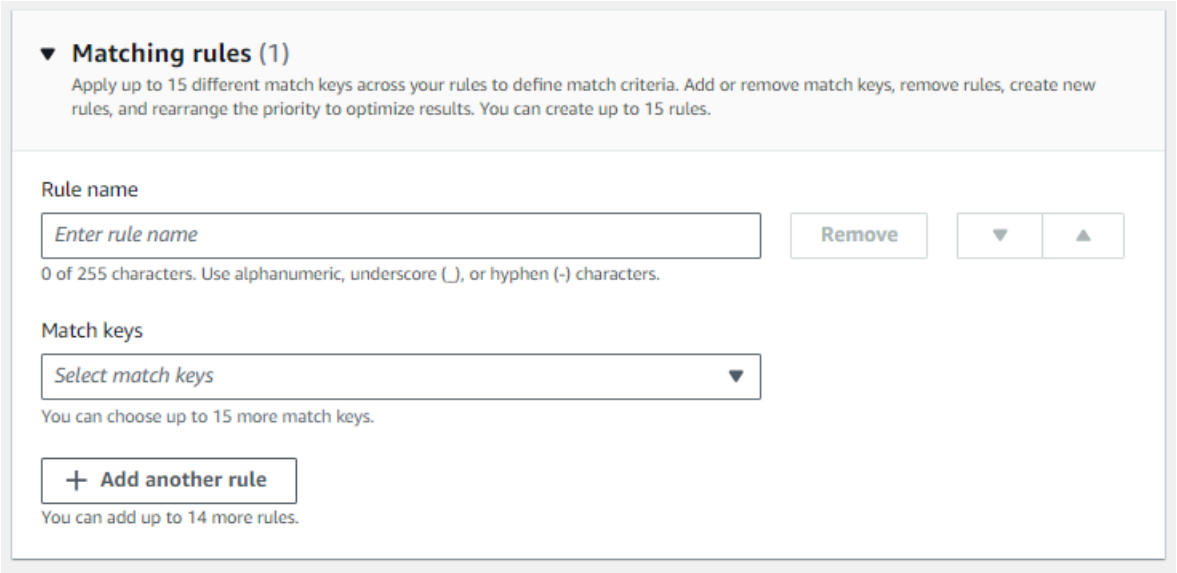
> **Note**
>
> 自動 を選択した場合は、S3 バケットに対して Amazon EventBridge 通知が有効になっていることを確認します。S3 コンソールを使用して Amazon EventBridge を有効にする手順については、「Amazon S3 EventBridgeユーザーガイド」のAmazon S3」を参照してください。

c. （オプション) ID マッピング のインデックスのみの場合、データのインデックスのみを有効にし、 を生成しないように選択できますIDs。

デフォルトでは、一致するワークフローは、データのインデックス作成IDs後に を生成します。

d. 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。

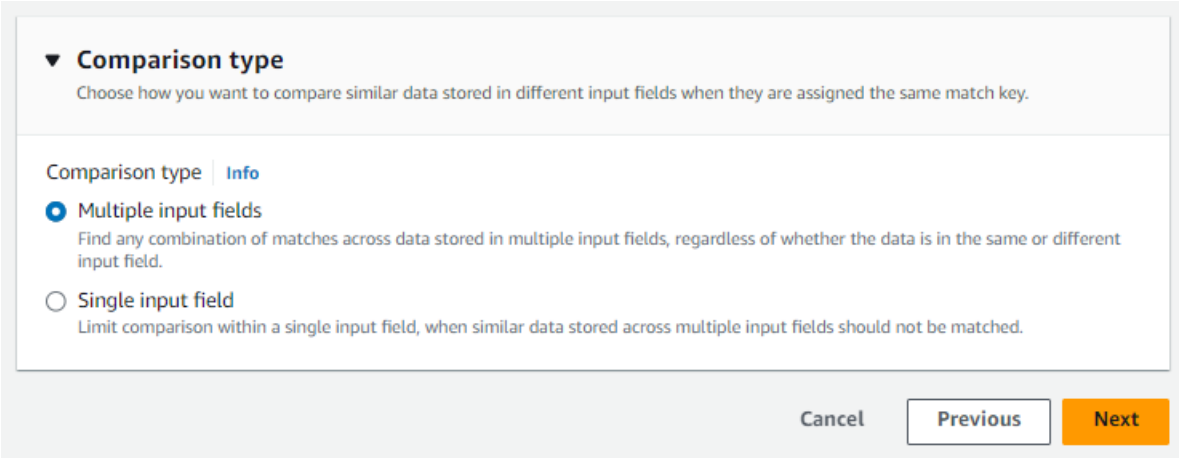
最大 15 個のルールを作成し、ルール全体に最大 15 個の異なる一致キーを適用して、一致基準を定義できます。



ルール名を入力し、一致キーを選択するためのフィールドを含む一致ルールインターフェイス。

e. 比較タイプ では、目標に基づいて次のいずれかのオプションを選択します。

目標	推奨オプション
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
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



比較タイプオプション: 複数のフィールドに保存されているデータ間で一致を検索する複数の入力フィールド、または 1 つのフィールド内で比較を制限する単一入力フィールド。

f. [Next (次へ)] を選択します。

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 を入力しますARN。

c. システム生成の出力 を表示します。

d. データ出力 では、含める、非表示にする、またはマスクするフィールドを決定し、目標に基づいて推奨アクションを実行します。

目標	推奨されるアクション
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. [Next (次へ)] を選択します。

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。
   - IDs 生成された一意の一致。
   - 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。

10. (手動処理タイプのみ) 手動処理タイプでルールベースのマッチングワークフローを作成した場合は、一致するワークフローの詳細ページでワークフローを実行するを選択して、一致するワークフローをいつでも実行できます。

機械学習ベースのマッチングワークフローの作成

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で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。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、以下が割り当てられます。

- 一致したデータセット内のレコードへの一致 ID
- 一致信頼度の割合。

ML ベースのマッチングワークフローの出力をデータサービスプロバイダーマッチングの入力として使用することも、その逆を使用して特定の目標を達成することもできます。例えば、ML ベースのマッチングを実行して、最初に独自のレコードでデータソース間の一致を検索できます。サブセットが一致しなかった場合は、プロバイダーのサービスベースのマッチングを実行して、追加のマッチングを見つけることができます。

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、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 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. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。

オプション	推奨されるアクション
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。

オプション	推奨されるアクション
	• 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、「このデータはKMSキーオプションで暗号化され」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。

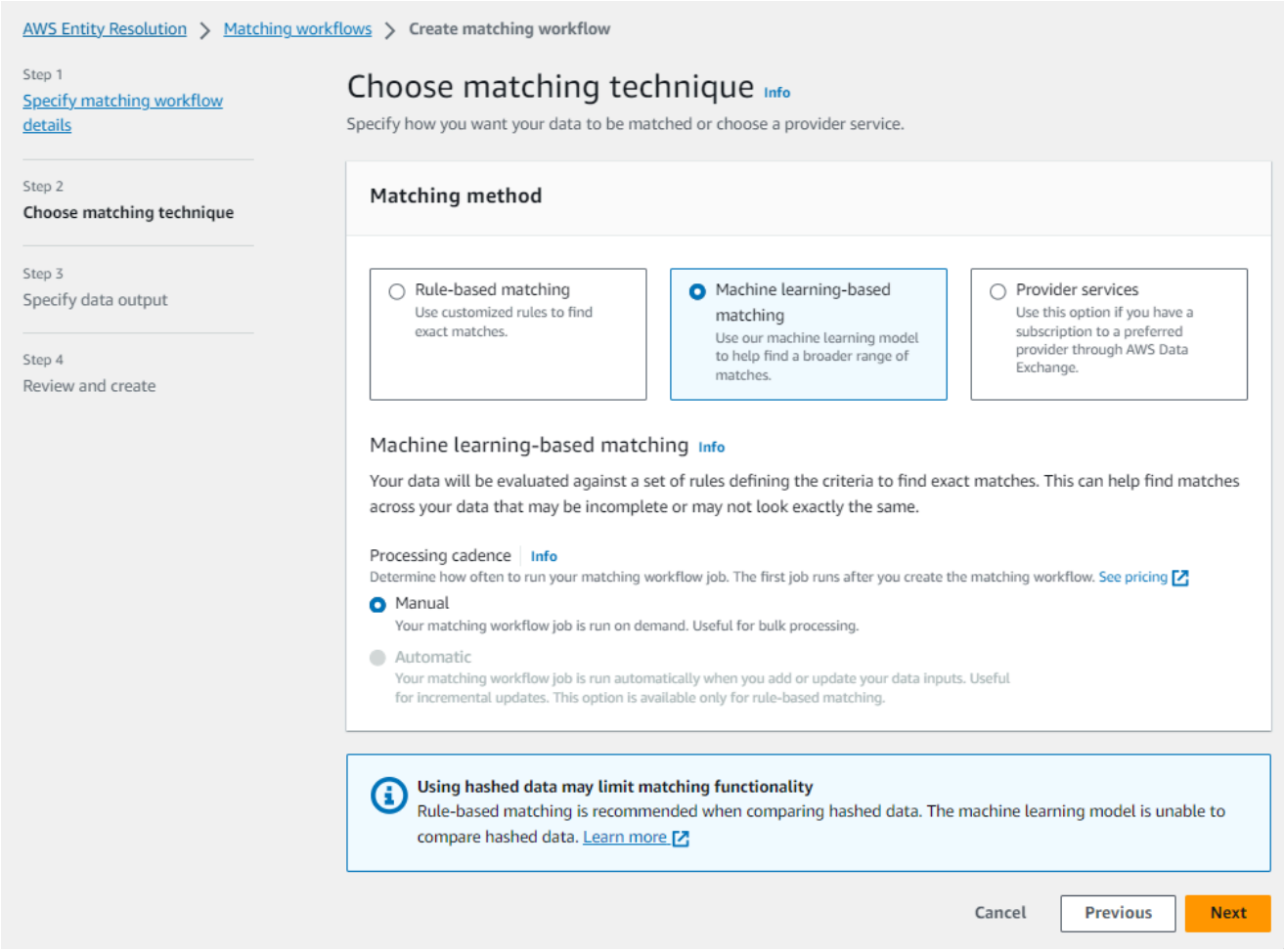
オプション	推奨されるアクション
既存のサービスロールを使用	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. 外部リンクで表示IAMを選択して、サービスロールを表示します。 デフォルトでは、 AWS Entity Resolution は既存のロールポリシーを更新して必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

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。



AWS Entity Resolution マッチングワークフロー作成インターフェイスと、ルールベースまたは機械学習マッチングのオプション。

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. [Next (次へ)] を選択します。

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、データ形式が正規化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 を入力しますARN。

c. システム生成の出力 を表示します。

d. データ出力 では、含める、非表示にする、またはマスクするフィールドを決定し、目標に基づいて推奨アクションを実行します。

目標	推奨オプション
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. [Next (次へ)] を選択します。

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。
- IDs 生成された一意の一致。
- 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。
10. (手動処理タイプのみ) 手動処理タイプで機械学習ベースのマッチングワークフローを作成した場合は、一致するワークフローの詳細ページでワークフローの実行を選択して、一致するワークフローをいつでも実行できます。

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の作成

プロバイダーのサービスベースのマッチングでは、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、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

サポートされているプロバイダーサービスの詳細については、「」を参照してくださいサードパーティーの入力データの準備。

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。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ステップ 1: 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

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

を使用したマッチング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、 LiveRamp サービスで一致するワークフローを作成して ID 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IDsで最も一般的に使用される 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 に解決できますRAMPIDs。

> **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 を置き換える *<user input placeholder>* 自分の情報を入力します。

staging-bucket	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. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。

オプション	推奨されるアクション
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、「このデータはKMSキーオプションで暗号化され」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。

オプション	推奨されるアクション
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. 外部リンクで表示IAM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. [Next (次へ)] を選択します。

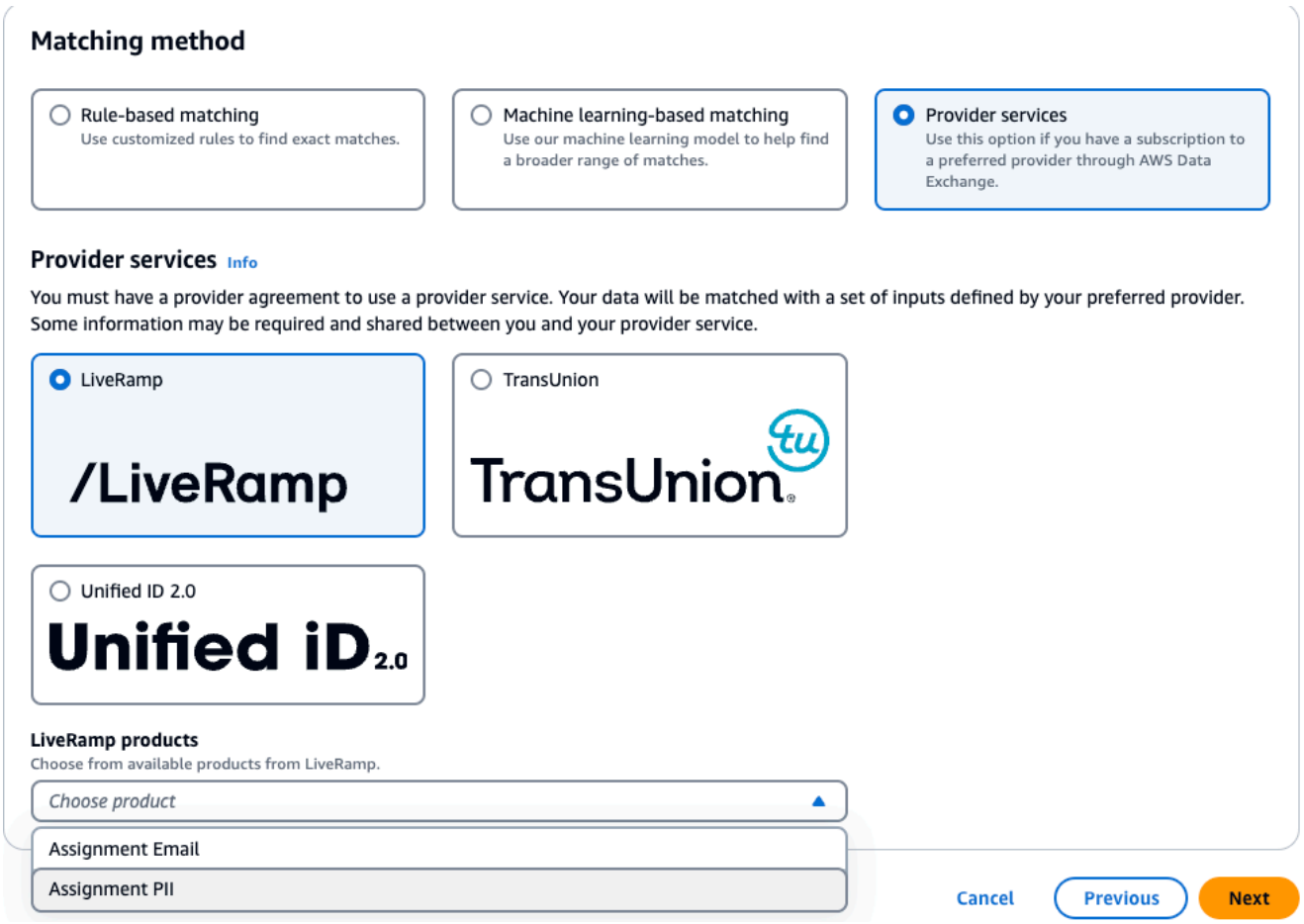
5. ステップ 2: 一致する手法を選択する：

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「 によるアイデンティティ解決の実行ADX」を参照してください。

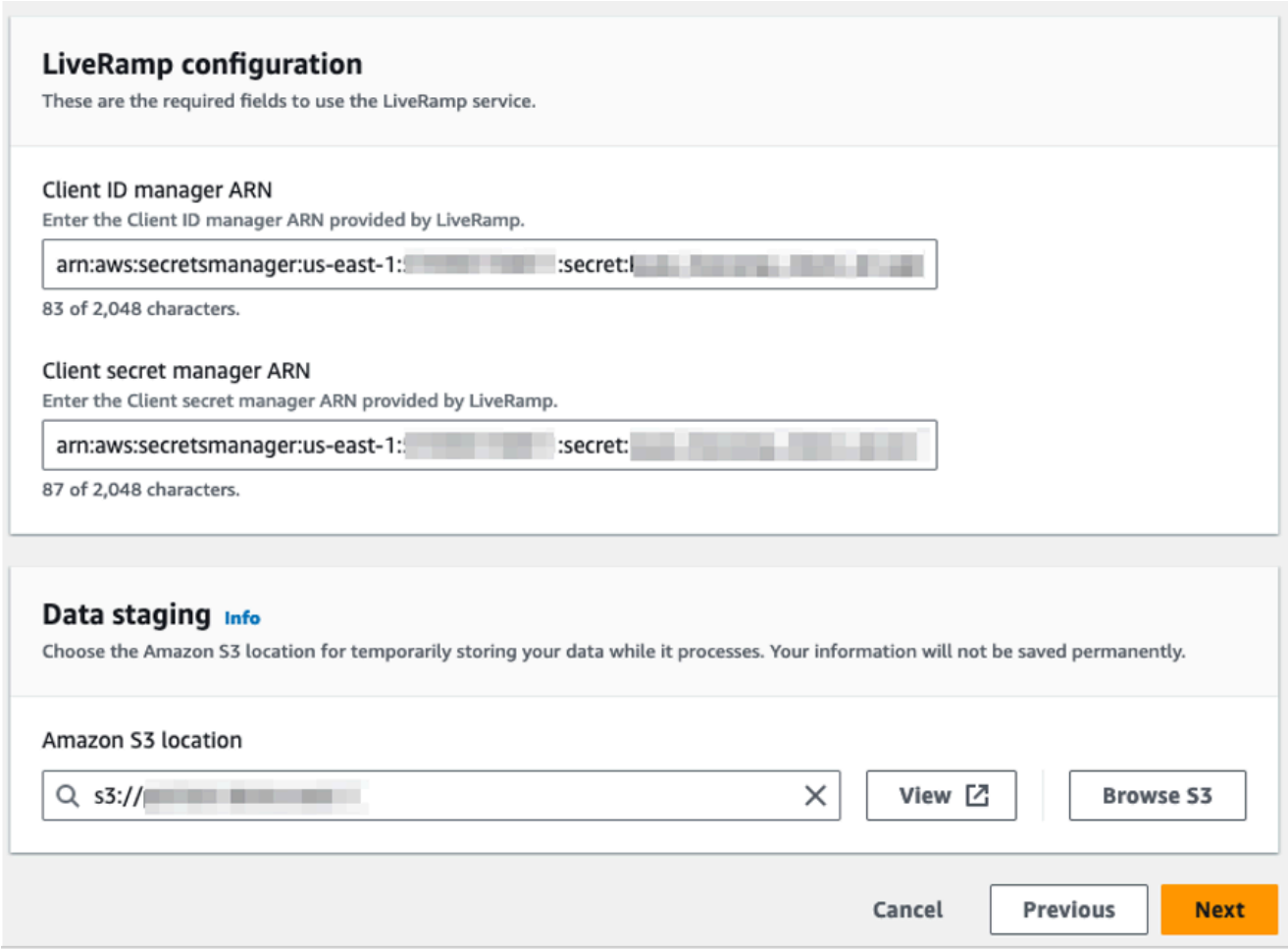
c. LiveRamp 製品 の場合、ドロップダウンリストから製品を選択します。



マッチング方法のオプション: 完全一致の場合はルールベース、より広範な一致の場合は機械学習、プロバイダーサービス。

> **Note**
>
> 割り当て を選択した場合はPII、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、 などですGENDER。

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。



LiveRa
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 のフィールドを含む 設定フォームARN。

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。

Amazon S3 ロケーション をステージングするデータに対するアクセス許可が必要です。詳細については、「のワークフローロールの作成 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 を入力しますARN。

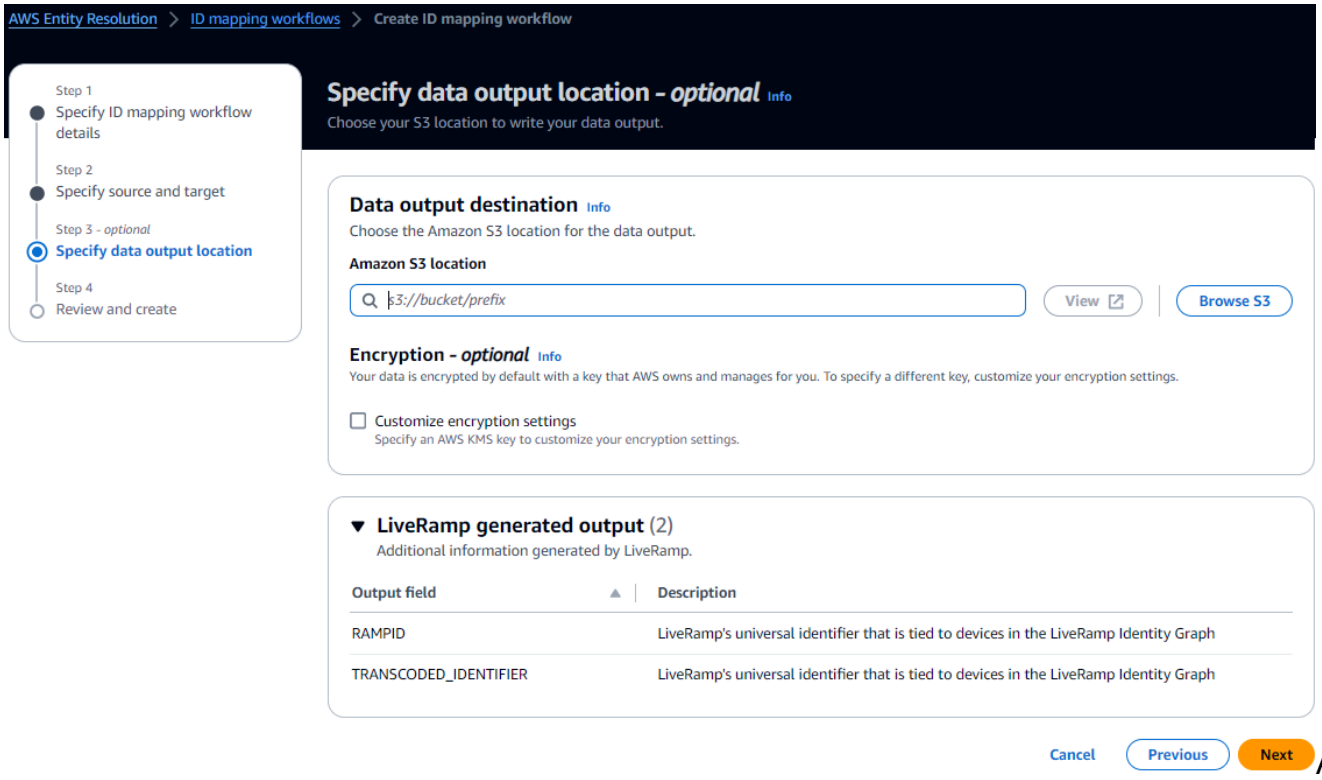
c. LiveRamp 生成された出力 を表示します。

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、含めるフィールド、非表示にするフィールド、またはマスクするフィールドを決定し、目標に基づいて推奨アクションを実行します。

> **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使用不可 と表示されます。

目標	推奨されるアクション
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。



AWS Entity Resolution データ出力場所を指定するオプションを備えた ID マッピングワークフロー作成インターフェイス。

e. [Next (次へ)] を選択します。

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。

- IDs 生成された一意の一致。
- 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ら (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。

を使用したマッチング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 個人および世帯 と呼ばれる識別子を提供しますIDs。名前、住所、電話番号、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) TransUnion 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 を置き換える *<user input placeholder>* 自分の情報を入力します。

staging-bucket	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、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 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. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。

オプション	推奨されるアクション
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、「このデータはKMS キーオプションで暗号化され」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。

オプション	推奨されるアクション
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. 外部リンクで表示IAM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. [Next (次へ)] を選択します。

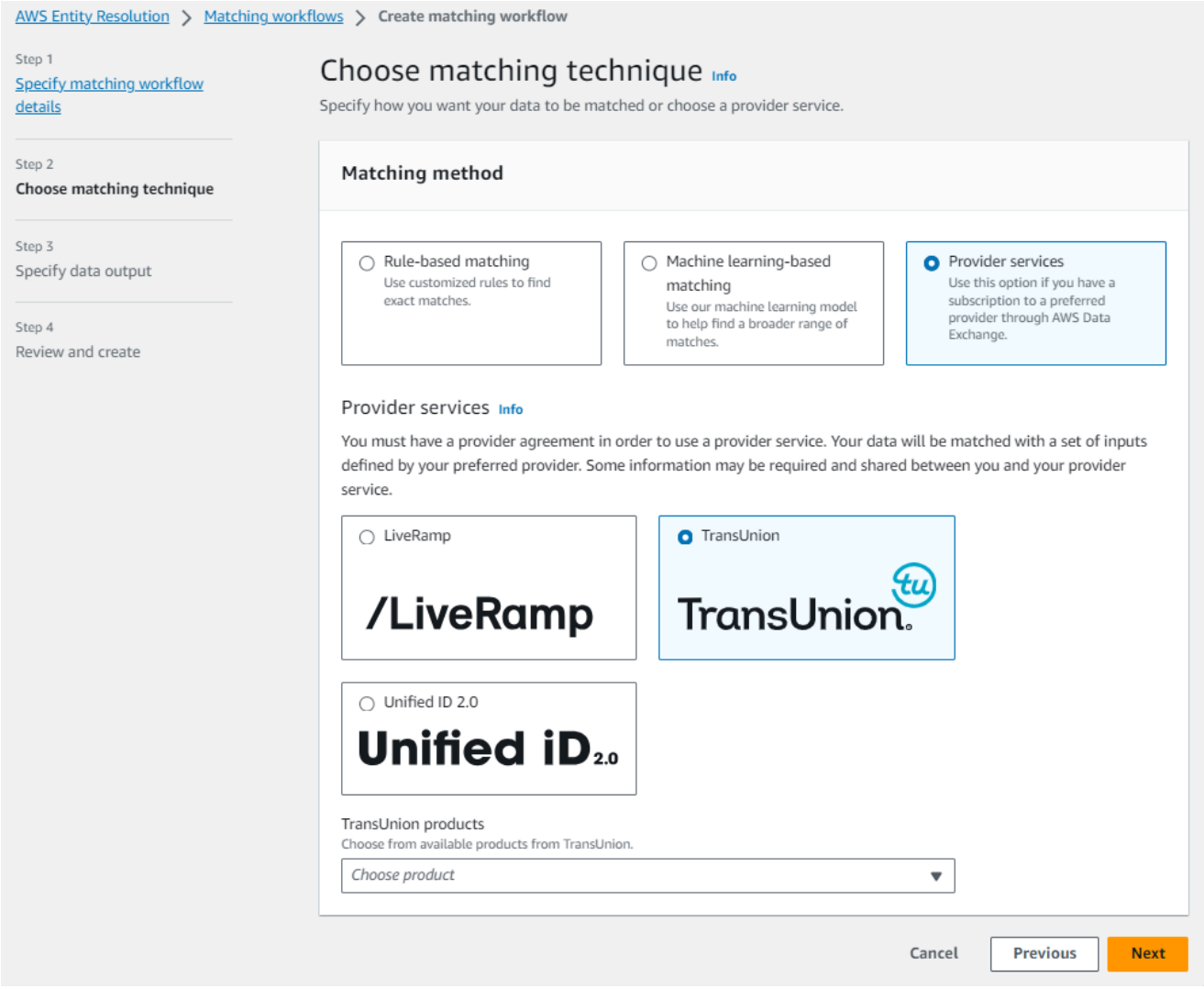
5. ステップ 2: 一致する手法を選択する：

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。



AWS Entity Resolution サービスマッチング手法オプション: ルールベース、機械学習ベース、またはプロバイダーサービス。

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 “ワークフロージョブロールの作成”」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 を入力しますARN。

   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、含める、非表示にする、またはマスクするフィールドを決定し、目標に基づいて推奨アクションを実行します。

目標	推奨されるアクション
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. 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. [Next (次へ)] を選択します。
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。
- IDs 生成された一意の一致。
- 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の一致に関する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。

2.0 UID 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で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 UID2が有効な多くの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、「統合 ID 2.0 の概要」を参照してください。

Unified ID 2.0 サービスは raw 2 UID を提供します。これは、Trade Desk 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UID2の生成**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**がマッピング**Email Address**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、1 年に約 1 回ローテーションされるソルトバケットからソルトを追加することで作成され、Raw UID2もローテーションされます。したがって、raw はUID2s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/「geting-started/gs-faqs#how-often-should-uid2s-be-refreshed-for-incremental-updates」を参照してください。

2.0 UID 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. 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 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、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。 UID

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

   d. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。

オプション	推奨されるアクション
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。

オプション	推奨されるアクション
	• 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キーオプションで暗号化され」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。

オプション	推奨されるアクション
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. 外部リンクでIAM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。

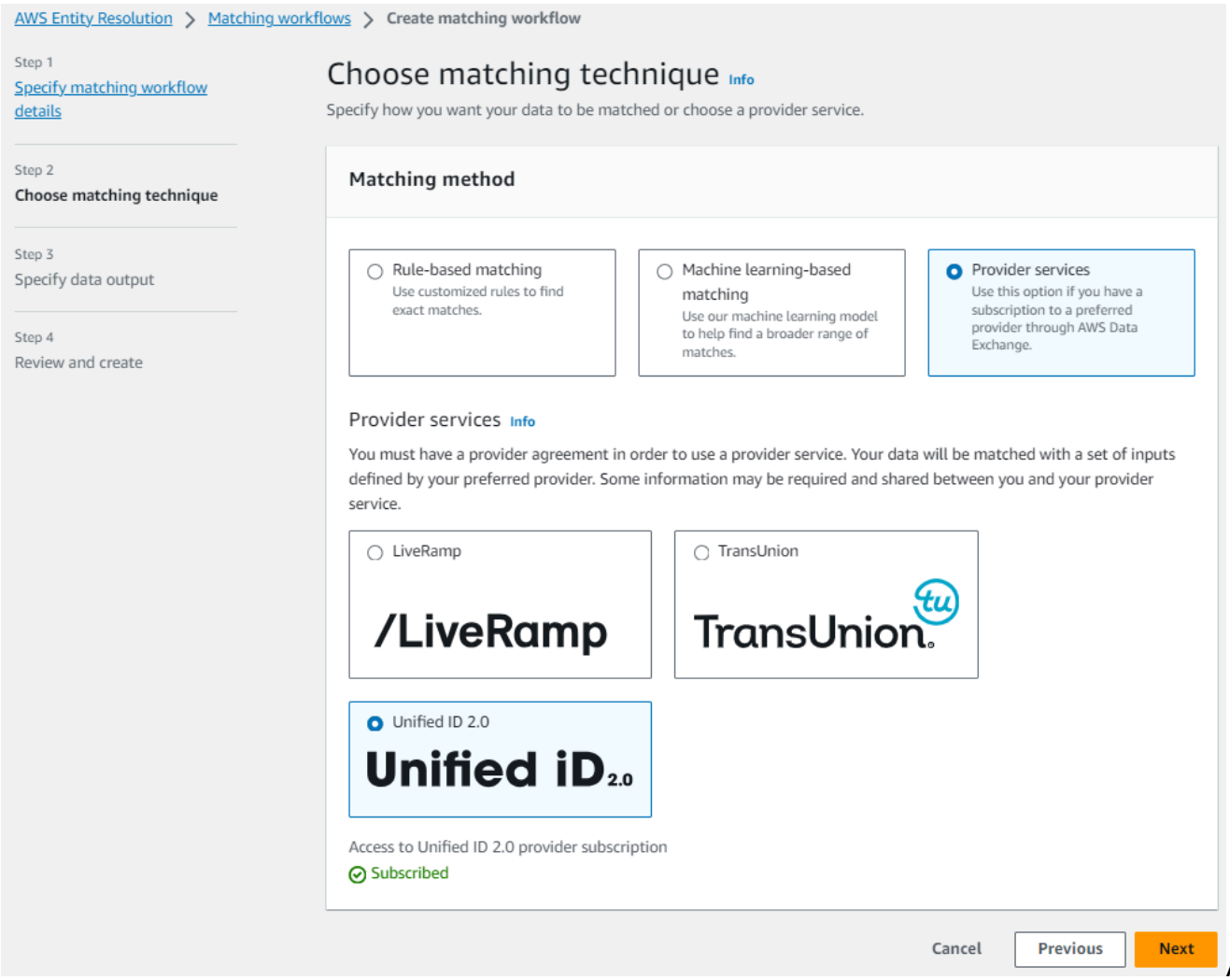
e. （オプション) リソースのタグを有効にするには、新しいタグの追加 を選択し、キーと値のペアを入力します。

f. [Next (次へ)] を選択します。

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。



AWS Entity Resolution サービスマッチング手法オプション: ルールベース、機械学習ベース、またはプロバイダーサービス。

c. [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 を入力しますARN。

c. Unified ID 2.0 で生成された出力 を表示します。

これは、 2.0 UID 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、含める、非表示にする、またはマスクするフィールドを決定し、目標に基づいて推奨アクションを実行します。

目標	推奨されるアクション
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. [Next (次へ)] を選択します。

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。
- 処理されていないレコードの数。
- IDs 生成された一意の一致。
- 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。

一致するワークフローの編集

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 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. データ出力の指定ページで、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の削除

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 の検索

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 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のレコードの削除

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. 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削除IDsを選択します。
5. 「ユニーク」セクションに、削除する一意の ID IDsを入力します。

   最大 10 個の一意の を入力できますIDs。
6. 一意の を削除する入力ソースを指定しますIDs。

   ワークフローの入力ソースが 1 つしかない場合、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の一意の は影響を受けません。
7. 一意の の削除 IDsを選択します。

マッチングワークフローのトラブルシューティング

次の情報は、一致する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。

一致するワークフローを実行した後にエラーファイルを受信しました

一般的な原因

一致する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。

一致するワークフローの成功結果は、複数のファイルを含む`success`フォルダに書き込まれ、各ファイルには成功したレコードのサブセットが含まれます。

一致するワークフローのエラーは、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。

エラーファイルは、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
  - が 38 文字を超えている (ルールベースのマッチングワークフローのみ)
- 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

> **Note**
>
> エラーファイルのレコードが前述の理由で作成された場合は、サービスの処理コストが発生するため、課金されます。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。

解決方法

この問題を解決するには

1. 一意の ID が有効かどうかを確認します。

   一意の ID が有効でない場合は、データテーブルの一意の ID を更新し、新しいデータテーブルを保存して、新しいスキーママッピングを作成し、一致するワークフローを再度実行します。

2. 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るかどうかを確認します。

   いずれかのフィールドに予約名が含まれている場合は、新しい名前で新しいスキーママッピングを作成し、一致するワークフローを再度実行します。

ID マッピングワークフローを使用して入力データをマッピングする

ID マッピングワークフローは、指定された ID マッピング方法に基づいて入力データソースから入力データターゲットにデータをマッピングするデータ処理ジョブです。ID マッピングテーブルを生成します。

ID マッピングワークフローには、入力データソースと入力データターゲットが必要です。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。ID マッピングを実行するには、ルールベースまたはプロバイダーサービスの 2 つの方法があります。

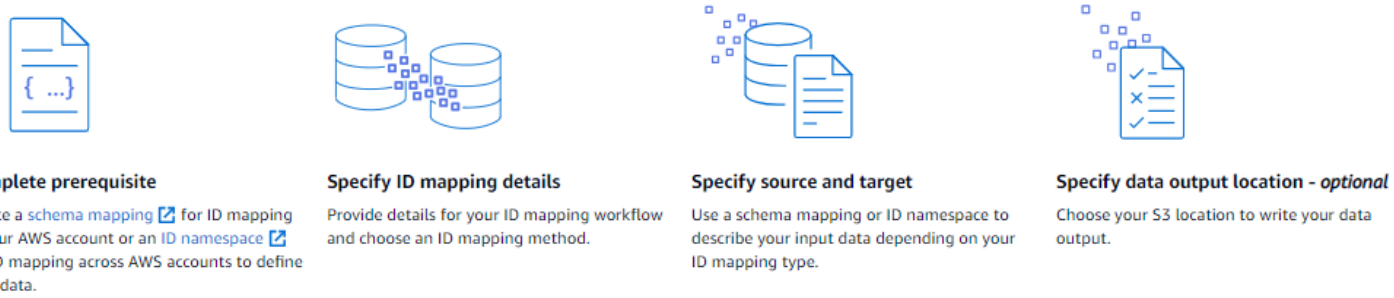
- ルールベースの ID マッピング — 一致するルールを使用して、ファーストパーティーデータをソースからターゲットに変換します。
- プロバイダーサービス ID マッピング — LiveRamp プロバイダーサービスを使用して、サードパーティーのデータをソースからターゲットに変換します。

> **Note**
>
> のプロバイダーサービス 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 ID マッピングワークフローを作成して LiveRamp 、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 R のセットampIDs を任意のターゲットターゲットの 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。詳細については、ドキュメントウェブサイトの「Perform Translation ThroughADX LiveRamp 」を参照してください。

次のシナリオのいずれかで、2 つのデータセット間で ID マッピングを実行できます。

- 独自の 内 AWS アカウント
- 2 つの異なる AWS アカウント

次の図は、ID マッピングワークフローを設定する方法をまとめたものです。



トピック

- 1 つの の ID マッピングワークフロー 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 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
- ID マッピングワークフローの編集
- ID マッピングワークフローの削除
- ID マッピングワークフローのリソースポリシーの追加または更新

1 つの の ID マッピングワークフロー AWS アカウント

1 つの の ID マッピングワークフロー AWS アカウントを使用すると、独自の で 2 つのデータセット間で ID マッピングを実行できます AWS アカウント。

独自の で 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、まず前提条件 を完了する必要があります。

ID マッピングワークフローを作成して実行したら、出力 (ID マッピングテーブル) を表示し、分析に使用できます。

以下のトピックでは、同じ で ID マッピングワークフローを作成する一連のステップについて説明します AWS アカウント。

トピック

- 前提条件
- ID マッピングワークフローの作成 (ルールベース)
- ID マッピングワークフローの作成 (プロバイダーサービス)

前提条件

ルールベースまたはプロバイダーサービス ID マッピング方式 AWS アカウント を使用して ID マッピングワークフローを作成する前に、まず次の操作を行う必要があります。

- AWS 「エンティティ解決の設定」のタスクを完了します。
- スキーママッピングを作成するか、一致するワークフローを作成します。
- (プロバイダーサービス ID マッピングのみ) で ID マッピングワークフローを作成する前に LiveRamp、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を選択する必要があります。

  LiveRamp プロバイダーサービスを使用してサードパーティーデータを翻訳する場合は、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>/*"
            ]
        }
    ]
}
```

前述のアクセス許可ポリシーで、各 を置き換えます。*<user input placeholder>* 自分の情報を入力します。

staging-bucket	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。

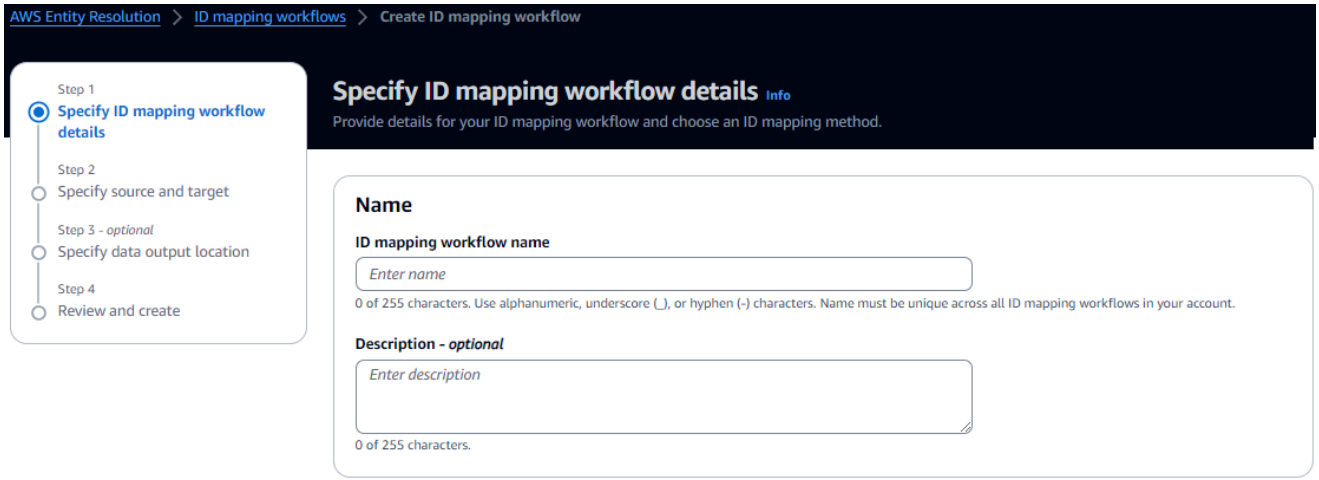
ID マッピングワークフローの作成 (ルールベース)

このトピックでは、一致するルールを使用してファーストパーティーデータをソースからターゲットに変換 AWS アカウント する ID マッピングワークフローを作成するプロセスについて説明します。

ルールベースの 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 マッピングメソッドで、ルールベースの 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。

d. [Next (次へ)] を選択します。

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、該当するシナリオを選択し、推奨アクションを実行します。

シナリオ	推奨されるアクション
ID マッピングワークフローで独自の AWS Glue データベース、 Glue AWS テーブル、スキーママッピングを使用します。	1. スキーママッピング を選択します。 2. 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。
ID マッピングワークフローで使用するレコードデータを指す既存のマッチングワークフローを使用します。	1. ワークフローの一致 を選択します。 2. ドロップダウンリストから既存の一致ワークフローを選択します。

b. ターゲット で、ドロップダウンリストから既存の一致ワークフローを選択します。

c. ルールパラメータ で、次の操作を行います。

i. ソースタイプに基づいて次のいずれかのオプションを選択して、ルールコントロールを指定します。

ソースタイプ	推奨されるアクション
マッチングワークフロー	ソース 、ターゲット 、またはその両方が ID マッピングワークフローでルールを提供できるかどうかを選択して、ルールコントロールを指定します。 ルールコントロールは、ID マッピングワークフローで使用するソースとターゲットの間で互換性がある必要があります。 例えば、ソース ID 名前空間がルールをターゲットに制限し、ターゲット ID 名前空間がルールをソースに制限する場合、エラーが発生します。
スキーママッピング	この手順をスキップしてください。

ii. 比較およびマッチングパラメータ の場合、比較タイプ は自動的に複数の入力フィールド に設定されます。

これは、両方の参加者が以前にこのオプションを選択したためです。

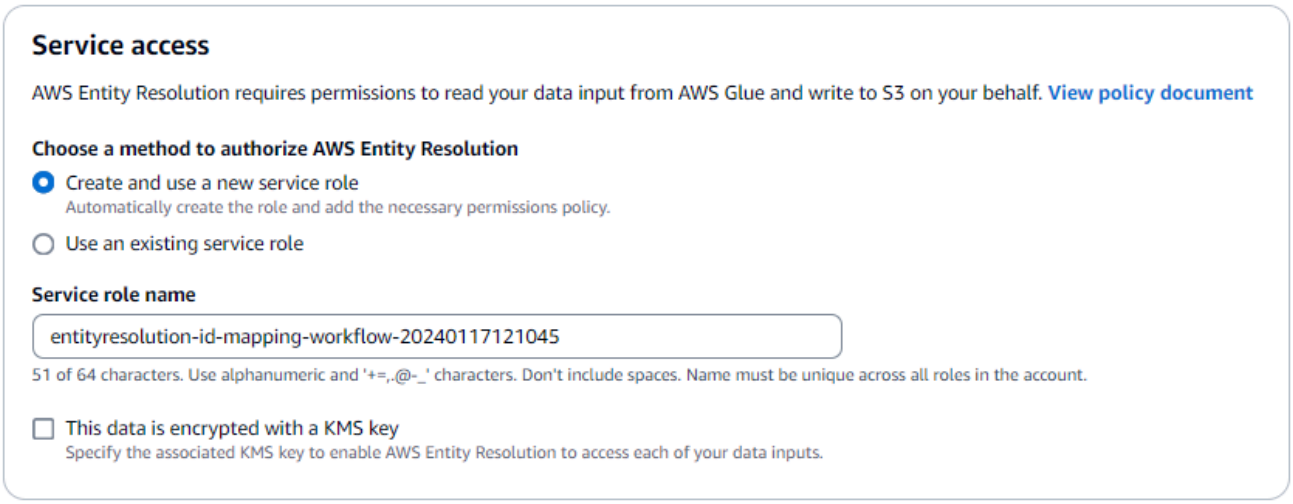
d. 目標に基づいて次のいずれかのオプションを選択して、レコードマッチングタイプを指定します。

目標	推奨オプション
ID マッピングワークフローを作成するときに、ターゲット内の一致したレコードごとにソースに一致レコードを 1 つだけ保存するようにレコード一致タイプを制限します。	1 つのソースから 1 つのターゲットへ

目標	推奨オプション
ID マッピングワークフローを作成するときに、レコード一致タイプを制限して、ターゲット内の一致した各レコードのソースにすべての一致レコードを保存します。	1 つのターゲットへの多くのソース

> **Note**
>
> ソース ID 名前空間とターゲット ID 名前空間に互換性のある制限を指定する必要があります。

e. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。



オプション	推奨されるアクション
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キーオプションで暗号化されます」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。

オプション	推奨されるアクション
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. [Next (次へ)] を選択します。
7. ステップ 3: データ出力場所を指定する – オプション で、次の手順を実行します。
   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 を入力するARN か、 AWS KMS キー の作成 を選択します。
   b. [Next (次へ)] を選択します。
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. [Create] (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。

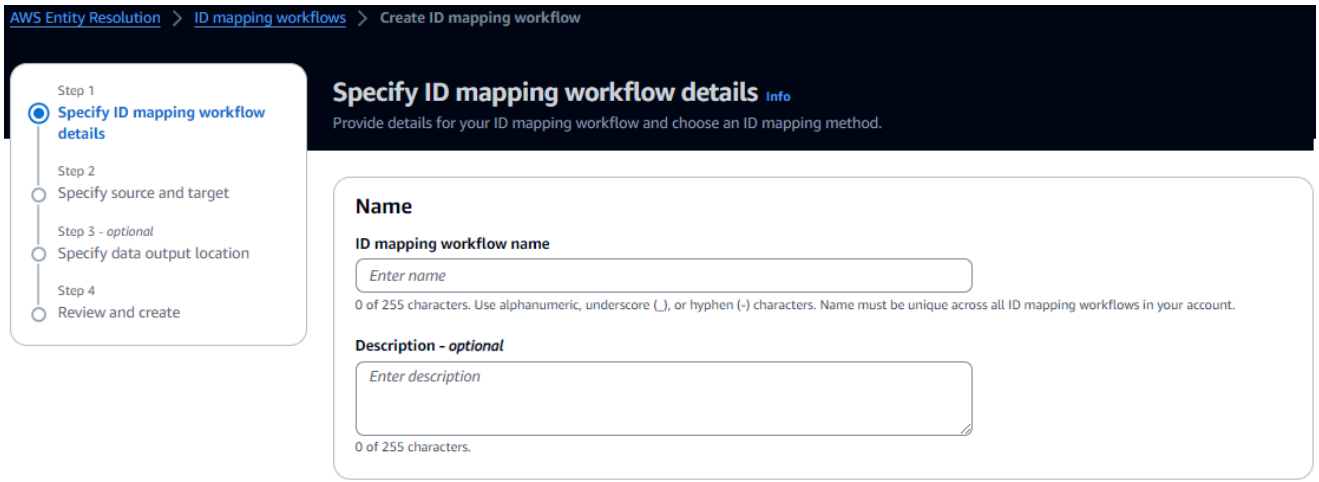
ID マッピングワークフローの作成 (プロバイダーサービス)

このトピックでは、 というプロバイダーサービス AWS アカウント を使用して ID マッピングワークフローを作成するプロセスについて説明します LiveRamp。 は、ソース R のセットampIDs を、維持されている R または派生した R を使用して別のセット LiveRamp に変換しますampIDs。

プロバイダーのサービスベースの 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

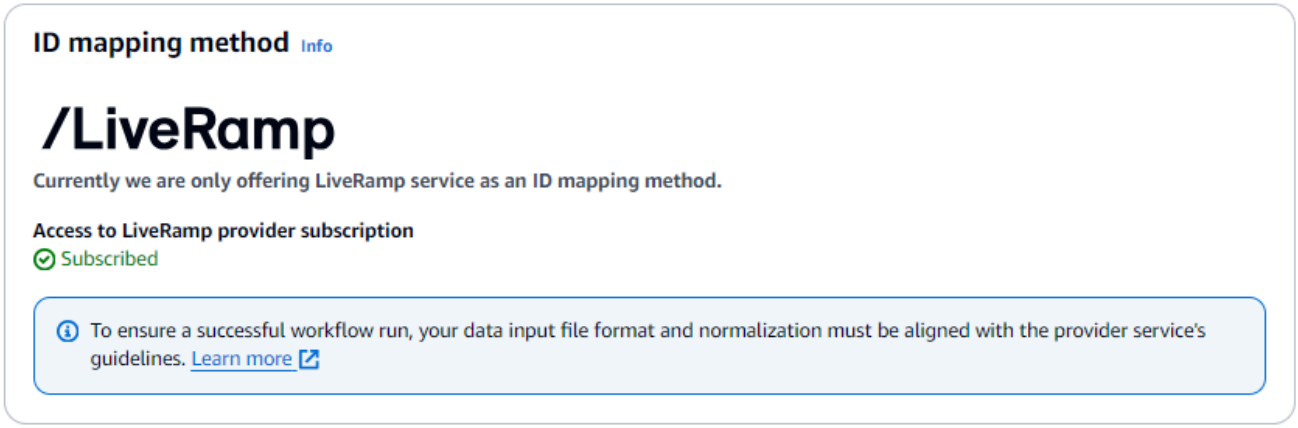
1. にサインイン AWS Management Console して AWS アカウント、まだ でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのワークフロー で、ID マッピング を選択します。
3. ID マッピングワークフローページの右上隅で、ID マッピングワークフローの作成 を選択します。
4. ステップ 1: ID マッピングワークフローの詳細を指定するには、次の手順を実行します。

   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 マッピングメソッド で、プロバイダーサービス を選択します。

      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ステップ 1: 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「Perform Translation ThroughADX」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。

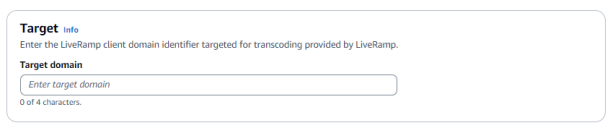
e. [Next (次へ)] を選択します。

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。

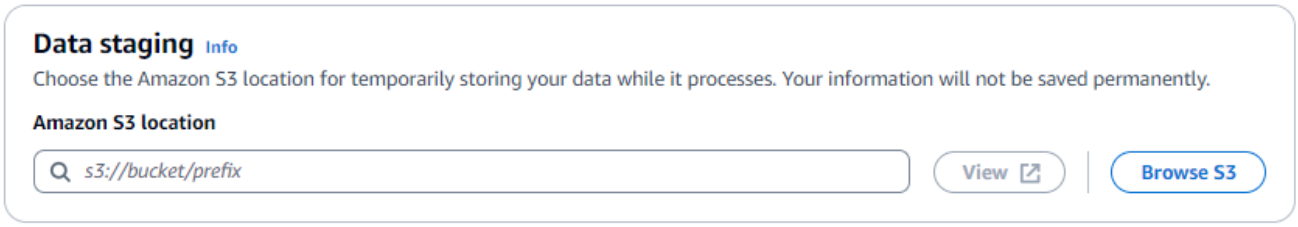
a. ソース で、該当するシナリオを選択し、推奨アクションを実行します。

シナリオ	推奨されるアクション
ID マッピングワークフローで独自の AWSGlue データベース、 Glue AWS テーブル、スキーママッピングを使用します。	1. スキーママッピング を選択します。 2. 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。
ID マッピングワークフローで使用するレコードデータを指す既存のマッチングワークフローを使用します。	1. 一致するワークフロー を選択します。 2. ドロップダウンリストから既存の一致ワークフローを選択します。

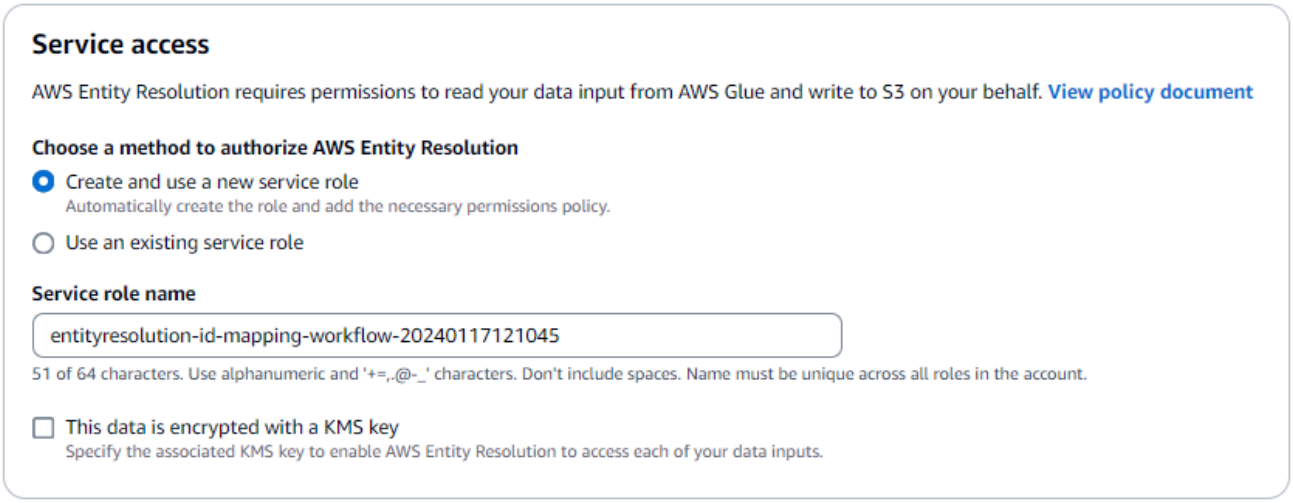
b. ターゲット では、選択した ID マッピング方法に基づいて、次のいずれかのアクションを実行します。

ID マッピング方法	推奨されるアクション
ルールベース	ドロップダウンリストから既存の一致ワークフローを選択します。
プロバイダーサービス	ターゲットドメイン で 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。



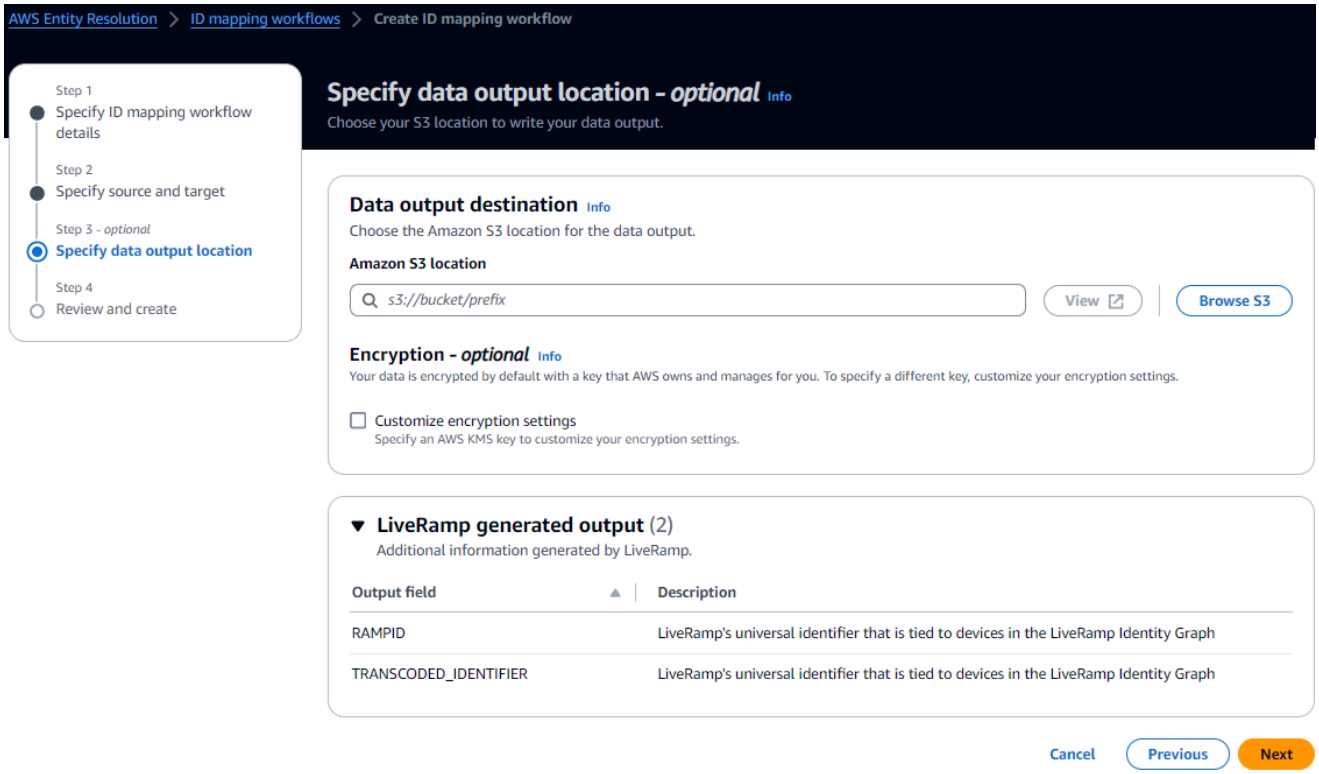
d. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。



オプション	推奨されるアクション
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キーオプションで暗号化されます」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。

オプション	推奨されるアクション
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. [Next (次へ)] を選択します。
7. ステップ 3: データ出力場所を指定する – オプション で、次の手順を実行します。
   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 を入力するARN 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. [Next (次へ)] を選択します。



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. [Create] (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。

9. 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 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 AWS アカウントを使用すると、2 つの にわたる 2 つのデータセット間の ID マッピングを実行できます AWS アカウント。これは通常、独自の AWS アカウント と別の の間で行われます AWS アカウント。

例えば、パブリッシャーは、独自のターゲット ID 名前空間 (独自の) とアドバタイザーのソース ID 名前空間 (別の AWS アカウント) を使用して ID マッピングワークフローを作成できます AWS アカウント。

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、まず前提条件 を完了する必要があります。

ID マッピングワークフローを作成したら、出力 (ID マッピングテーブル) を表示して分析に使用できます。

以下のトピックでは、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一連のステップについて説明します AWS アカウント。

トピック

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前に AWS アカウント、まず以下を実行する必要があります。

- 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。
- 別の から ID 名前空間ソースを使用している場合ARNは、ID 名前空間を取得します AWS アカウント。
- (プロバイダーサービスのみ) 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、 LiveRamp は S3 バケットとカスタマーマネージドキー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"
            }
        }
    }]
}
```

前述のアクセス許可ポリシーで、各 を置き換えます。*<user input placeholder>* 自分の情報を入力します。

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

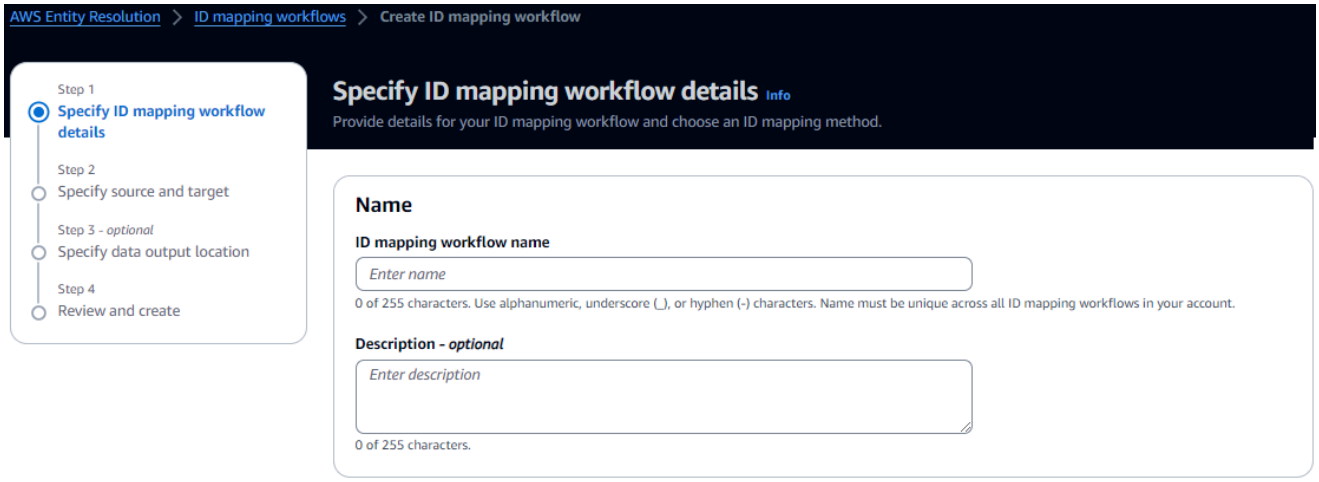
ID マッピングワークフローの作成 (ルールベース)

前提条件 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、一致するルールを使用してファーストパーティーデータをソースからターゲットに変換できます。

2 つの にまたがるルールベースの 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 マッピングメソッド で、ルールベースの 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。

d. [Next (次へ)] を選択します。

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、一致ワークフロー を選択し、ドロップダウンリストから既存の一致ワークフローを選択します。

c. ターゲット で、一致ワークフロー を選択し、ドロップダウンリストから既存の一致ワークフローを選択します。

d. ルールパラメータ で、ソースまたはターゲットが ID マッピングワークフローでルールを提供できるかどうかを選択して、ルールコントロールを指定します。

ルールコントロールは、ID マッピングワークフローで使用するソースとターゲットの間で互換性がある必要があります。例えば、ソース ID 名前空間がルールをターゲットに制限し、ターゲット ID 名前空間がルールをソースに制限する場合、エラーが発生します。

e. 比較および一致するパラメータ については、次の操作を行います。

i. 目標に基づいてオプションを選択して、比較タイプを指定します。

目標	推奨オプション
データが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	複数の入力フィールド

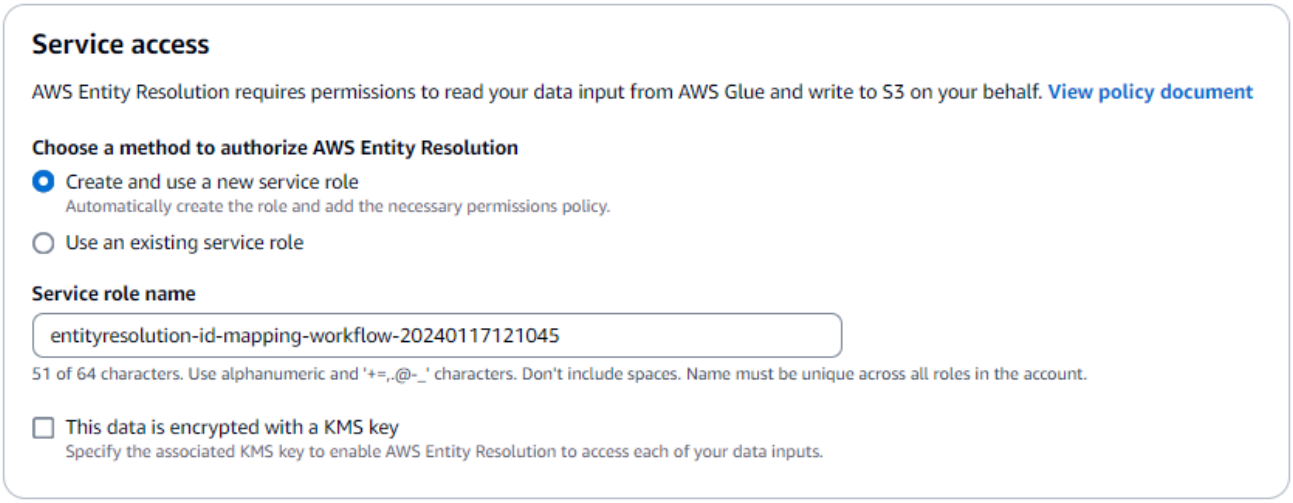
目標	推奨オプション
、複数の入力フィールドに保存されているデータ間で一致の任意の組み合わせを検索します。	
複数の入力フィールドに保存されている類似データを一致させない場合、1 つの入力フィールド内で比較を制限します。	単一入力フィールド

ii. 目標に基づいてオプションを選択して、レコードマッチングタイプを指定します。

目標	推奨オプション
ID マッピングワークフローを作成するときに、ターゲット内の一致したレコードごとにソースに一致レコードを 1 つだけ保存するようにレコード一致タイプを制限します。	1 つのソースから 1 つのターゲットへ
ID マッピングワークフローを作成するときに、レコード一致タイプを制限して、ターゲット内の一致した各レコードのソースにすべての一致レコードを保存します。	1 つのターゲットへの多くのソース

> **Note**
>
> ソース ID 名前空間とターゲット ID 名前空間に互換性のある制限を指定する必要があります。

f. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。



オプション	推奨されるアクション
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キーオプションで暗号化されます」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。

オプション	推奨されるアクション
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. [Next (次へ)] を選択します。
7. ステップ 3: データ出力場所を指定する – オプション で、次の手順を実行します。
   a. データ出力先 の場合、次の手順を実行します。
      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 を入力するARN 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. [Next (次へ)] を選択します。
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. [Create] (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。

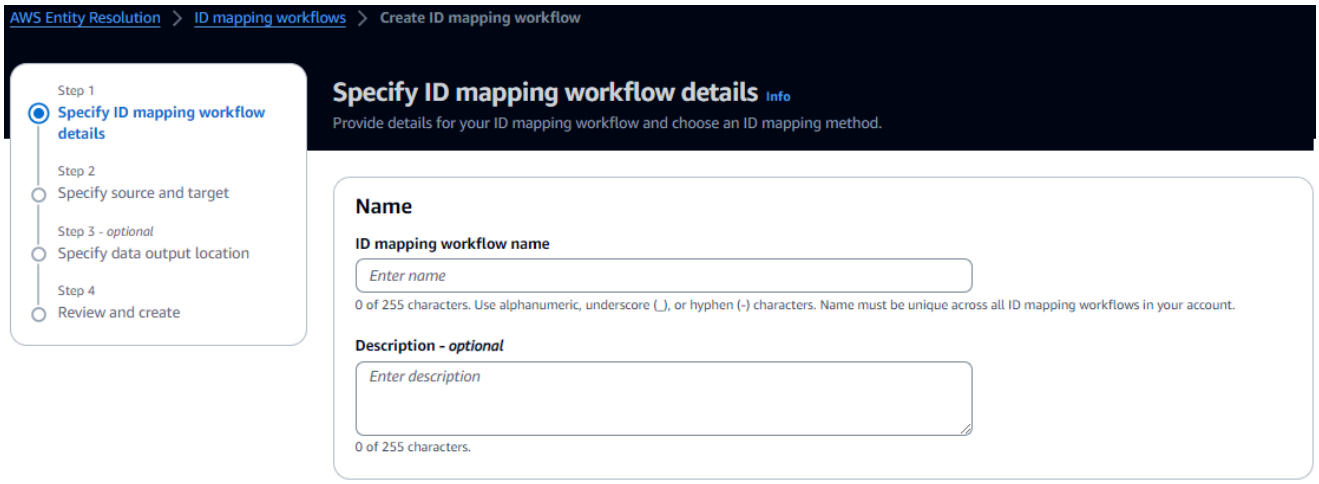
ID マッピングワークフローの作成 (プロバイダーサービス)

前提条件 を完了したら、 LiveRamp プロバイダーサービスを使用して 1 つ以上の ID マッピングワークフローを作成できます。 は、維持されている R または派生した R を使用して、ソース R のセットampIDs を別のセット LiveRamp に変換しますampIDs。

プロバイダーサービスを使用して ID マッピ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 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。

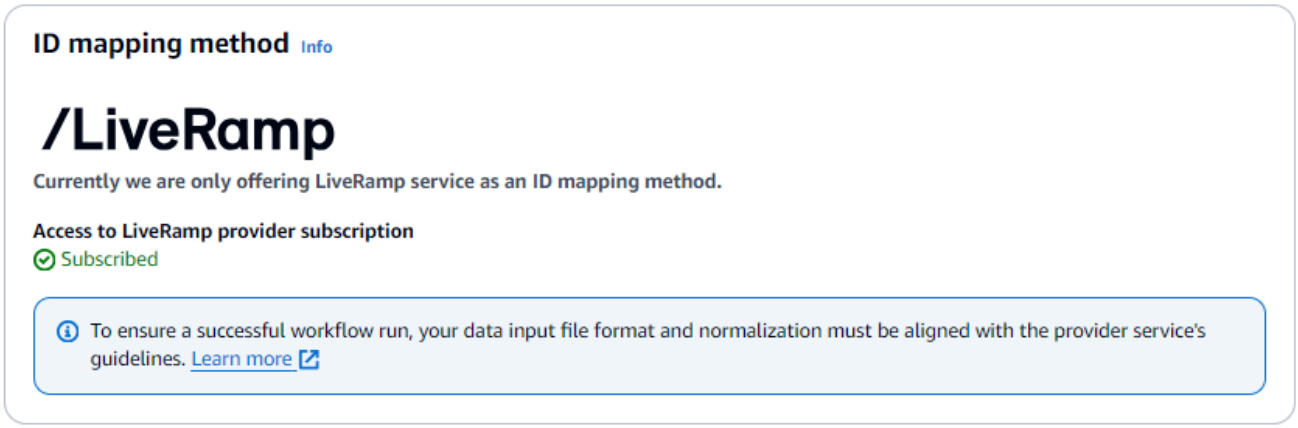
   a. ID マッピングワークフロー名とオプションの説明 を入力します。



   b. ID マッピングメソッド で、プロバイダーサービス を選択します。

   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

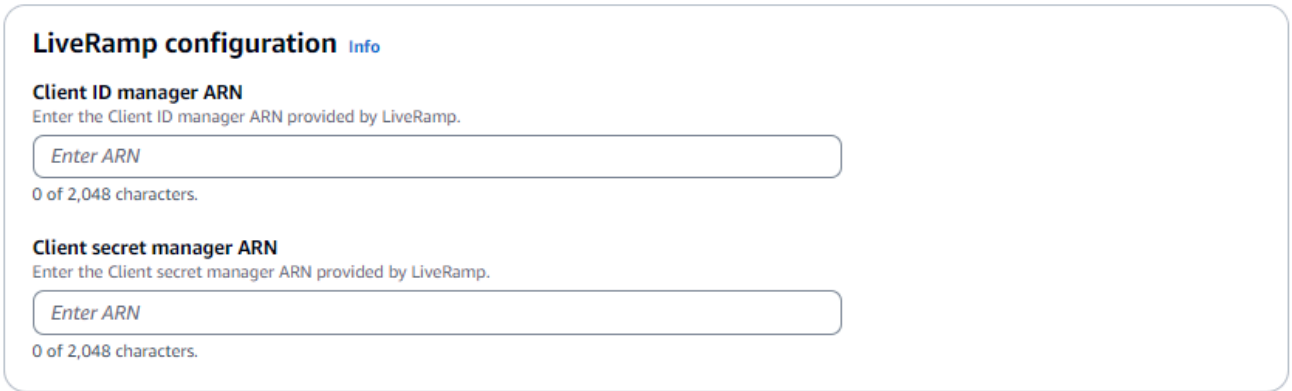
タスは Subscribed と表示されます。をサブスクライブする方法の詳細については、LiveRamp「」を参照してくださいステップ 1: でプロバイダーサービスをサブスクライブする AWS Data Exchange。



> **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「Perform Translation ThroughADX」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



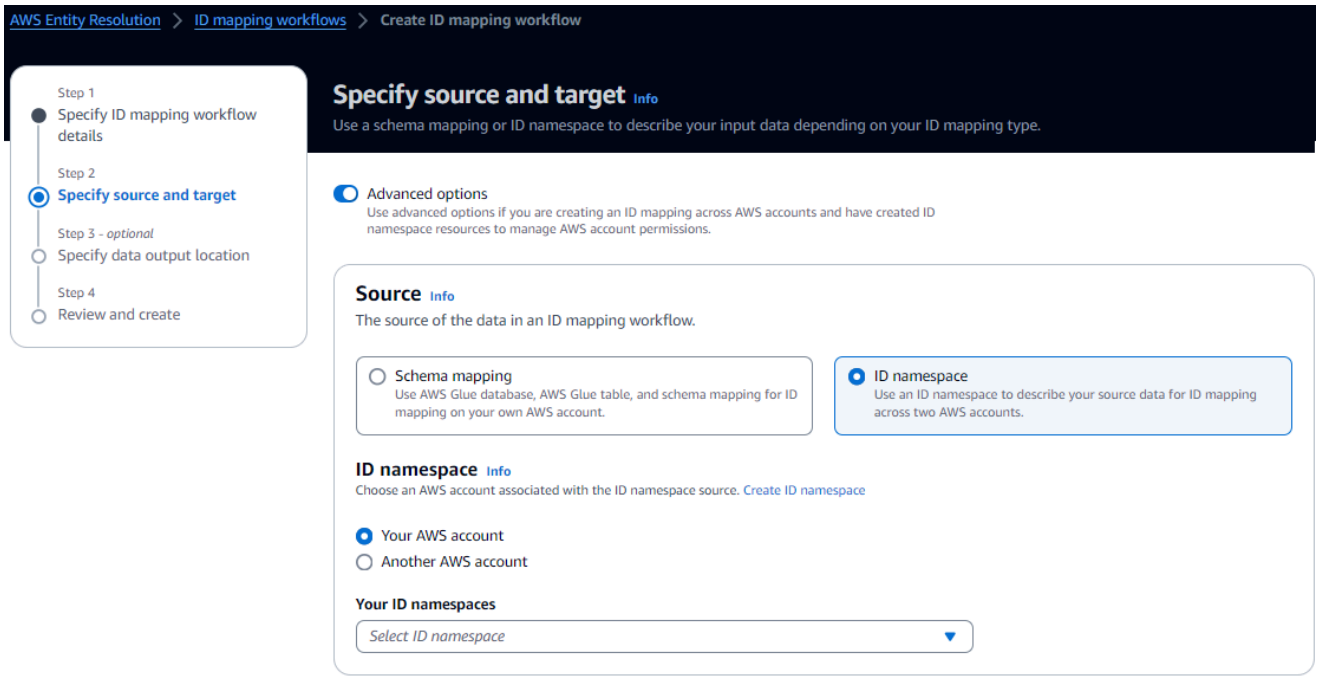
d. （オプション) リソースのタグを有効にするには、新しいタグの追加 を選択し、キーと値のペアを入力します。

e. [Next (次へ)] を選択します。

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。

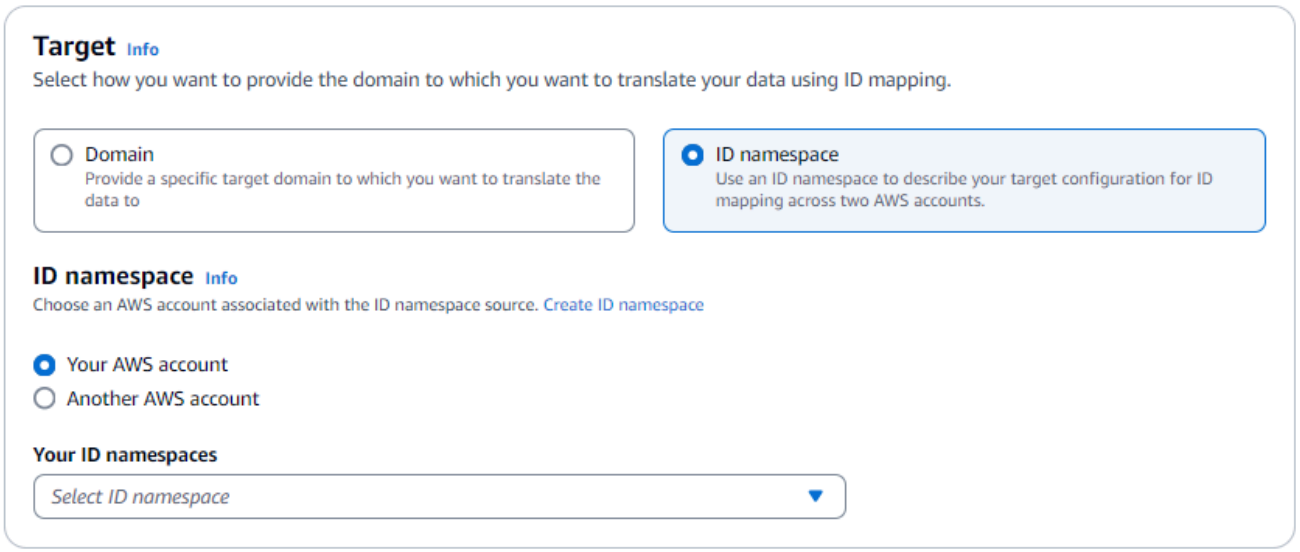
b. ソース で、ID 名前空間 を選択します。



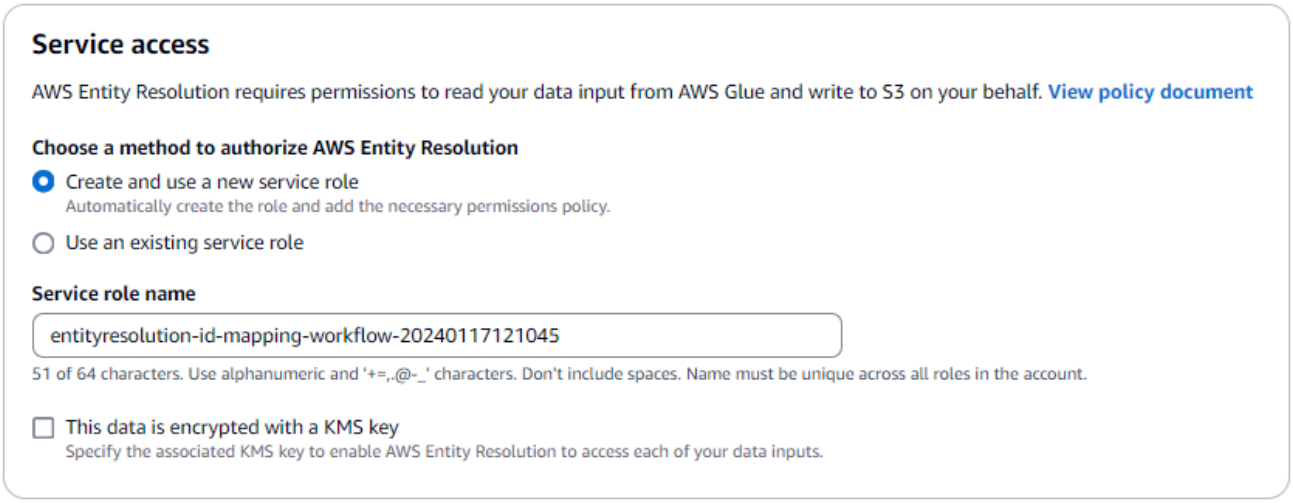
c. ID 名前空間の場合は、ID 名前空間の場所を特定し、推奨されるアクションを実行します。

ID 名前空間の場所	推奨されるアクション
独自の AWS アカウント	1. を選択します AWS アカウント。 2. ID 名前空間ドロップダウンリストから ID 名前空間を選択します。
他のユーザーの AWS アカウント	1. 別の AWS アカウントを選択します。 2. ID 名前空間 ARNを入力します。

d. ターゲット で、ID 名前空間 を選択します。



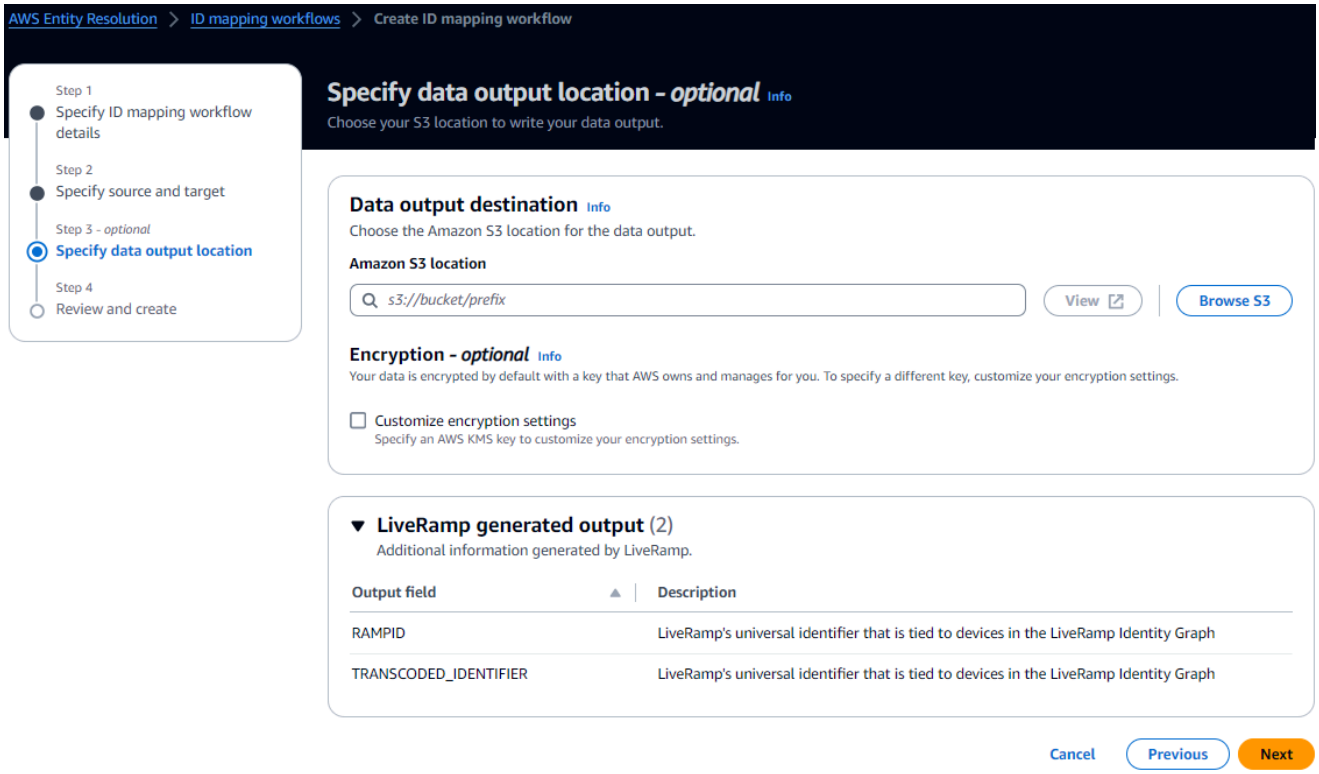
e. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。



オプション	推奨されるアクション
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キーオプションで暗号化されます」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。

オプション	推奨されるアクション
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. [Next (次へ)] を選択します。
7. ステップ 3: データ出力場所を指定する – オプション で、次の手順を実行します。
   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 を入力するARN 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. [Next (次へ)] を選択します。



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. [Create] (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はCSVファイルを出力します。

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、「最終ジョブメトリクス」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 を入力するARN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、 オプションを選択し、推奨アクションを実行します。

オプション	推奨されるアクション
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キーオプションで暗号化されます」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。 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

オプション	推奨されるアクション
	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. [Run] (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`。

ID マッピングワークフローの編集

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の削除

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。

ID マッピングワークフローの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 マッピングワークフロー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 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. [Save changes] (変更の保存) をクリックします。

プロバイダー AWS Entity Resolution として と統合する

AWS Entity Resolution サードパーティープロバイダーの統合は、顧客が消費者のプライバシーを保護し、データ主権法への準拠を維持するのに役立ちます。 LiveRamp や などのサードパーティープロバイダーは、コンシューマー識別子を Ramp IDsや Fabrick IDsなどの広告 TransUnionに変換しますIDs。これらの広告識別子は、コンシューマーデータが非AWS マネージドシステムにエクスポートされないようにするために、広告およびマーケティングツールで一般的に使用されます。このセクションでは、プロバイダーが と統合して AWS Entity Resolution 、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 で使用する広告にコンシューマー識別子をエンコードまたはトランスコードIDsするためのガイダンスを提供します。

現在 と統合されているプロバイダーサービスの詳細については、 AWS Entity Resolution「」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の作成。

トピック

- 要件
- AWS Entity Resolution OpenAPI 仕様の使用
- プロバイダー統合のテスト

要件

をプロバイダーサービスとして と統合する前に AWS Entity Resolution、次の要件を満たしてください。

トピック

- でプロバイダーサービスを一覧表示する AWS Data Exchange
- 属性を特定する
- AWS Entity Resolution Open API仕様をリクエストする

でプロバイダーサービスを一覧表示する AWS Data Exchange

サードパーティープロバイダーは、Data AWS Exchange (ADX) 製品カタログに製品を一覧表示する必要があります。製品が AWS Data Exchange Product Catalog に一覧表示されると、サブスクライバーはパブリックオファーまたはプライベートオファーのいずれかを通じて製品をサブスクライブできます。

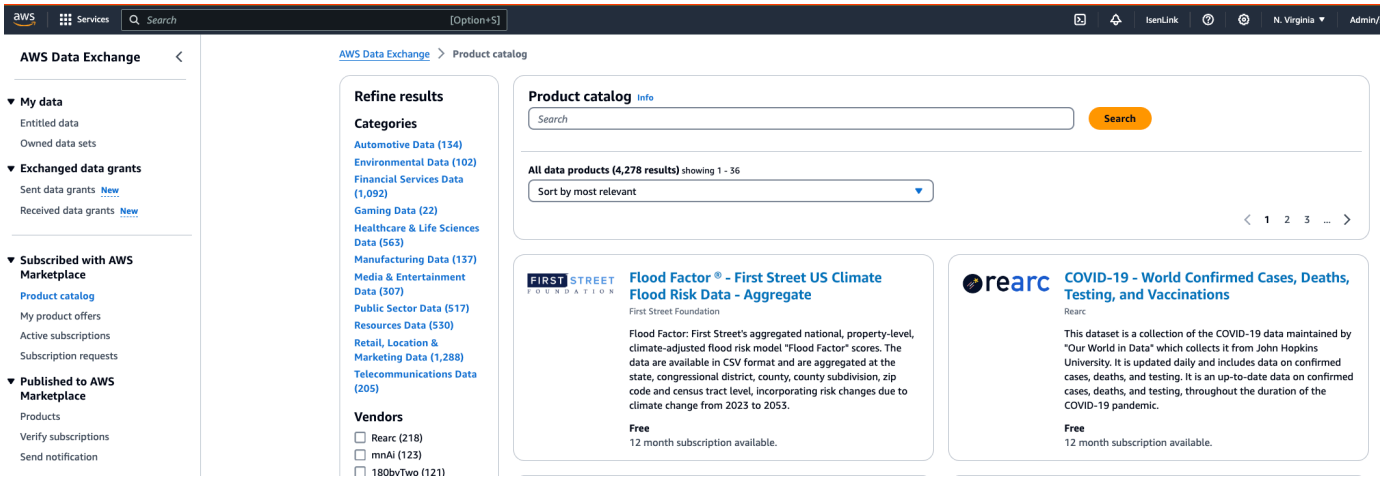
でプロバイダーサービスを一覧表示するには AWS Data Exchange

1. で新しいデータ製品プロバイダーである場合は AWS Data Exchange、「 AWS Data Exchange ユーザーガイド」の「プロバイダーとしての開始方法」セクションのステップを完了します。
2. REST API データセットを作成し、 AWS Data Exchange ユーザーガイドAPIsの「 を含む製品の公開方法」セクションの AWS Data Exchange 手順に従って、 を含む新しい製品を公開します。 APIs AWS Data Exchange コンソールまたは を使用してプロセスを完了できます AWS Command Line Interface。

   製品の可視性パブリック を設定した場合、パブリックオファーはすべてのサブスクライバーが利用できます。

   製品の可視性プライベート を設定している場合は、ユースケースに応じて、AWS Data Exchange 「 ユーザーガイド」の「カスタムオファーの作成」セクションのステップを完了します。

   次の図は、Product Catalog で利用可能な AWS Data Exchange 製品の例を示しています。



3. 製品が AWS Data Exchange Product Catalog で利用可能になると、サブスクライバーは次の方法で製品をサブスクライブできます。

   - パブリック製品をサブスクライブします。
   - プロバイダーサービスによって発行されたプライベートオファー (カスタムオファー) を使用します。
   - Bring Your Own Subscription (BYOS) オファーを使用します。

詳細については、「 ユーザーガイド」の「 を含む製品をサブスクライブしてアクセスAPIsするAWS Data Exchange 」を参照してください。

属性を特定する

入力データの属性は、ワークフローで解決されるエンティティのタイプ定義です。属性の例には、FirstName、LastName、Email、または がありますCustom String。

属性を特定するときは、要件やガイドラインに注意してください。

Example 例

以下は、プロバイダー属性を識別するための検証の例です。

- FirstName または LastName 属性のいずれかは必須です。
- Email 属性が存在する場合は、ハッシュ化する必要があります。

プロバイダーは、プロバイダーサービス製品の属性を特定し、これらの属性を AWS Entity Resolution <aws-entity-resolution-bd@amazon.com> のビジネス開発チームに伝達して、さらに検証する必要があります。

AWS Entity Resolution Open API仕様をリクエストする

AWS Entity Resolution には、プロバイダーとして統合APIsに関係する を含むハンドシェイクとして使用できる OpenAPI 仕様があります。詳細については、「AWS Entity Resolution OpenAPI 仕様の使用」を参照してください。

オープンAPI定義をリクエストするには、<aws-entity-resolution-bd@amazon.com>の AWS Entity Resolution ビジネス開発チームにお問い合わせください。

AWS Entity Resolution OpenAPI 仕様の使用

OpenAPI 仕様は、 に関連付けられているすべてのプロトコルを定義します AWS Entity Resolution。この仕様は、統合を実装するために必要です。

OpenAPI 定義には、次のAPIオペレーションが含まれます。

- POST AssignIdentities

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

Open 仕様をAPIリクエストするには、`<aws-entity-resolution-bd@amazon.com>` の AWS Entity Resolution Business Development チームにお問い合わせください。

OpenAPI 仕様は、コンシューマー識別子のバッチ処理と同期処理の両方について、2 種類の統合をサポートしています。Open API仕様を取得したら、ユースケースの処理統合のタイプを実装します。

トピック

バッチ処理の統合

バッチ処理の統合は、非同期設計パターンに従います。でワークフローが開始されると AWS Data Exchange、プロバイダー統合エンドポイントを介してジョブが送信され、ワークフローはジョブのステータスを定期的にポーリングしてこのジョブの完了を待ちます。このソリューションは、時間がかかり、プロバイダーのスループットが低いジョブ実行に適しています。プロバイダーは、データセットの場所を Amazon S3 リンクとして取り込み、それを処理して、結果をあらかじめ決められた出力 S3 の場所に書き込むことができます。

バッチ処理統合は、3 つのAPI定義を使用して有効 AWS Entity Resolution になります。 は、 を介して利用可能なプロバイダーエンドポイントを次の順序 AWS Data Exchange で呼び出します。

1. `POST CreateJob`: このAPIオペレーションは、処理するジョブ情報をプロバイダーに送信します。これらの情報は、エンコーディングまたはトランスコーディング、S3 ロケーション、顧客が提供するスキーマ、必要なその他のジョブプロパティなど、ジョブのタイプに関するものです。

   これにより APIが返され`JobId`、ジョブのステータスは `PENDING`、、`READY`、、`IN_PROGRESS`または `COMPLETE` のいずれかになります`FAILED`。

   エンコードのサンプルリクエスト

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

レスポンス例

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

2. POST StartJob: これにより、プロバイダーAPIはJobId提供された に基づいてジョブを開始することを知らせます。これにより、プロバイダーは から CreateJobまで必要な検証を実行できますStartJob。

   これによりJobId、、ジョブStatusの 、、statusMessageおよび APIが返されますstatusCode。

   エンコードのサンプルリクエスト

```
POST/jobs/{jobId}
```

```
{
  "customerSpecifiedJobProperties": {
    "property1": "string",
    "property2": "string"
  }
}
```

レスポンス例

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

3. GET GetJob: ジョブが完了した AWS Entity Resolution か、その他のステータスになったかAPIを通知します。

   これによりJobId、、ジョブStatusの 、、statusMessageおよび APIが返されますstatusCode。

   エンコードのサンプルリクエスト

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

   レスポンス例

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

これらに関する完全な定義APIsは、 AWS Entity Resolution 「OpenAPI 仕様」に記載されています。

同期処理の統合

同期処理ソリューションは、スループットが高く が高いリアルタイム応答時間を持つほぼリアルタイムの応答時間を持つプロバイダーにとってより望ましいですTPS。この AWS Entity Resolution ワークフローはデータセットをパーティション化し、複数のAPIリクエストを並行して行います。その後、 AWS Entity Resolution ワークフローは、目的の出力場所に結果を書き込む処理を行います。

このプロセスは、 API 定義の 1 つを使用して有効になります。 は、 から利用可能なプロバイダーエンドポイントを AWS Entity Resolution 呼び出します AWS Data Exchange。

`POST AssignIdentities`: これにより、`source_id`識別子 を使用してプロバイダーにデータAPIが送信され、そのレコード`recordFields`に関連付けられます。

これにより、 APIが返されます`assignedRecords`。

エンコードのサンプルリクエスト

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

レスポンス例

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

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

これらに関する完全な定義APIsは、 AWS Entity Resolution 「OpenAPI 仕様」に記載されています。

プロバイダーが選択したアプローチに応じて、 AWS Entity Resolution はエンコードまたはトランスコードの開始に使用されるプロバイダーの設定を作成します。さらに、これらの設定は、 APIsが提供する を使用してお客様が利用できます AWS Entity Resolution。

この設定には、 のプロバイダーサービスがホスト AWS Data Exchange されている場所から派生した Amazon リソースネーム (ARN) と、プロバイダーサービスのタイプを使用してアクセスできます。 はこれを ARNと AWS Entity Resolution 呼びます`providerServiceARN`。

プロバイダー統合のテスト

はデータマッチングサービスを AWS Entity Resolution ホストしますが、プロバイダー統合は end-to-end マッチングワークフローにとって重要なサードパーティーコンポーネントです。この統合が失敗したときに保護を追加するテスト AWS Entity Resolution がプロバイダーに定義されています。このアプローチは、プロバイダーがこれらの end-to-end テストケースに従ってサービスのヘルスをモニタリングする機会を提供します。

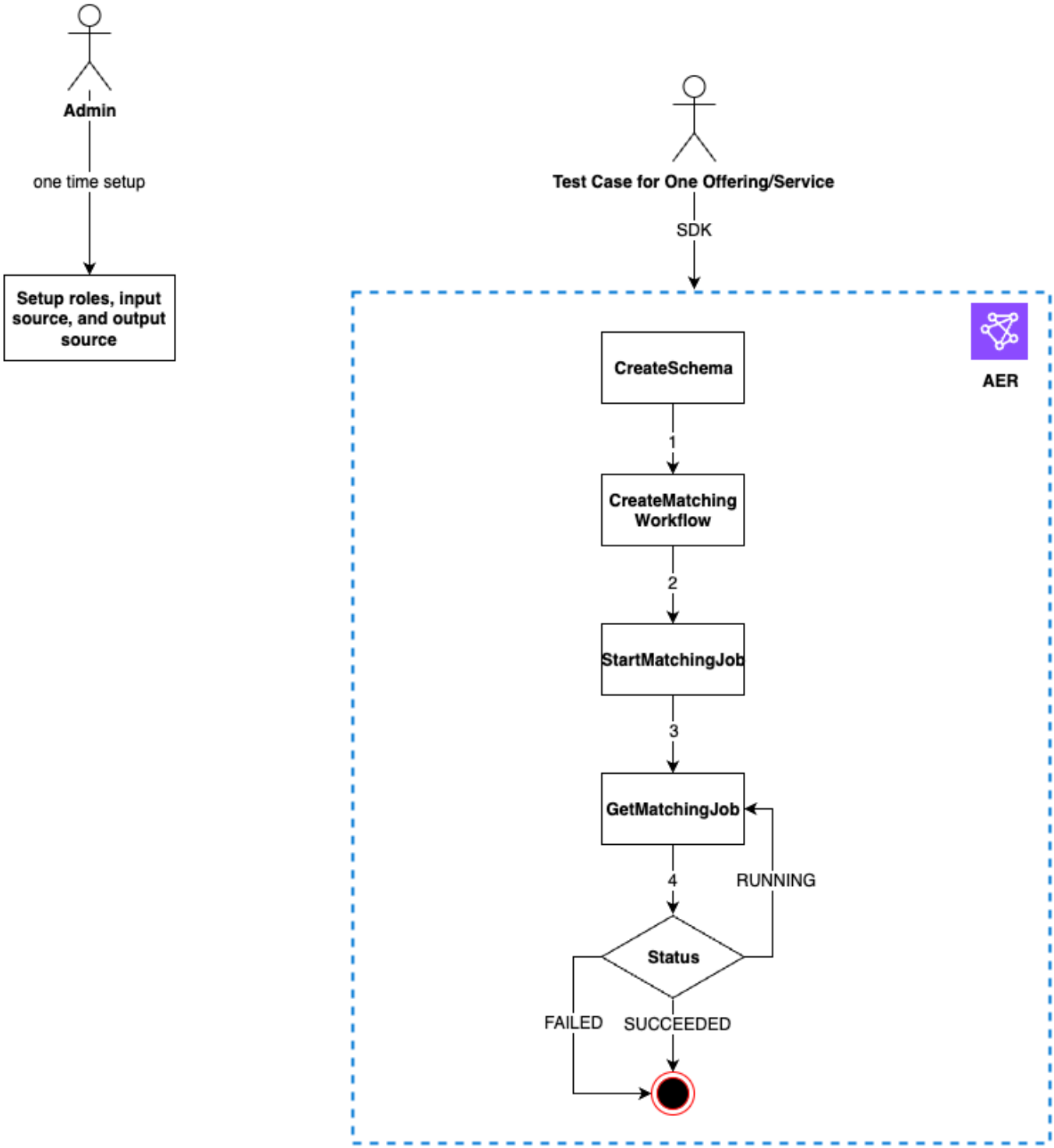
プロバイダーは、テストアカウントと独自のデータを使用して、 AWS Entity Resolution Software Development Kit () を使用してこれらの end-to-end テストケースを実行できますSDK。プロバイダーから問題が発生した場合、 は優先エスカレーションパス AWS Entity Resolution を使用して問題をエスカレーションします。さらに、プロバイダーはテスト結果に独自のモニタリングを実装する必要があります。プロバイダー AWS アカウント IDsは、これらのテストを実行するために使用される と共有する必要があります AWS Entity Resolution。

実行が成功すると、プロバイダーはデータをセットアップし、 を通じて独自のサービスを使用し AWS Entity Resolution、ジョブのステータスはエラーなしで完了を返します。これは、 APIsが提供する を使用してプログラムで実現できます AWS Entity Resolution。

例えば、プロバイダーは、サービスに応じて S3 バケット、入力ソース、ロール、スキーマ、ワークフローを設定できます。これらのセットアップが完了すると、プロバイダーは 200 レコードで 1 日 1 回これらのワークフローを実行してサービスをテストできます。このアプローチでは、プロバイダーは選択した を使用し、 end-to-end テストアカウント AWS Data Exchange を使用して提供されるサービスのテストSDKを実行します。プロバイダーは、サービスごとにこれらのテストを実行することが期待されます。

> **Note**
>
> プロバイダーは AWS Entity Resolution 、テストのためにこれらのワークフローを実行するために使用する AWS アカウント ID (`accountId`)) を指定する必要があります。さらに、プロバイダーはこれらのテストをモニタリングし、合格であることを確認する必要があります。つまり、障害が発生した場合にプロバイダーはそれに応じて問題に対処するための通知を有効にする必要があります。

次の図は、一般的な end-to-end ワークフローテストケースを示しています。



プロバイダー統合をテストするには

1. （ワンタイムセットアップ）AWS Entity Resolution の手順に従って のリソースを設定しますセットアップ AWS Entity Resolution。

1 回限りのセットアップ手順が完了したら、ロール、データ、データソースの準備が整っているはずです。これで、 AWS Entity Resolution コンソールまたは を使用してプロバイダー統合をテストする準備が整いましたAPIs。

2. または コンソールを使用してプロバイダー統合を AWS Entity Resolution APIsテストします。

API

を使用してプロバイダー統合をテストするには AWS Entity Resolution APIs

1. を使用してスキーママッピングを作成しますCreateSchemaMapping API。
サポートされているプログラミング言語の完全なリストについては、「」のhttps://docs.aws.amazon.com/entityresolution/latest/apireference/API_CreateSchemaMapping.html#API_CreateSchemaMapping_SeeAlso「」セクションを参照してくださいCreateSchemaMapping API。

   スキーママッピングは、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。AWS Entity Resolution が一致するワークフローに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を作成するときは、一意の識別子を指定し、AWSEntity Resolution が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。例えば、`Primary_key`、`Row_ID`、`Record_ID` などが挙げられます。

   Example 例

   以下は、 `id`と を含むデータソースのスキーママッピングの例です`email`。

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

Example 例

Java を含むデータソースのスキーママッピングidの例emailを次に示しますSDK。

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

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

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

)
```

2. を使用して一致するワークフローを作成しますCreateMatchingWorkflow API。サポートされているプログラミング言語の完全なリストについては、「」のhttps://docs.aws.amazon.com/entityresolution/latest/apireference/API_CreateMatchingWorkflow.html#API_CreateMatchingWorkflow_SeeAlso「」セクションを参照してくださいCreateMatchingWorkflow API。

   Example 例

   Java を使用したマッチングワークフローの例を次に示しますSDK。

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

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

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

 .resolutionTechniques(ResolutionTechniques.builder()

   .resolutionType(PROVIDER)
```

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

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

一致するワークフローを設定したら、ワークフローを実行できます。

3. を使用して一致するワークフローを実行しますStartMatchingJob API。一致するワークフローを実行するには、CreateMatchingWorkflowエンドポイントを使用して一致するワークフローを作成しておく必要があります。

   サポートされているプログラミング言語の完全なリストについては、「」のhttps://docs.aws.amazon.com/entityresolution/latest/apireference/API_StartMatchingJob.html#API_StartMatchingJob_SeeAlso「」セクションを参照してくださいStartMatchingJob API。

   Example 例

   Java を使用して一致するワークフローを実行する例を次に示しますSDK。

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

4. を使用してワークフローのステータスをモニタリングしますGetMatchingJob API。

これにより、ジョブに関連付けられているステータス、メトリクス、エラー (存在する場合) APIが返されます。

Example 例

以下は、Java を使用して一致するワークフロージョブをモニタリングする例ですSDK。

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

ワークフローが正常に完了すると、 end-to-end テストは完了です。

Console

AWS Entity Resolution コンソールを使用してプロバイダー統合をテストするには

1. 「」の手順に従ってスキーママッピングを作成しますスキーママッピングの作成。

   スキーママッピングは、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を作成するときは、一意の識別子を指定し、 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。例えば、`Primary_key`、`Row_ID`、`Record_ID` などが挙げられます。

   Example 例

   以下は、 `id`と を含むデータソースのスキーママッピングの例です`email`。

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

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

2. 「」の手順に従って、一致するワークフローを作成して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の作成。

   マッチングワークフローの作成は、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セットアップしたプロセスです。プロバイダーベースのワークフローでは、アカウントが を通じてプロバイダーサービスにサブスクリプションを持っている場合 AWS Data Exchange、既知の識別子を任意のプロバイダーと照合できます。エンドツーエンドのテストを実行するために使用しているプロバイダーとサービスに応じて、一致するワークフローを設定できます。

   AWS Entity Resolution コンソールは、作成と実行のアクションを 1 つのボタンで組み合わせます。作成と実行を選択すると、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。

3. ワークフローのステータスは、「ワークフローの一致」ページでモニタリングします。

   ワークフローが正常に完了すると、 end-to-end テストは完了します (ジョブのステータスは完了) 。

   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」で以下を表示できます。

   - 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。
   - IDs 生成された一意の一致。
   - 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。

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 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 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 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
- の耐障害性 AWS Entity Resolution

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 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 FAQ」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」のAWS 「責任共有モデル」とGDPRブログ記事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 () 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IAM。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。1TLS.2 が必要で、1.3 TLS をお勧めします。
- を使用して 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 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 AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、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) 140-3」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、 AWS Entity Resolution 、または を使用して または他の AWS サービス を操作する場合API AWS CLI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。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

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 – デフォルトでは、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 ポリシーと許可の確立と維持
- キーポリシーの有効化と無効化
- キー暗号化マテリアルのローテーション
- 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マッチング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。の権限 AWS KMS は、カスタマーアカウントの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、次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権限が必要です。

- 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 を使用しますAPIs。

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 ステップに従います。

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キーを区別するのに役立つ KeySpec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 の生成と検証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。 KeySpec は SYMMETRIC_DEFAULTで、 は KeyUsageであることを AWS Entity Resolution 検証します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、必要な許可オペレーション 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「Using Grants」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、保存された暗号化データキーを使用して暗号化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

KMS キーを暗号化のデフォルトキーとして設定すると、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と CreateGrantリクエストを AWS KMS に送信します。これには、カスタマーマネージド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、 CreateIdMappingWorkflowおよび をカスタマーマネージドKMSキーでStartIdMappingJobリクエストする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。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。

以下は、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です。

```
{
    "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 を置き換える *<user input placeholder>* 自分の情報を入力します。

<KMSKeyARN>	AWS KMS Amazon リソースネーム。

同様に、 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StartMatchingJobAPI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、 を入力してデータキーを指定できます。これはKMSArn、 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ARNキー識別子であるキー 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、 を入力してデータキーを指定できます。これはKMSArn、 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ARNキー識別子であるキー 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、 AWS KMS 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。

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

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、「AWS Key Management Service デベロッパーガイド」を参照してください。

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 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 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 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ます。詳細については、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」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。次に、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、の基本概念を理解してくださいIAM。会社で を使用する方法の詳細については、IAM AWS Entity Resolution「」を参照してくださいと の AWS Entity Resolution 連携方法 IAM。

IAM 管理者 - IAM管理者は、 へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります AWS Entity Resolution。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IAM、「」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ロールを引き受けることによって認証 (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と、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。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「 へのサインイン AWS アカウント方法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、 はソフトウェア開発キット (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AWS API「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高め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「 ユーザーガイド」の「 での多要素認証 (MFA) AWS IAM 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 およびリソースへの AWS サービス 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「ルートユーザーの認証情報を必要とするタスク」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 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、または ID ソースを通じて提供された認証情報 AWS 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、ロールが引き受けられ、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。Identity Center でユーザーとグループを作成することも、独自の IAM 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、「 ユーザーガイド」のIAM「Identity Center とはAWS IAM Identity Center 」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持つIAMユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする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、「 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でアクセスキーを定期的にローテーションするIAM」を参照してください。

IAM グループは、IAMユーザーのコレクション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、 という名前のグループIAMAdminsを作成し、そのグループにIAMリソースを管理するアクセス許可を付与できます。

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、ロールでは一時認証情報が提供されます。詳細については、「 ユーザーガイド」のIAM「 (ロールの代わりに) ユーザーを作成する場合IAM」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。ユーザーと似ていますがIAM、特定のユーザーに関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、 で 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 オペレーションを AWS CLI 呼び出すか、カスタム を使用しますURL。ロールの使用方法の詳細については、「 ユーザーガイド」のIAM「ロールの使用IAM」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下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ロールの詳細については、「 ユーザーガイド」の「サードパーティー ID プロバイダーのロールの作成IAM」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス許可セットを のロールに関連付けますIAM。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ユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に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、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS 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、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」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 サービス を使用します AWS サービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行 EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。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 サービス、ダウンストリームサービス AWS 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 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権限が必要です。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 – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAMロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS サービスIAM」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 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アクセス許可を表示できますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – 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インスタンス内にアクセスキーを保存するよりも望ましいです。 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 ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM」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、「 ユーザーガイド」の「 (ユーザーではなく) IAMロールを作成する場合IAM」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、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。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) AWS がリクエストを行うと、 はこれらのポリシー 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、「 ユーザーガイド」のJSON「ポリシーの概要IAM」を参照してください。

管理者はポリシーを使用して AWS JSON、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対してどのような条件下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。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用するメソッドに関係なく、アクションのアクセス許可を定義します。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 からロール情報を取得できますAPI。

アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス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、「 ユーザーガイド」のIAM「ポリシーの作成IAM」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。管理ポリシーとインラインポリシーのどちらかを選択する方法については、「 ユーザーガイド」の「管理ポリシーとインラインポリシーの選択」を参照してください。 IAM

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、リソースにアタッチする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の例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。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コントロールできます。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 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IAMでは、 の AWS 管理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 (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs 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を使用しません。

Amazon S3、 AWS WAF、および Amazon VPCは、 をサポートするサービスの例ですACLs。の詳細についてはACLs、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がIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可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 (SCPs) をアカウントの一部またはすべてに適用できます。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SCP を制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」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、「 ユーザーガイド」の「セッションポリシーIAM」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係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、「 ユーザーガイド」の「ポリシー評価ロジックIAM」を参照してください。

と の AWS Entity Resolution 連携方法 IAM

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機能を確認してください AWS Entity Resolution。

IAM で使用できる 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	あり
リソースベースのポリシー	あり
ポリシーアクション	あり
ポリシーリソース	Yes
ポリシー条件キー	あり

IAM 機能	AWS Entity Resolution サポート
ACLs	なし
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	あり
サービスリンクロール	なし

AWS Entity Resolution およびその他の AWS のサービスがほとんどの IAM 機能とどのように連携するかの概要を把握するには、IAM「 ユーザーガイド」のAWS 「 と連携する のサービスIAM」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のポリシーのサポート: あり

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできる JSONアクセス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、「 ユーザーガイド」のIAM「ポリシーの作成IAM」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、許可または拒否されたアクションとリソース、およびアクションが許可または拒否され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、「 ユーザーガイド」の「 IAMJSONポリシー要素のリファレンスIAM」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、リソースにアタッチする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の例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。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コントロールできます。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 サービス。

クロスアカウントアクセスを有効にするには、リソースベースのポリシーのプリンシパルとして、アカウント全体または別のアカウントのIAMエンティティを指定できます。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、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」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のサポート: あり

管理者はポリシーを使用して AWS JSON、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対してどのような条件下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`要素は、ポリシーで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を記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションを持たないアクセス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

ポリシーリソースのサポート: あり

管理者はポリシーを使用して AWS JSON、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対してどのような条件下でアクションを実行できるかということです。

Policy ResourceJSON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 のリストを確認するにはARNs、「サービス認証リファレンス」の「 で定義されるリソース AWS Entity Resolution」を参照してください。各リソース

ARNの を指定できるアクションについては、「 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。

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: あり

管理者はポリシーを使用して AWS JSON、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、どのリソースに対してどのような条件下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 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では 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、ユーザー名でタグ付けされている場合にのみ、リソースにアクセスするアクセス許可をIAMユーザーに付与できますIAM。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグIAM」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、「 ユーザーガイド」のAWS 「 グローバル条件コンテキストキーIAM」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 の AWS Entity Resolution

をサポートACLs： いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs 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を使用しません。

ABAC と AWS Entity Resolution

サポート ABAC (ポリシー内のタグ): 部分的

属性ベースのアクセスコントロール (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、の最初のステップですABAC。次に、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する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が煩雑になる状況に役立ちます。

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ありです。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。

の詳細についてはABAC、「 IAMユーザーガイド」の「 とはABAC」を参照してください。のセットアップ手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用するIAM」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: あり

一部の は、一時的な認証情報を使用してサインインすると機能 AWS サービス しません。一時的な認証情報 AWS サービス を使用する などの詳細については、「 ユーザーガイドAWS サービス 」の「 と連携IAMする IAM 」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、会社のシングルサインオン (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。ロールの切り替えの詳細については、「 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 を使用して手動で作成できます AWS API。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、「」の「一時的なセキュリティ認証情報IAM」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をサポート (FAS): 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 サービス、ダウンストリームサービス AWS 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 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権限が必要です。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

サービスロールのサポート: あり

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

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 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アクセス許可を表示できますが、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、「 AWS と連携する のサービスIAM」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 を使用してタスクを実行することはできません AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

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

ARNs 各リソースタイプの 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。

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、「 ユーザーガイド」の「 AWS 管理ポリシー」または「 ジョブ機能の 管理ポリシーIAM」を参照してください。 AWS
- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス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 を使用してアクセス許可を適用する方法の詳細については、「 ユーザーガイド」の「 のポリシーとアクセス許可IAMIAM」を参照してください。
- IAM ポリシーの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、アクションと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 を使用して送信する必要があることを指定できますSSL。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 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、「 ユーザーガイド」のIAMJSON「ポリシー要素: 条件IAM」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、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、「 ユーザーガイド」のIAM「Access Analyzer ポリシーの検証IAM」を参照してください。
- 多要素認証を要求する (MFA) – 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MFAするために をオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、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「 で保護されたAPIアクセスの設定」を参照してください。

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「 のセキュリティのベストプラクティスIAMIAM」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 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 AWS API。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を許可します。

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、「 ユーザーガイド」の「ユーザーへのアクセス許可の追加IAM」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、IAMユーザーがユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または 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 AWS API。

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

```
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 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 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 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
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、 および 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IAM。

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

からアクションを実行する権限がないと AWS Management Console 通知された場合は、管理者に連絡してサポートを依頼する必要があります。担当の管理者はお客様のユーザー名とパスワードを発行した人です。

次の例のエラーは、mateojacksonIAMユーザーが コンソールを使用して架空の*my-example-widget*リソースの詳細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* リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

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 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。

次の例のエラーは、 というIAMユーザーがコンソールを使用して marymajor でアクションを実行しようする場合に発生します AWS Entity Resolution。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 (ACLs) をサポートするサービスでは、これらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

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 の AWS Entity Resolution 連携方法 IAM。
- 所有している のリソースへのアクセスを提供する方法については、 AWS アカウント 「 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IAM」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通じ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、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

のコンプライアンス検証 AWS Entity Resolution

AWS 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 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 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。 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HIPAAのセキュリティとコンプライアンスのためのアーキテクチャ – 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**
>
> すべての AWS サービス がHIPAA対象となるわけではありません。詳細については、HIPAA「対象サービスリファレンス」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 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) など) 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 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 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DSS、 PCI 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 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 コンプライアンスのベストプラクティス

このセクションでは、 を使用する際のコンプライアンスに関するベストプラクティスと推奨事項について説明します AWS Entity Resolution。

Payment Card Industry Data Security Standards (PCI DSS)

AWS Entity Resolution は、マーチャントまたはサービスプロバイダーによるクレジットカードデータの処理、保存、および送信をサポートし、Payment Card Industry (PCI) Data Security Standard () に準拠していることが確認されていますDSS。コンプライアンスパッケージのコピーを AWS PCIリクエストする方法などPCIDSS、 の詳細については、PCIDSS「レベル 1」を参照してください。

システムと組織のコントロール (SOC)

AWS Entity Resolution は、1、SOC2、3 SOC を含むシステムおよび組織コントロール (SOC) SOC の対策に準拠しています。SOC レポートは、 が AWS 主要なコンプライアンスコントロールと目標を達成した方法を示す、独立したサードパーティーによる審査レポートです。これらの監査によって、お客様のデータや企業データのセキュリティ、機密保持、アベイラビリティーに影響を及ぼす可能性のあるリスクから守るために、適切な安全策と手順を講じます。これらのサードパーティー監査の結果は、AWS SOCコンプライアンスウェブサイト で確認できます。このウェブサイトでは、公開されたレポートを表示して、 AWS オペレーションとコンプライアンスをサポートするコントロールに関する詳細情報を取得できます。

の耐障害性 AWS Entity Resolution

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。物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供し、低レイテンシー、高スループット、高冗長ネットワークで接続されます。アベイラビリティーゾーンでは、ゾーン間で中断することなく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することができます。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 および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。

グローバル AWS インフラストラクチャに加えて、 AWS Entity Resolution では、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、いくつか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。

を使用してAWSエンティティ解決リソースを作成する 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 1 回記述し、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して設定するには、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または でフォーマットされたテキストファイルですYAML。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 に慣れていない場合はYAML、 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 エンティティ解決では、 AWS::EntityResolution::PolicyStatement での AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace と の作成がサポートされています AWS CloudFormation。および の テンプレートJSON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 AWS::EntityResolution::PolicyStatement」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 」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 AWS Entity Resolution APIリファレンスの
- 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 AWS Entity Resolution APIリファレンスの
- 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 AWS Entity Resolution APIリファレンスの
- 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 AWS Entity Resolution APIリファレンスの
- 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 AWS Entity Resolution APIリファレンスの

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 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フィードをサブスクライブできます。RSS更新をサブスクライブするには、使用しているブラウザで RSSプラグインが有効になっている必要があります。

変更	説明	日付
プロバイダーの統合	ドキュメントのみの更新。お客様は、プロバイダーサービスとして と統合する方法を学習できます AWS Entity Resolution。	2024 年 8 月 8 日
ID マッピングワークフロー – 更新	お客様は、一致するルールを使用して、ID マッピングワークフローでファーストパーティーデータを変換できるようになりました。	2024 年 7 月 23 日
マッチングワークフロー – 更新	お客様は、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`	2024 年 4 月 2 日

	`AWS::EntityResolution::PolicyStatement` および および は次のリソースを更新しました: `AWS::EntityResolution::IdMappingWorkflow` 。	
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 と関連するルールを見つけることができるようになりました。	2024 年 3 月 25 日
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PIIベースのマッチングワークフローで 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呼び出しなど、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。

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たときに自動的に で実行できるようにします。

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**、 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 ビット (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 マッピング方法

ID マッピングの実行方法。

ID マッピングには 2 つの方法があります。

- ルールベース – 一致するルールを使用して、ID マッピングワークフローでソースからターゲットにファーストパーティデータを変換する方法。

- プロバイダーサービス — プロバイダーサービスを使用して、ID マッピングワークフローでサードパーティーでエンコードされたデータをソースからターゲットに変換する方法。

  AWS Entity Resolution は現在、プロバイダーのサービスベースの ID マッピング方法 LiveRamp として をサポートしています。この方法 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、「ステップ 1: 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 マッピングワークフロー

指定された ID マッピング方法に基づいて、入力データソースから入力データターゲットにデータをマッピングするデータ処理ジョブ。ID マッピングテーブルを生成します。このワークフローでは、ID マッピング方法と、ソースからターゲットに変換する入力データを指定する必要があります。

ID マッピングワークフローは、独自の または 2 つの AWS アカウント で実行するように設定できます AWS アカウント。

ID 名前空間

複数の AWS アカウント にまた AWS Entity Resolution が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 ユーザーガイドをご参照ください。

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 AWS Entity Resolution 、提示するデータの種類を指示し、適切に分類および正規化できるようにします。

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 のいずれかの組み合わせhome_phoneが一致した場合、「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 OR Record One mobile_phone = Record Two home_phone OR 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、両方の一致キーを「Phone」にすることができます。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 (「ワークフローの一致」セクションの「1 対 1 のマッチングと多対多のマッチングの定義」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、特定の一致基準を満たすことに基づいて (例えば、一致するルールやモデルを通じて) 、どちらが類似しているか、または「一致する」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、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

- TRIM = 先頭と末尾の空白を切り捨てる
- 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隠す
- REMOVE_ALLNON_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切り捨てる
- 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隠す
- REMOVE_ALLNON_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_ALLNON_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切り捨てる
- 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隠す
- REMOVE_ALLNON_ALPHA = 英数字以外の文字をすべて削除します [a-zA-Z]
- RENAME__WORDSADDRESSRENAMEWORD_= を使用してMAPアドレス文字列の単語を ADDRESS_RENAME_ の単語に置き換えWORDるMAP
- RENAME__DELIMITERS_ を使用した ADDRESSRENAMEDELIMITER_MAP = Address 文字列の区切り文字を ADDRESS_RENAME_ の文字列に置き換えDELIMITERるMAP
- RENAME__DIRECTIONSRENAMEDIRECTION_= を使用した ADDRESS_MAP は、アドレス文字列の区切り文字を ADDRESS_RENAME_ の文字列に置き換えDIRECTIONますMAP
- RENAME__NUMBERS_ を使用した ADDRESSRENAMENUMBER_MAP = アドレス文字列の数値を ADDRESS_RENAME_ の文字列に置き換えNUMBERますMAP
- RENAME_SPECIAL__CHARS_ を使用する ADDRESSRENAME_SPECIALCHAR_MAP = アドレス文字列の特殊文字を ADDRESS_RENAME_SPECIAL_ の文字列に置き換えCHARますMAP

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切り捨てる

Source_ID

- TRIM = 先頭と末尾の空白を切り捨てる

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_phoneAND。 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 の送信先。

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、比較データを一致として宣言し、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記述。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、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。

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。
- が 38 文字を超えている (ルールベースのマッチングワークフローのみ)

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。