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を照合、リンク、強化するの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。ストア全体で異なるコード (SKU、UPC など) を使用する製品をより適切に追跡することもできます。を使用すると AWS Entity Resolution 、データの移動を最小限に抑えながら、マッチングの精度を制御し、データセキュリティをより適切に保護できます。

トピック

- を初めて AWS Entity Resolution お使いになる方向けの情報
- 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

を初めて AWS Entity Resolution お使いになる方向けの情報

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。 は、暗号化されたデータセットで操作 AWS Entity Resolution 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。デフォルトでは、 はマッチング前にデータ入力 AWS Entity Resolution を正規化して、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、マッチング処理を改善します。データ入力がすでに正規化されている場合は、正規化をオフにできます。また、GitHub ライブラリも用意されています。これを使用して、ニーズに合わせてデータの正規化プロセスをさらにカスタマイズできます。

- 設定可能なエンティティマッチングワークフロー

  エンティティマッチングワークフローは、データ入力の照合 AWS Entity Resolution 方法と統合データ出力の書き込み場所を に指示するようにセットアップする一連のステップです。1 つ以上のマッチングワークフローを設定して、異なるデータ入力を比較し、エンティティ解決や ML エクスペリエンスなしで、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のマッチングなど、さまざまなマッチング手法を使用できます。リソース番号、処理されたレコード数、見つかった一致の数など、既存の一致ワークフローとメトリクスのジョブステータスを表示することもできます。

  - Ready-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 () ready-to-use一連のルールが含まれますAWS CLI。 AWS Management Console 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、ルールを削除し、ルールの優先度を再配置して、新しいルールを作成することで、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 生成するマッチ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、各一致グループの関連する信頼スコアが 0.0 ~ 1.0 の場合で、一致の精度を示します。

- データサービスプロバイダーとのレコードの照合

  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、到達、サービスを提供する能力を拡張できます。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使用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使用できるため、複雑な独自の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持つ統合データ出力テーブルに、データ入力を変換できます。API および AWS Management Console または を使用すると AWS CLI、既存の抽出、変換、ロード (ETL) データパイプラインに基づいて、オンデマンドで手動一括処理を実行できます。ETL データパイプラインは、新しいマッチングと既存のマッチングの更新のためにすべてのデータを再処理します。また、ルールベースのマッチングシナリオでは、自動増分処理を開始して、Amazon S3 バケットで新しいデータが利用可能になるとすぐに、サービスはそれらの新しいレコードを読み取り、既存のレコードと比較できます。これにより、Amazon S3 データの変更と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 オペレーションを使用してエンティティフィールドを検索すると、既存の一致 ID を同期的に取得できます。さまざまなソースやチャネルを通じて取得

し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それらの属性を 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、および郵送先住所で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ている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) システム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見つけることができます。

- データ保護と設計によるリージョン化

  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、サービスへのデータ入力ごとに暗号化キーを提供します。たとえば、 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。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することもできます。

- マルチパーティートランスコーディング

  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一致する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 のサービス 、 に関連しています AWS Entity Resolution。

- Amazon S3

  に取り込んだデータを Amazon S3 AWS Entity Resolution に保存します。

  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 ログ AWS Entity Resolution で を使用して、アクティビティの分析 AWS のサービス を強化します。

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

- AWS CloudFormation

  次のリソースを作成します AWS CloudFormation。AWS::EntityResolution::MatchingWorkflow、AWS::EntityResolution::SchemaMapping、および 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。

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

の料金 AWS Entity Resolution

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

セットアップ AWS Entity Resolution

AWS Entity Resolution を初めて使用する場合は、 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

がすでにある場合は 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/signup を開きます。
2. オンラインの手順に従います。

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

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

管理者ユーザーの作成

管理者ユーザーを作成するには、以下のいずれかのオプションを選択します。

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

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

ロールを使用して短期認証情報を作成できます。これはセキュリティを強化するために推奨されます。[ユーザー] を選択して長期間の認証情報を作成することもできます。

3. [ロールの作成] を選択します。
4. ロールの作成ウィザードで、信頼されたエンティティタイプで を選択しますAWS アカウント。
5. このアカウントを選択したまま、次へを選択します。
6. アクセス許可を追加する で、ポリシーの作成 を選択します。

   新しいタブが開きます。

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

      - AWS マネージドポリシー: 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、「アクセス許可の追加」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には、コンソールを使用してこのロールを作成できます。アクセスCreateRole許可がない場合は、管理者にロールの作成を依頼してください。

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

1. 管理者アカウントを使用して、https://console.aws.amazon.com/iam/ 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、セキュリティを強化するために推奨される短期認証情報を作成できます。[ユーザー] を選択して長期間の認証情報を作成することもできます。
3. [ロールの作成] を選択します。
4. [ロールの作成] ウィザードの [信頼されたエンティティタイプ] で [カスタム信頼ポリシー] を選択します。
5. 次のカスタム信頼ポリシーをコピーして JSON エディタに貼り付けます。

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

6. [次へ] をクリックします。
7. アクセス許可を追加する 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 に存在する必要があります AWS Entity Resolution。
> データソースが暗号化または復号されていない場合は、アクセス AWS KMS 許可を付与する必要はありません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{input-buckets}}",
                "arn:aws:s3:::{{input-buckets}}/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "{{accountId}}"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::{{output-bucket}}",
                "arn:aws:s3:::{{output-bucket}}/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "{{accountId}}"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:GetSchema",
                "glue:GetSchemaVersion",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:{{aws-region}}:{{accountId}}:database/{{input-
databases}}",
                "arn:aws:glue:{{aws-region}}:{{accountId}}:table/{{input-
database}}/{{input-tables}}",
                "arn:aws:glue:{{aws-region}}:{{accountId}}:catalog"
            ]
        }
    ]
}
```

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

aws-region	AWS リージョン of your resources. Your AWS Glue resources, underlying Amazon S3 resources and AWS KMS resources must be in the same AWS リージョン as `AWS Entity Resolution` .

accountId	Your AWS アカウント ID.
######	Amazon S3 buckets which contains the underlying data objects of AWS Glue where `AWS Entity Resolution` will read from.
######	Amazon S3 buckets where `AWS Entity Resolution` will generate the output data.
########	AWS Glue databases where `AWS Entity Resolution` will read from.

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

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

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

aws-region	AWS リージョン of your resources. Your AWS Glue resources, underlying Amazon S3 resources and AWS KMS resources must be in the same AWS リージョン as `AWS Entity Resolution` .
accountId	Your AWS アカウント ID.

inputKeys	Managed keys in AWS Key Managemen t Service. If your input sources are encrypted, AWS Entity Resolution must decrypt your data using your key.

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

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

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

aws-region	AWS リージョン of your resources. Your AWS Glue resources, underlying Amazon S3 resources and AWS KMS resources must be in the same AWS リージョン as AWS Entity Resolution .
accountId	Your AWS アカウント ID.
outputKeys	Managed keys in AWS Key Management Service. If you need your output sources to be encrypted, AWS Entity Resolutio n must encrypt the output data using your key.

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

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

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

aws-region	The AWS リージョン where the provider resource is granted. You can find this value in the asset ARN on the AWS Data Exchange console. For example: `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
datasetId	The ID of the dataset, found on the AWS Data Exchange console.
revisionId	The revision of the dataset, found on the AWS Data Exchange console.
assetId	The ID of the asset, found on the AWS Data Exchange console.

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entityresolutionに を必ず含めてください。

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ています。これらのレコードには、名、姓、E メールアドレス、電話番号などのコンシューマー識別子が含まれます。これらのソースレコードは、同じまたは他の入力データテーブル内で指定した他のソースレコードと照合できます。各レコードには一意のレコード ID (一意の ID) が必要です。また、スキーママッピングの作成時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か、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。

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 が AWS Entity Resolution 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)

- 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 および AWS リージョン の Amazon Simple Storage Service (Amazon S3) に保存する必要があります。

入力データテーブルを Amazon S3 にアップロードするには

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

   フォルダを選択して、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

> **Note**
>
> パーティション AWS Glue テーブルが必要な場合は、「」に進みますステップ 4: パーティション分割された 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、「 AWS Glue デベロッパーガイド」の「コンソールでのクローラの使用AWS Glue 」を参照してください。

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し、 AWS Glue AWS Glue テーブルを作成するクローラを 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、 AWS Glue コンソールを https://console.aws.amazon.com/glue/:://www.com で開きます。
2. ナビゲーションバーから、[クローラ] を選択します。
3. リストから S3 バケットを選択し、クローラの作成を選択します。
4. クローラプロパティの設定ページで、クローラ名オプションの説明を入力し、次へを選択します。
5. 引き続き [クローラを追加] ページで、詳細を指定します。
6. [IAM ロールの選択] ページで [既存の IAM ロールを選択] を選択し [次へ] 選択します。

   [IAM ロールを作成する] を選択することも、必要に応じて管理者に IAM ロールを作成してもらうこともできます。
7. [このクローラのスケジュールを設定する] で、[頻度] をデフォルト ([オンデマンドで実行]) のままにして、[次へ] を選択します。
8. クローラの出力を設定する 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、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。

ステップ 4: パーティション分割された AWS Glue テーブルを作成する

> **Note**
>
> の AWS Glue パーティショニング機能は AWS Entity Resolution 、ID マッピングワークフローでのみサポートされています。この AWS Glue パーティショニング機能を使用すると、で処理する特定のパーティションを選択できます AWS Entity Resolution。
> パーティション AWS Glue テーブルが必要ない場合は、このステップをスキップできます。

パーティション分割された AWS Glue テーブルは、データ構造に新しいフォルダ (1 か月未満の新しい日フォルダなど) を追加すると、 AWS Glue テーブル内の新しいパーティションを自動的に反映します。

でパーティション分割された AWS Glue テーブルを作成するときに AWS Entity Resolution、ID マッピングワークフローで処理するパーティションを指定できます。次に、ID マッピングワークフローを実行するたびに、 AWS Glue テーブル全体のすべてのデータを処理するのではなく、それらのパーティションのデータのみが処理されます。この機能を使用すると、 でより正確で効率的で費用対効果の高いデータ処理が可能になり AWS Entity Resolution、エンティティ解決タスクをより細かく制御し、柔軟に管理できます。

ID マッピングワークフローでソースアカウントのパーティション AWS Glue テーブルを作成できます。

まず、 で Amazon S3 の入力データをカタログ AWS Glue 化し、テーブルとして AWS Glue 表現する必要があります。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、「 AWS Glue デベロッパーガイド」の「コンソールでのクローラの使用AWS Glue 」を参照してください。

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、パーティション分割された AWS Glue テーブルを作成するクローラを 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。

パーティション分割された AWS Glue テーブルを作成するには

1. にサインイン AWS Management Console し、 AWS Glue コンソールを https://console.aws.amazon.com/glue/://www.com で開きます。
2. ナビゲーションバーから、[クローラ] を選択します。
3. リストから S3 バケットを選択し、クローラの作成を選択します。
4. クローラのプロパティの設定ページで、クローラ名、オプションの 説明を入力し、次へ を選択します。
5. 引き続き [クローラを追加] ページで、詳細を指定します。
6. [IAM ロールの選択] ページで [既存の IAM ロールを選択] を選択し [次へ] 選択します。

   [IAM ロールを作成する] を選択することも、必要に応じて管理者に IAM ロールを作成してもらうこともできます。
7. [このクローラのスケジュールを設定する] で、[頻度] をデフォルト ([オンデマンドで実行]) のままにして、[次へ] を選択します。
8. クローラの出力を設定する 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、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のテーブルで、パーティション化するテーブルを選択します。
13. テーブルの概要で、アクションドロップダウンを選択し、テーブルの編集を選択します。

    a. テーブルプロパティで、追加 を選択します。

    b. 新しいキーには、「」と入力します**aerPushDownPredicateString**。

    c. 新しい値には、「」と入力します**'<PartitionKey>=<PartitionValue'**。

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

これで次の作業に進むことができます。

- スキーママッピングを作成し、1 つの の ID マッピングワークフローを作成します AWS アカウント。

- ID 名前空間ソースを作成し、ID 名前空間ターゲットを作成し、2 つの にまたがる ID マッピングワークフローを作成します AWS アカウント。

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 ID 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でサブスクリプションをお持ちの場合は AWS Data Exchange、次のいずれかのプロバイダーサービスで一致するワークフローを実行して、既知の識別子を優先プロバイダーと一致させることができます。データは、優先プロバイダーによって定義された一連の入力と照合されます。

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. プロバイダーのリストを表示します AWS Data Exchange。次のプロバイダーリストを利用できます。

   - LiveRamp
     - LiveRamp ID の解決
     - LiveRamp のトランスコーディング
   - TransUnion
     - TransUnion TruAudience 転送レスアイデンティティ解決とエンリッチメント
     - TransUnion TruAudience 転送レスアイデンティティ解決
   - 統合 ID 2.0
     - 統合 ID 2.0 ID 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、プライベートオファーを受け入れます AWS Data Exchange。
   - 独自のサブスクリプションを使用する – プロバイダーで既存のデータサブスクリプションを既にお持ちの場合は、 AWS Data Exchange ユーザーガイドの Bring Your Own Subscription (BYOS) オファー手順に従って BYOS オファーを受け入れます 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。

APIsAWS Data Exchange 「 ユーザーガイド」の「 API 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の推奨事項とガイドラインのセットがあります。

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。

データプロバイダーサービスのガイドライン

プロバイダーサービス	一意の ID が必要ですか？	アクション
LiveRamp	はい	以下を確認してください。 • 一意の ID は、独自の仮名識別子または行 ID のいずれかです。 • データ入力ファイルの形式と正規化は、LiveRamp ガイドラインに沿っています。 一致するワークフローの入力ファイルフォーマットガイドラインの詳細については、LiveRamp ドキュメントの「ADX による ID 解決の実行」を参照してください。 ID マッピングワークフローの入力ファイルフォーマットガイドラインの詳細については、LiveRamp ドキュメントの「ADX によるトランスコーディングの実行」を参照してください。
TransUnion	はい	以下を確認してください。 • TransUnion Data Enrichment には一意の ID が存在します。 Note パススルー属性は、TransUnion への入力と出力に保持できます。世帯

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

		E キーと HHID はクライアント名前空間に固有です。
		• **Phone number** は 10 桁で、スペースやハイフンなどの特殊文字は使用できません。
		• **Addresses** を に分割する必要があります
		  • 1 つのアドレス行 (存在する場合は、1 行と 2 行の組み合わせ)
		  • 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 で指定
		• **Email addresses** はプレーンテキストである必要があります。
		• **First Name** は小文字でも大文字でもかまいませんが、ニックネームはサポートされていますが、タイトルとサフィックスは除外する必要があります。
		• **Last Name** 小文字または大文字、ミドルネームを除外できます。

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	はい	以下を確認してください。 • 一意の ID をハッシュにすることはできません。 • UID2 は、UID2 生成用の E メールと電話番号の両方をサポートしています。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内の各レコードを複製します。1 つのレコードは UID2 生成用の E メールを使用し、2 番目のレコードは電話番号を使用します。データに E メールと電話番号が混在していて、出力にこのレコードの重複が必要ない場合は、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、任意の時点で同じ raw UID2 値になります。 Raw UID2sは、1 年に 1 回程度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、それに伴って 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年間を通じて異なる時間にローテーションされます。 AWS Entity

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
		Resolution は現在、ソルトバケットと未加工UID2s のローテーションを追跡していないため、未加工の UID2s 毎日再生成することをお勧めします。詳細については、UID2s「増分更新のために UID2 を更新する頻度」を参照してください。

ステップ 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 が AWS Entity Resolution 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 および AWS リージョン の Amazon Simple Storage Service (Amazon S3) に保存する必要があります。

入力データテーブルを Amazon S3 にアップロードするには

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

   フォルダを選択して、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、「 AWS Glue デベロッパーガイド」の「コンソールでのクローラの使用AWS Glue 」を参照してください。

> **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し、 AWS Glue AWS Glue テーブルを作成するクローラを 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、 AWS Glue コンソールを https://console.aws.amazon.com/glue/:://www.com で開きます。
2. ナビゲーションバーから、[クローラ] を選択します。
3. リストから S3 バケットを選択し、[クローラを追加] を選択します。
4. [クローラを追加] ページで [クローラの名前] を入力し、[次へ] を選択します。
5. 引き続き [クローラを追加] ページで、詳細を指定します。
6. [IAM ロールの選択] ページで [既存の IAM ロールを選択] を選択し [次へ] 選択します。

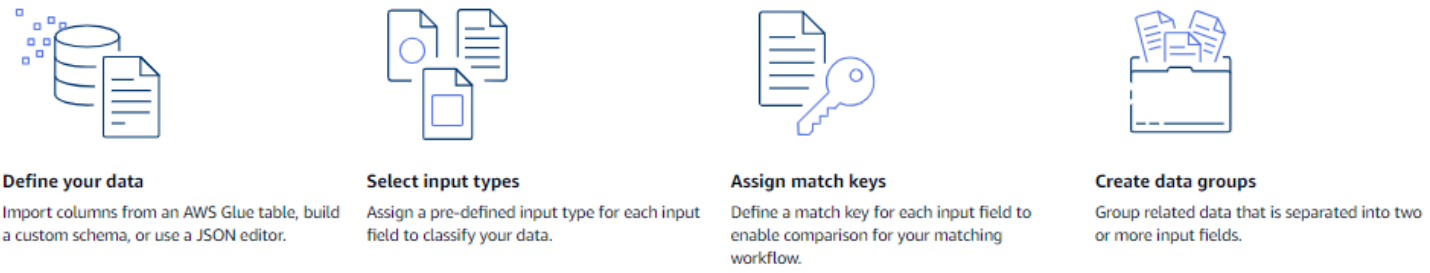
   [IAM ロールを作成する] を選択することも、必要に応じて管理者に IAM ロールを作成してもらうこともできます。
7. [このクローラのスケジュールを設定する] で、[頻度] をデフォルト ([オンデマンドで実行]) のままにして、[次へ] を選択します。
8. クローラの出力を設定する で、 AWS Glue データベースを入力し、次へ を選択します。
9. 詳細を確認し、[完了] を選択します。
10. [クローラ] ページで、S3 バケットの横にあるチェックボックスをオンにし、[クローラの実行] を選択します。
11. クローラの実行が完了したら、 AWS Glue ナビゲーションバ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

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、サンプルを使用する、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 AWS アカウント、 でAWS Entity Resolution コンソールを開きます。まだ開いていない場合は、 を開きます。
2. 左側のナビゲーションペインのデータ準備で、スキーママッピングを選択します。
3. スキーママッピングページの右上隅で、スキーママッピングの作成を選択します。
4. ステップ 1: スキーマの詳細を指定するには、次の手順を実行します。

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

   b. 作成方法 で、 からインポート AWS Glueを選択します。

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

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

d. 一意の ID には、データの各行を個別に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、単一のテーブル内の一意の識別子である必要があります。ただし、異なるテーブル間で、一意の ID に重複する値が含まれる場合があります。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列とオプションのパススルーに使用する列を選択します。

マッチングとパススルーの両方について、合計で最大 34 列を選択できます。

i. 「一致」で、一致の入力フィールドとして使用する列を選択します。

マッチングには最大 24 列を選択できます。

ii. マッチングに使用されない列を指定する場合は、パススルーする列の追加を選択します。

iii. (オプション) パススルーで、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. 一致させる入力フィールドについては、各入力フィールドについて、

- 属性タイプを指定してデータを分類します。

- 一致キー名を指定して、入力フィールドを一致するワークフローと比較できるようにします。特定の一致キー名は、デフォルトで特定の属性タイプに自動的に関連付けられます。
- その入力フィールドの列値がハッシュされている場合は Hashed チェックボックスを選択し、値がクリアテキストの場合は空白のままにします。

> **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。
>
> - プロバイダー ID の属性タイプを LiveRamp ID として指定します。
> - 名前フィールドの属性タイプを複数のフィールド (名、姓など) または 1 つのフィールドで指定します。
> - 住所フィールドの属性タイプを複数のフィールド (住所 1、住所 2、 など) または 1 つのフィールド (住所全体) に指定します。
>
> アドレスと照合する場合は、郵便番号 (郵便番号) が必要です。
> - 名前に E メール (E メールアドレス) または電話番号 (電話番号) 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、データセットには次の属性タイプが少なくとも 1 つ含まれている必要があります。
>
> - フルネーム
> - 完全な住所
> - フルフォン
> - [E メールアドレス]
> - 一致キー名が生年月日の日付

これらの属性の属性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、名前、住所、電話番号の入力フィールドを複数のフィールドに区切ってグループ化します。

このステップでは、関連する入力フィールドを 1 つのフィールドに連結します。これにより、一致するワークフローで 1 つのフィールドとして比較できます。

名前、住所、または電話番号の入力フィールドにデータがマッピングされていない場合、このセクションは空白になります。

より多くのタイプのデータがある場合は、さらにグループを追加することもできます。

a. 名前入力データをグループ化する場合：

フルネームで、グループ化する入力フィールドを 2 つ以上選択します。

グループ名と一致キーは、データ型に自動的に関連付けられます。

グループ名を更新でき、カスタム一致キーには、文字、数字、アンダースコア (_)、ハイフン (-) など、最大 255 文字を含めることができます。

グループの追加 を選択して、別のグループを追加します。

> **Note**
>
> 正規化はフルネームでのみサポートされます。
> フルネームサブタイプを正規化する場合は、フルネームグループに名、ミドルネーム、姓のサブタイプを割り当てます。

b. Address 入力データをグループ化する場合：

フルアドレス で、グループ化する入力フィールドを 2 つ以上選択します。

グループ名と一致キー。 は自動的にデータ型に関連付けられます。

グループ名を更新でき、カスタム一致キーには、文字、数字、アンダースコア (_)、ハイフン (-) など、最大 255 文字を含めることができます。

グループの追加を選択して、別のグループを追加します。

> **Note**
>
> 正規化はフルアドレスでのみサポートされます。
> 完全なアドレスサブタイプを正規化する場合は、完全なアドレスグループに次のサブタイプを割り当てます。住所 1、住所 2: 住所 3 の名前、市区町村名、州、国、郵便番号。

c. 電話入力データをグループ化する場合：

フルフォンで、グループ化する入力フィールドを 2 つ以上選択します。

グループ名と一致キー。 は自動的にデータ型に関連付けられます。

グループ名を更新でき、カスタム一致キーには、文字、数字、アンダースコア (_)、ハイフン (-) など、最大 255 文字を含めることができます。

グループの追加を選択して、別のグループを追加します。

> **Note**
>
> 正規化はフルフォンでのみサポートされています。
> 完全な電話サブタイプを正規化する場合は、完全な電話グループに電話番号と電話の国コードのサブタイプを割り当てます。

d. [Next (次へ)] を選択します。

7. ステップ 4: 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、 でAWS Entity Resolution コンソールを開きます。まだ開いていない場合は、 を開きます。
2. 左側のナビゲーションペインのデータ準備で、スキーママッピングを選択します。
3. スキーママッピングページの右上隅で、スキーママッピングの作成を選択します。
4. ステップ 1: スキーマの詳細を指定するには、次の手順を実行します。
   a. 名前と作成方法には、スキーママッピング名とオプションの 説明を入力します。
   b. 作成方法 で、カスタムスキーマの構築 を選択します。
   c. 一意の ID には、一意の ID を入力してデータの各行を識別します。

      Example

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

> **Note**
>
> 一意の ID 列は必須です。一意の ID は、単一のテーブル内の一意の識別子である必要があります。ただし、異なるテーブル間で、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。

   マッチングとパススルーの両方に最大 34 列を定義できます。

   a. 一致させる入力フィールドには、入力フィールドに入力します。

   b. 属性タイプを選択してデータを分類します。

> **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、providerID 属性タイプを 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、属性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、データセットには次の属性タイプが少なくとも 1 つ含まれている必要があります。
>
> - フルネーム
> - 完全な住所
> - フルフォン
> - [E メールアドレス]
> - 一致キー名が生年月日の日付
>
> これらの属性の属性タイプをカスタム文字列として指定しないでください。

   c. 一致キー名を選択して、入力フィールドを一致するワークフローと比較できるようにします。

特定の一致キー名は、デフォルトで特定の属性タイプに自動的に関連付けられます。

d. その入力フィールドの列値がハッシュされている場合はハッシュされたチェックボックスをオンにし、値がクリアテキストの場合は空白のままにします。

e. 入力フィールドを追加 を選択して、さらに入力フィールドを追加します。

マッチングには最大 24 個の入力フィールドを追加できます。

f. (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。

g. [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、名前、住所、電話番号の入力フィールドを複数のフィールドに区切ってグループ化します。

このステップでは、関連する入力フィールドを 1 つのフィールドに連結します。これにより、一致するワークフローで 1 つのフィールドとして比較できます。

名前、住所、電話番号の入力フィールドにデータがマッピングされていない場合、このセクションは空白になります。

より多くのタイプのデータがある場合は、さらにグループを追加することもできます。

a. 名前入力データをグループ化する場合：

フルネームで、グループ化する入力フィールドを 2 つ以上選択します。

グループ名と一致キーは、データ型に自動的に関連付けられます。

グループ名を更新でき、カスタム一致キーで一致キーには、文字、数字、アンダースコア (_)、ハイフン (-) など、最大 255 文字を含めることができます。

グループの追加を選択して、別のグループを追加します。

> **Note**
>
> 正規化はフルネームでのみサポートされます。
> フルネームサブタイプを正規化する場合は、フルネームグループに名、ミドルネーム、姓のサブタイプを割り当てます。

b. Address 入力データをグループ化する場合：

フルアドレス で、グループ化する入力フィールドを 2 つ以上選択します。

グループ名と一致キー。 は自動的にデータ型に関連付けられます。

グループ名を更新でき、カスタム一致キーで一致キーには、文字、数字、アンダースコア (_)、ハイフン (-) など、最大 255 文字を含めることができます。

グループを追加 を選択して、別のグループを追加します。

> **Note**
>
> 正規化はフルアドレスでのみサポートされます。
> 完全なアドレスサブタイプを正規化する場合は、完全なアドレスグループに次のサブタイプを割り当てます。住所 1、住所 2: 住所 3 の名前、市区町村名、州、国、郵便番号。

c. 電話入力データをグループ化する場合：

フルフォンで、グループ化する入力フィールドを 2 つ以上選択します。

グループ名と一致キー。 は自動的にデータ型に関連付けられます。

グループ名を更新できます。カスタム一致キーには、文字、数字、アンダースコア (_)、ハイフン (-) など、最大 255 文字を含めることができます。

グループの追加 を選択して、別のグループを追加します。

> **Note**
>
> 正規化はフルフォンでのみサポートされています。
> 完全な電話サブタイプを正規化する場合は、完全な電話グループに電話番号と電話の国コードのサブタイプを割り当てます。

d. [Next (次へ)] を選択します。

7. ステップ 4: 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。

Use 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 AWS アカウント、 でAWS Entity Resolution コンソールを開きます。
2. 左側のナビゲーションペインのデータ準備で、スキーママッピングを選択します。
3. スキーママッピングページの右上隅で、スキーママッピングの作成を選択します。
4. ステップ 1: スキーマの詳細を指定するには、次の手順を実行します。
   a. 名前と作成方法には、スキーママッピング名とオプションの 説明を入力します。
   b. 作成方法 で、JSON エディタを使用する を選択します。
   c. （オプション) リソースのタグを有効にする場合は、新しいタグを追加を選択し、キーと値のペアを入力します。
   d. [Next (次へ)] を選択します。
5. ステップ 2: マッピングを指定するには：
   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	推奨されるオプション
スキーママッピングの構築を開始する	サンプル JSON を挿入し、必要に応じて情報を編集します。
既存の JSON ファイルを使用する	ファイルからインポート

> **Note**
>
> 正規化は、、、NAME、ADDRESS、 PHONEの各タイプでのみサポートされますEMAIL_ADRESS。
> NAME サブタイプを正規化する場合は、NAMEgroupName に次のサブタイプを割り当てます: NAME_FIRST、NAME_MIDDLE、および NAME_LAST
> ADDRESS サブタイプを正規化する場合は、ADDRESSgroupName に次のサブタイプを割り当てます:
> ADDRESS_STREET1、ADDRESS_STREET2、ADDRESS_STREET3、ADDRESS_CITY、ADD
> PHONE サブタイプを正規化する場合は、PHONEgroupName に次のサブタイプを割り当てます: PHONE_NUMBERおよび PHONE_COUNTRYCODE。

b. [Next (次へ)] を選択します。

6. ステップ 3: 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**
>
> 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。

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 AWS アカウント、 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. スキーマの詳細の指定ページで、必要な変更を加え、次へを選択します。
6. 一致する手法の選択ページで、必要な変更を加え、次へを選択します。
7. マップ入力フィールドページで、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、 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. スキーマの詳細の指定ページで、必要な変更を加え、次へを選択します。
6. 一致する手法の選択ページで、必要な変更を加え、次へを選択します。
7. マップ入力フィールドページで、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。

> **Note**
>
> 正規化は、フルネーム、フルアドレス、フルフォン、E メールアドレスでのみサポートされます。
> フルネームサブタイプを正規化する場合は、フルネームグループに名、ミドルネーム、姓のサブタイプを割り当てます。
> 完全なアドレスサブタイプを正規化する場合は、完全なアドレスグループに次のサブタイプを割り当てます。住所 1、住所 2: 住所 3 の名前、市区町村名、州、国、郵便番号。
> 完全な電話サブタイプを正規化する場合は、完全な電話グループに電話番号と電話の国コードのサブタイプを割り当てます。

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、 でAWS Entity Resolution コンソールを開きます。まだ開いていない場合は、 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

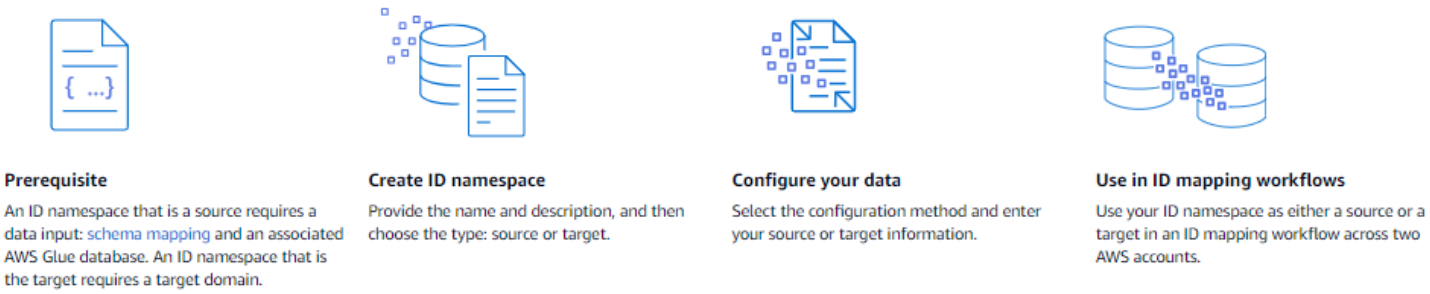
ID 名前空間は、入力データテーブルのラッパーです。ID 名前空間を使用して、入力データとマッチング手法、および ID マッピングワークフローでそれらを使用する方法を説明するメタデータを提供します。

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 が AWS Entity Resolution 処理するソースデータの設定が含まれています。
- ターゲットには、すべてのソースが解決するターゲットデータの設定が含まれています。

ID マッピングワークフロー AWS アカウント 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ともに使用できます。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と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。このメソッドは、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します。

> **Note**
>
> 入力データがソースの場合、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、 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。
既存の一致ワークフロー	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: AWS アカウント自分または別の AWS アカウント。 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 ARN を入力します。

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	推奨されるオプション
ソースとターゲットの両方からルールを許可する	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する	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するが、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. 比較パラメータと一致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	推奨されるオプション
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かかわらず、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	推奨されるオプション
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の、単一の入力フィールド内の制限比較。	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、レコード一致タイプを指定します。

目標	推奨されるオプション
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、レコード一致タイプを制限して、ターゲット内の一致するレコードごとに、一致するレコードを 1 つだけソースに保存します。	レコードマッチングの制限 and 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するレコードごとに、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 and 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するが、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。この方法では、LiveRamp というプロバイダーサービスを使用します。LiveRamp は、ID マッピングワークフロー中に、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します。

> **Note**
>
> 入力データがソースの場合、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 (プロバイダーサービス) を作成するには

1. にサインイン AWS Management Console し AWS アカウント、 でAWS Entity Resolution コンソールを開きます。まだ開いていない場合は、 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。LiveRamp のサブスクリプションをお持ちの場合、ステータスは Subscribed と表示されます。LiveRamp をサブスクライブする方法の詳細につい

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。

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。
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。

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がない場合、[既存のサービスロールを使用] オプションは使用できません。 2. [IAM で表示] 外部リンク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。

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整いました。

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 名前空間ソースとともに使用できます。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と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 AWS アカウント、 でAWS Entity Resolution コンソールを開きます。まだ開いていない場合は、 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、ルールベースを選択します。
6. データ入力の場合、一致ワークフロー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: AWS アカウント自分または別の AWS アカウント。
   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 ARN を入力します。
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	推奨されるオプション
ソースとターゲットの両方からルールを許可する	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する	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するが、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. 比較パラメータとマッチング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	推奨されるオプション
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かかわらず、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
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の、単一の入力フィールド内の制限比較。	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	推奨されるオプション
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、レコード一致タイプを制限して、タ	レコードマッチングの制限 and

目標	推奨されるオプション
ーゲット内の一致するレコードごとに、一致するレコードを 1 つだけソースに保存します。	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するレコードごとに、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 and 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するが、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、LiveRamp というプロバイダーサービスを使用します。LiveRamp は、ID マッピングワークフロー中に、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、 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。
> LiveRamp のサブスクリプションをお持ちの場合、ステータスは Subscribed と表示されます。
> LiveRamp をサブスクライブする方法の詳細については、「」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。

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

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、 でAWS Entity Resolution コンソールを開きます。まだ開いていない場合は、 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

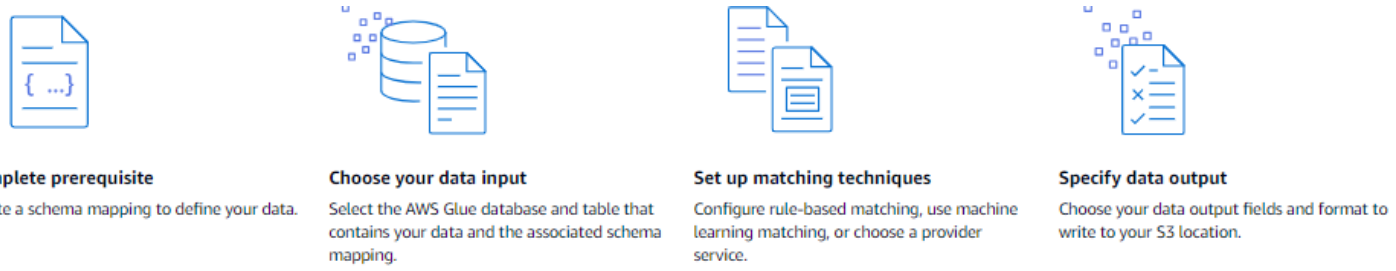
マッチングワークフローは、さまざまな入力ソースのデータを組み合わせて比較し、さまざまなマッチング手法に基づいて一致するワークフローを決定するデータ処理ジョブです。これにより、データ出力テーブルが生成されます。

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、次に必要な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 Match 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) は名前jobIdとして を持つフォルダに書き込まれます。

データ出力には、マッチングが成功するための ファイルとエラーのための 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、機械学習ベース、プロバイダーサービスベースの 3 つの方法があります。

一致するワークフローを作成して実行したら、次の操作を実行できます。

- 指定した S3 の場所の結果を表示します。一致するワークフローはIDs を生成します。
- ビジネスニーズを満たすために、プロバイダーのサービスベースのマッチング、またはその逆の入力として、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使用します。 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

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。次に、一致しないレコードのサブセットをプロバイダーのサービスベースのマッチングに送信できます。

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、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、 によって提案され AWS Entity Resolution、入力したデータに基づいて完全に設定可能です。ルール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。

は、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、以下を割り当てます。

- 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。

      > **Note**
      >
      > 正規化は、スキーママッピングの作成で以下のシナリオでのみサポートされます。
      >
      > - 名前サブタイプがグループ化されている場合: 名、ミドルネーム、姓。
      > - 住所サブタイプがグループ化されている場合: 住所 1、住所 2、住所 3、市区町村、州、国、郵便番号。
      > - 電話番号、電話番号の国コードの電話番号サブタイプがグループ化されている場合。

   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。

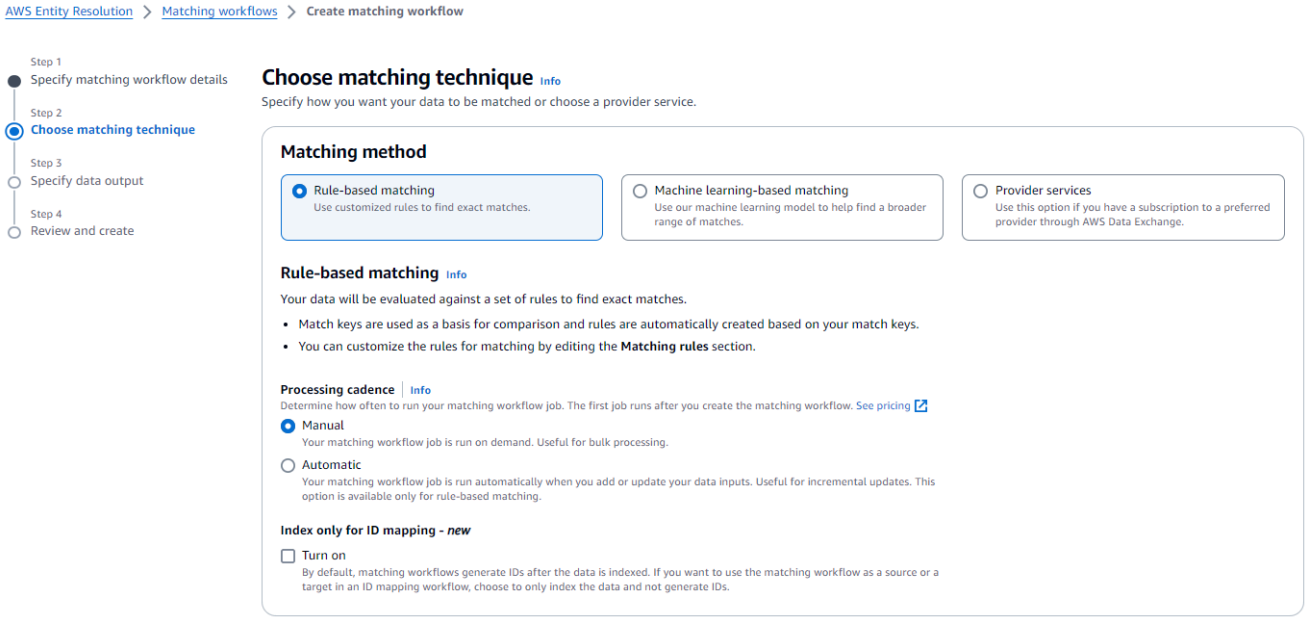
オプション	推奨されるアクション
	• ロールを作成してポリシーをアタッチするアクセス許可が必要です。 • 入力データが暗号化されている場合は、「このデータは KMS キーオプションで暗号化されます」を選択します。次に、データ入力の復号に使用される AWS KMS キーを入力します。
既存のサービスロールを使用	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. [IAM で表示] 外部リンク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。



b. Processing cadence 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	推奨されるオプション
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

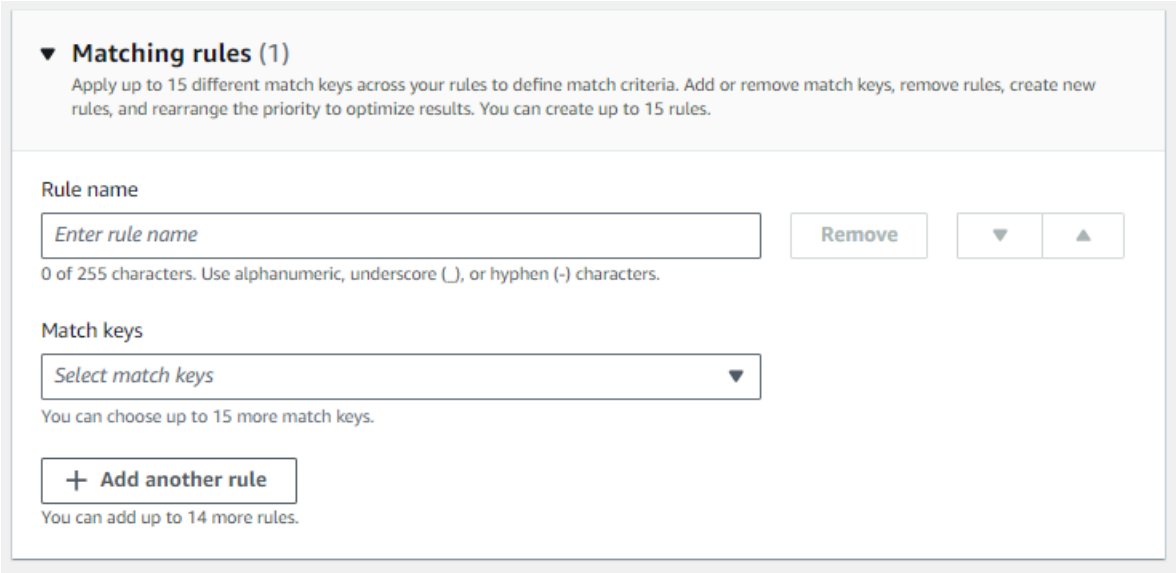
> **Note**
>
> 自動 を選択した場合は、S3 バケットに対して Amazon EventBridge 通知が有効になっていることを確認します。S3 コンソールを使用して Amazon EventBridge を有効にする手順については、「Amazon S3 ユーザーガイド」の「Amazon EventBridge の有効化」を参照してください。 Amazon S3

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作成のみを有効にし、IDsを生成しないように選択できます。

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後に IDs を生成します。

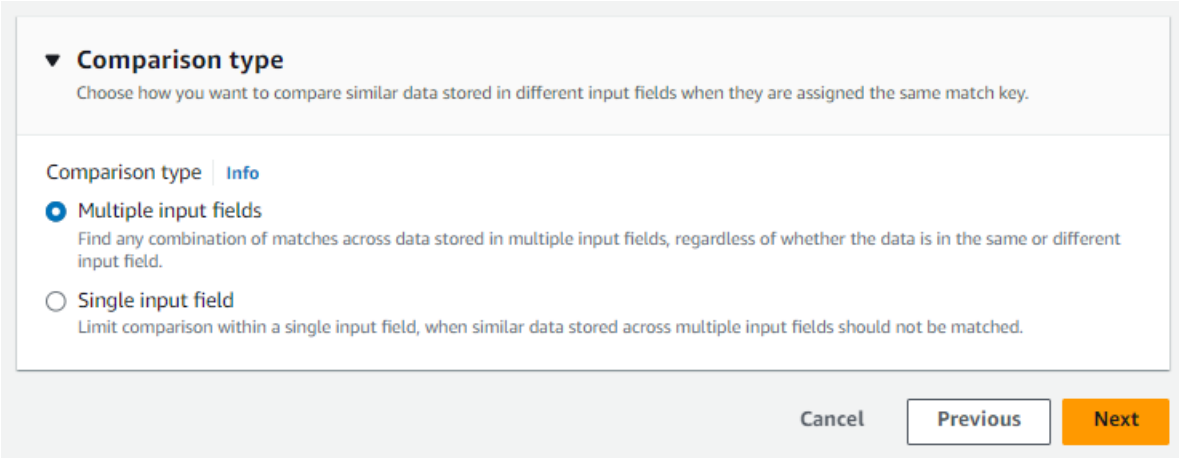
d. 一致ルールには、ルール名を入力し、そのルールの一致キーを選択します。

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、一致条件を定義できます。



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	推奨されるオプション
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



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には：

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

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

   c. システム生成の出力を表示します。

   d. データ出力では、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。

目標	推奨されるオプション
フィールドを含める	出力状態を 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、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: 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。
- 生成された一意の一致 IDs。
- 入力レコードの数。

ジョブ履歴で以前に実行された一致する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. 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。
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。

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にわたってレコードのマッチングを試みるプリセットプロセスです。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、ハッシュされたデータの比較をサポートしていません。

は、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、以下を割り当てます。

- 一致したデータセット内のレコードへの一致 ID
- 一致信頼度レベルのパーセンテージ。

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、まず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、追加の一致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、次の手順を実行します。

    a. 一致するワークフロー名とオプションの 説明を入力します。

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

    最大 20 個のデータ入力を追加できます。

    c. データ正規化オプション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。

    機械学習ベースのマッチングでは名前、、電話、および のみが正規化されますE メール。

    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。

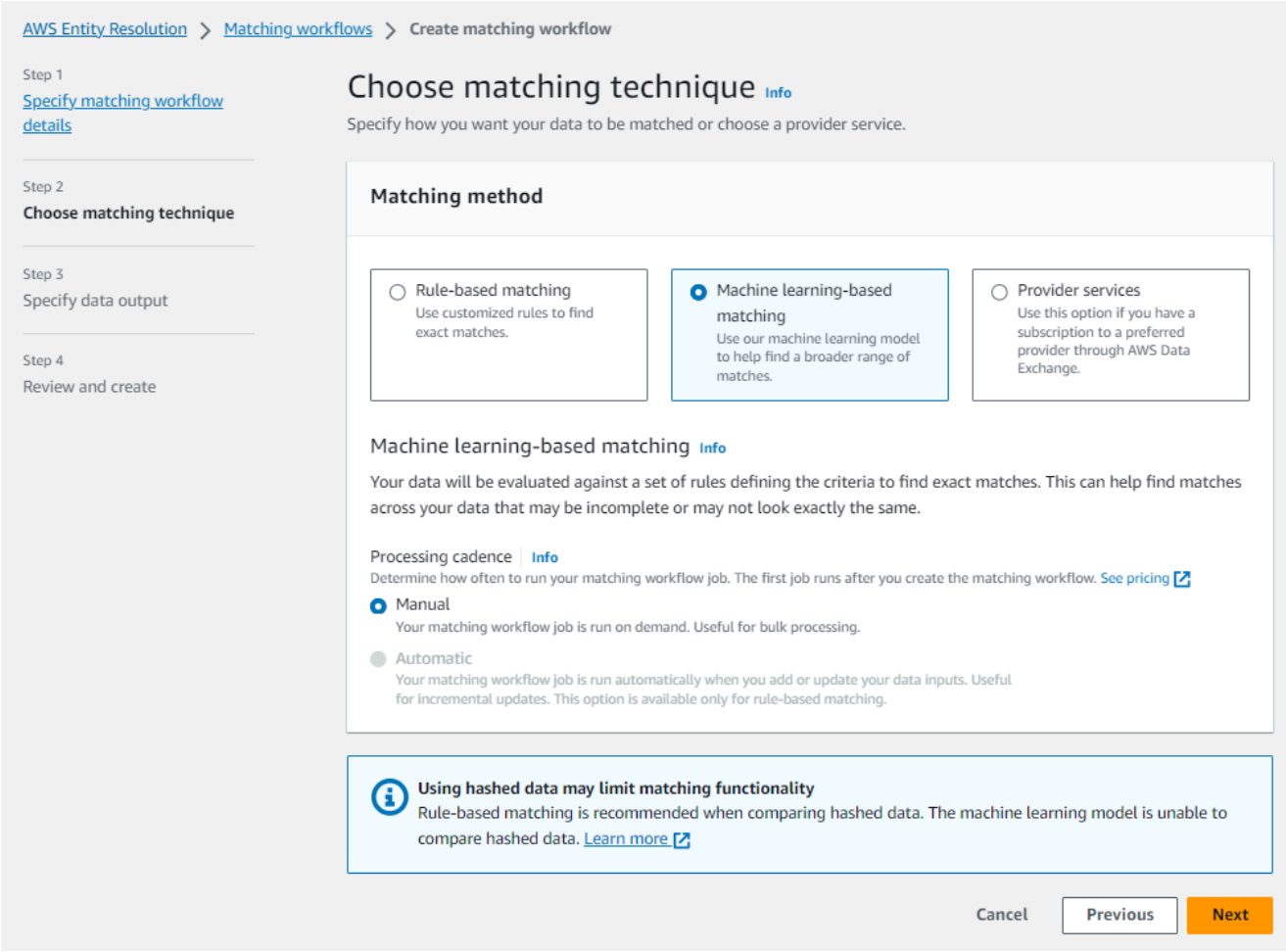
オプション	推奨されるアクション
	• デフォルトの [サービスロール名] は `entityresolution-matching-workflow-<timestamp>` です。 • ロールを作成してポリシーをアタッチするアクセス許可が必要です。 • 入力データが暗号化されている場合は、「このデータは KMS キーオプションで暗号化されます」を選択します。次に、データ入力の復号に使用される AWS KMS キーを入力します。
既存のサービスロールを使用	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. [IAM で表示] 外部リンク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。



b. 処理ケイデンスでは、手動オプションが選択されます。

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には：

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

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

c. システム生成の出力を表示します。

d. データ出力では、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。

目標	推奨されるオプション
フィールドを含める	出力状態を 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、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: 確認して作成する :

a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

b. Create and run を選択します。

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

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

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

ジョブ履歴で以前に実行された一致する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. 一致するワークフロージョブが完了したら (ステータスが完了) 、データ出力タブに移動し、Amazon S3 の場所を選択して結果を表示できます。
10. (手動処理タイプのみ) 手動処理タイプを使用して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を実行を選択して、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を使用すると、既知の識別子を任意のデータサービスプロバイダーと照合できます。

AWS Entity Resolution は現在、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。

で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使用する AWS Data Exchange か、データプロバイダーと直接プライベートオファーを交渉できます。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

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

LiveRamp サービスのサブスクリプションをお持ちの場合は、LiveRamp サービスを使用して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。

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対象者を作成するために需要側のプラットフォームで最も一般的に使用される IDs の 1 つです。LiveRamp で一致するワークフローを使用すると、ハッシュされた E メールアドレスを RAMPIDs に解決できます。

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

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。LiveRamp で ID マッピングワークフローを作成する前に、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 *<user input placeholder>* を独自の情報に置き換えます。

##########	Amazon S3 bucket that temporarily stores your data while running a provider service-based workflow.

LiveRamp 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、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 テーブルを選択してから、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。

> **Note**
>
> 正規化は、スキーママッピングの作成で以下のシナリオでのみサポートされます。
>
> - 名前サブタイプがグループ化されている場合: 名、ミドルネーム、姓。
> - 住所サブタイプがグループ化されている場合: 住所 1、住所 2: 住所 3 名、市区町村名、州、国、郵便番号。
> - 電話番号、電話番号の国コードの電話番号サブタイプがグループ化されている場合。

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 キーで暗号化されます」オプションを選択します。次に、データ入力の復号に使用される AWS KMS キーを入力します。

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. [IAM で表示] 外部リンク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 :

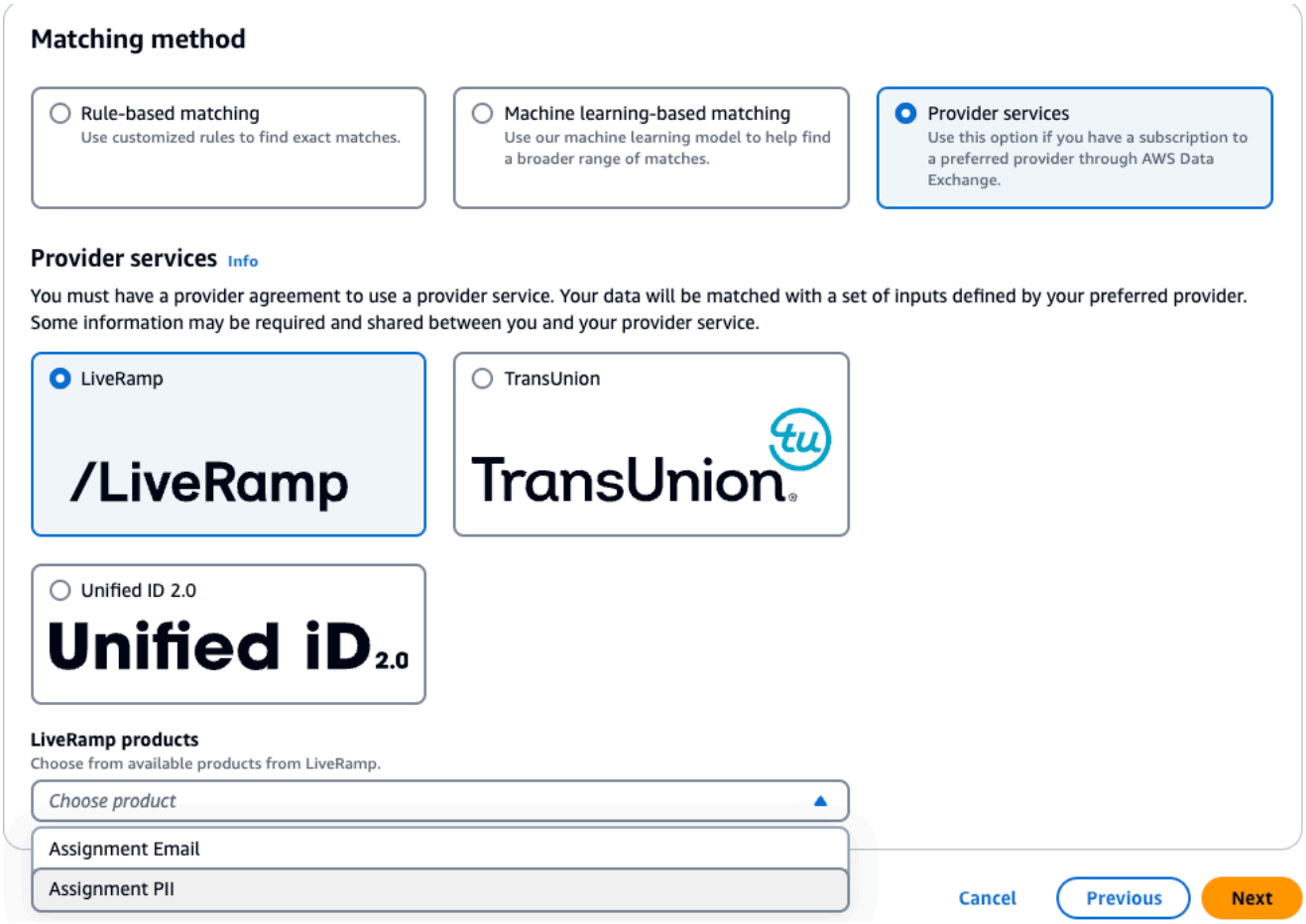
a. マッチング方法 で、プロバイダーサービス を選択します。

b. プロバイダーサービスで、LiveRamp を選択します。

> **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に沿っていることを確認します。

マッチングワークフローの入力ファイルフォーマットガイドラインの詳細については、LiveRamp ドキュメントの「ADX によるアイデンティティ解決の実行」を参照してください。

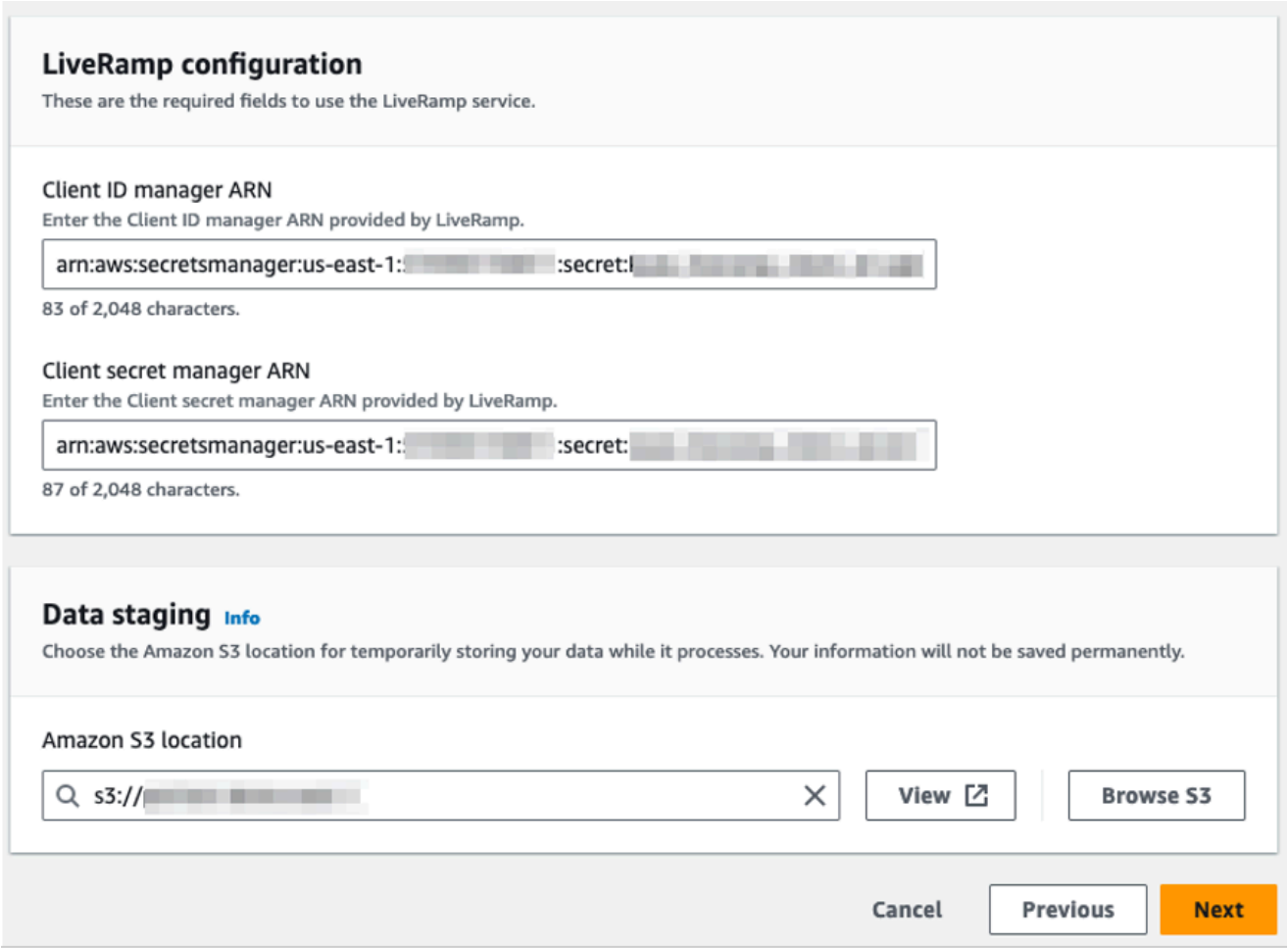
c. LiveRamp 製品の場合は、ドロップダウンリストから製品を選択します。



Note

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

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



e. データのステージングでは、処理中のデータの一時ストレージの 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へのアクセス許可が必要です。詳細については、「のワークフロージョブロールの作成 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: データ出力を指定するには：

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

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

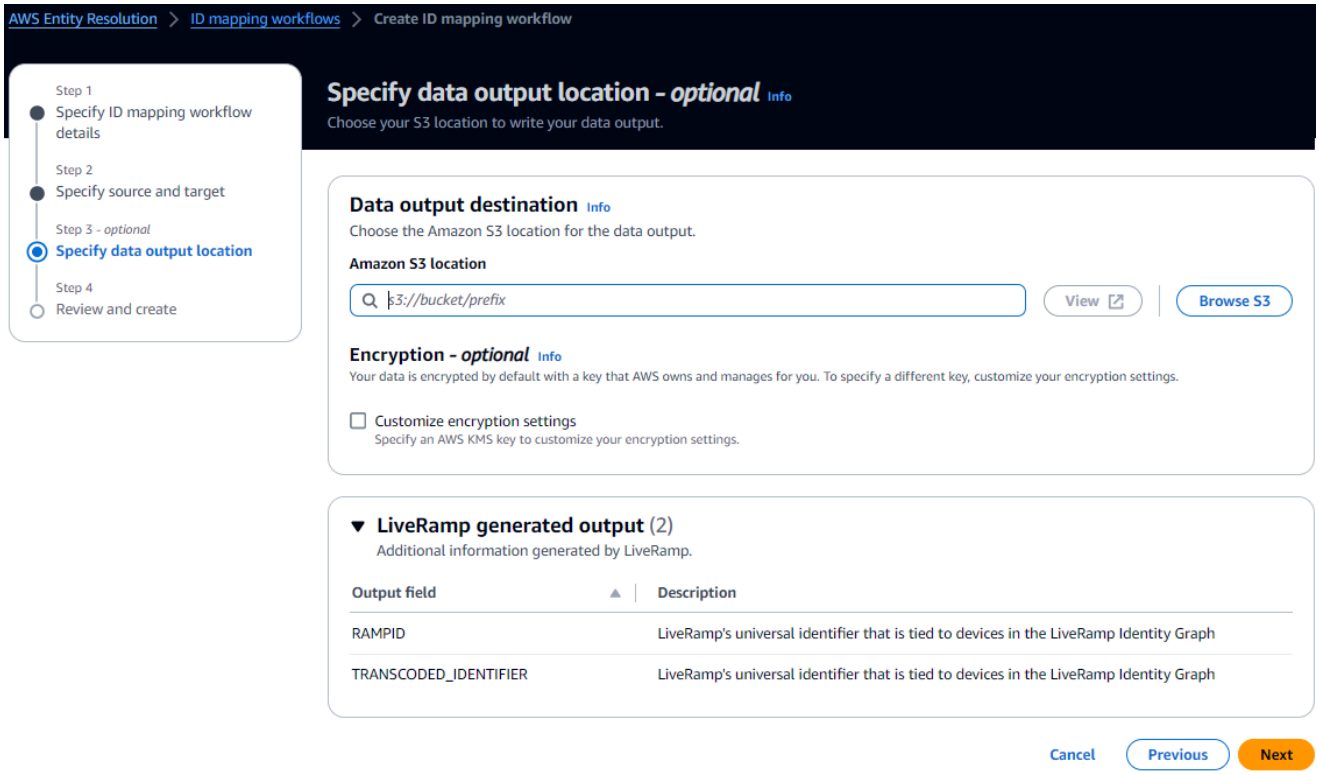
c. LiveRamp が生成した出力を表示します。

これは LiveRamp によって生成された追加情報です。

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

目標	推奨されるオプション
フィールドを含める	出力状態を 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、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: 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」の下に以下を表示します。

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

ジョブ履歴で以前に実行された一致する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. 一致するワークフロージョブが完了したら (ステータスが完了) 、データ出力タブに移動し、Amazon S3 の場所を選択して結果を表示できます。

TransUnion を使用したマッチングワークフローの作成

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

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

このワークフローには、一致するワークフロー出力を一時的に書き込む Amazon S3 データステージングバケットが必要です。TransUnion で一致するワークフローを作成する前に、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 *<user input placeholder>* を独自の情報に置き換えます。

##########	Amazon S3 bucket that temporarily stores your data while running a provider service-based workflow.

TransUnion 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、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 テーブルを選択してから、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はデフォルトで選択されているため、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。

> **Note**
>
> 正規化は、スキーママッピングの作成で以下のシナリオでのみサポートされます。
>
> - 名前サブタイプがグループ化されている場合: 名、ミドルネーム、姓。
> - 住所サブタイプがグループ化されている場合: 住所 1、住所 2: 住所 3 名、市区町村名、州、国、郵便番号。
> - 電話番号、電話番号の国コードの電話番号サブタイプがグループ化されている場合。

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

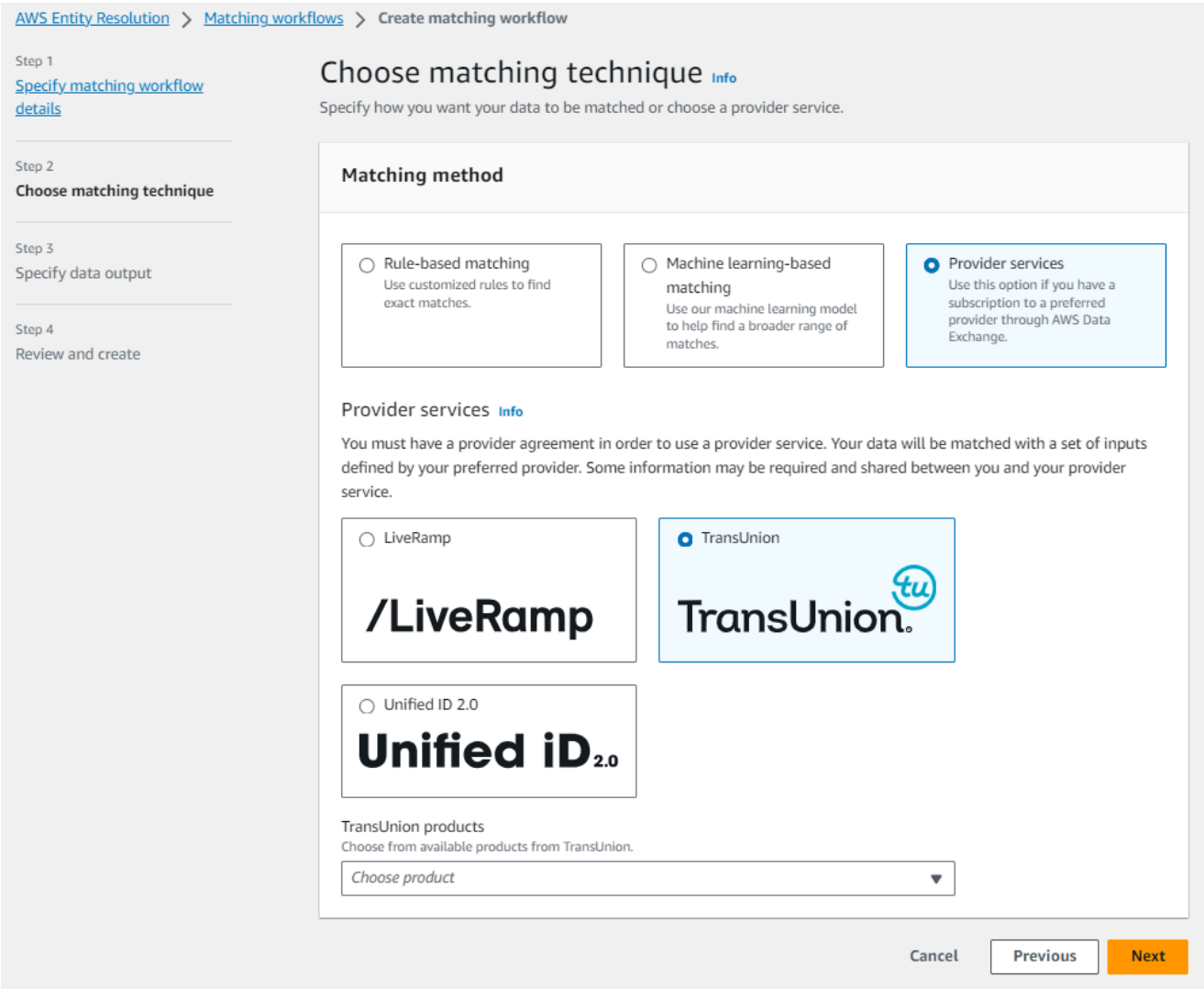
5. ステップ 2: 一致する手法を選択する :

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、TransUnion を選択します。

> **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に沿っていることを確認します。

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



d. データステージングでは、処理中のデータの一時ストレージの 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への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: データ出力を指定するには：

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

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

c. TransUnion が生成した出力を表示します。

これは、TransUnion によって生成される追加情報です。

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。

目標	推奨されるオプション
フィールドを含める	出力状態を 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、非表示を選択します。
マスクフィールド	出力フィールドを選択し、ハッシュ出力を選択します。
以前の設定をリセットする	[リセット] を選択します。

e. システム生成出力では、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: 確認して作成する :

a. 前のステップで行った選択内容を確認し、必要に応じて編集します。

b. Create and run を選択します。

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

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

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

ジョブ履歴で以前に実行された一致する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。

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

UID 2.0 を使用したマッチングワークフローの作成

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

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

1 つのワークフローでは、未加工の UID2 生成**Phone number**に **Email Address**または のいずれかを使用できますが、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、それに伴って raw UID2 もローテーションされます。したがって、未加工の UID2sを毎日更新することをお勧めします。詳細については、https://unifiedid.com/docs/getting-started/gs-faqs#how-often-should-uid2s-be-refreshed-for-incremental-updates を参照してください。

UID 2.0 で一致するワークフローを作成するには：

1. にサインイン AWS Management Console し、 で AWS Entity Resolution コンソールを開きます AWS アカウント （ まだ開いていない場合 ）。
2. 左側のナビゲーションペインのワークフローで、一致を選択します。

3. 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 テーブルを選択してから、対応するスキーママッピングを選択します。

      最大 20 個のデータ入力を追加できます。

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

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

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

   d. 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	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。

オプション	推奨されるアクション
	ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. [IAM で表示] 外部リンク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。

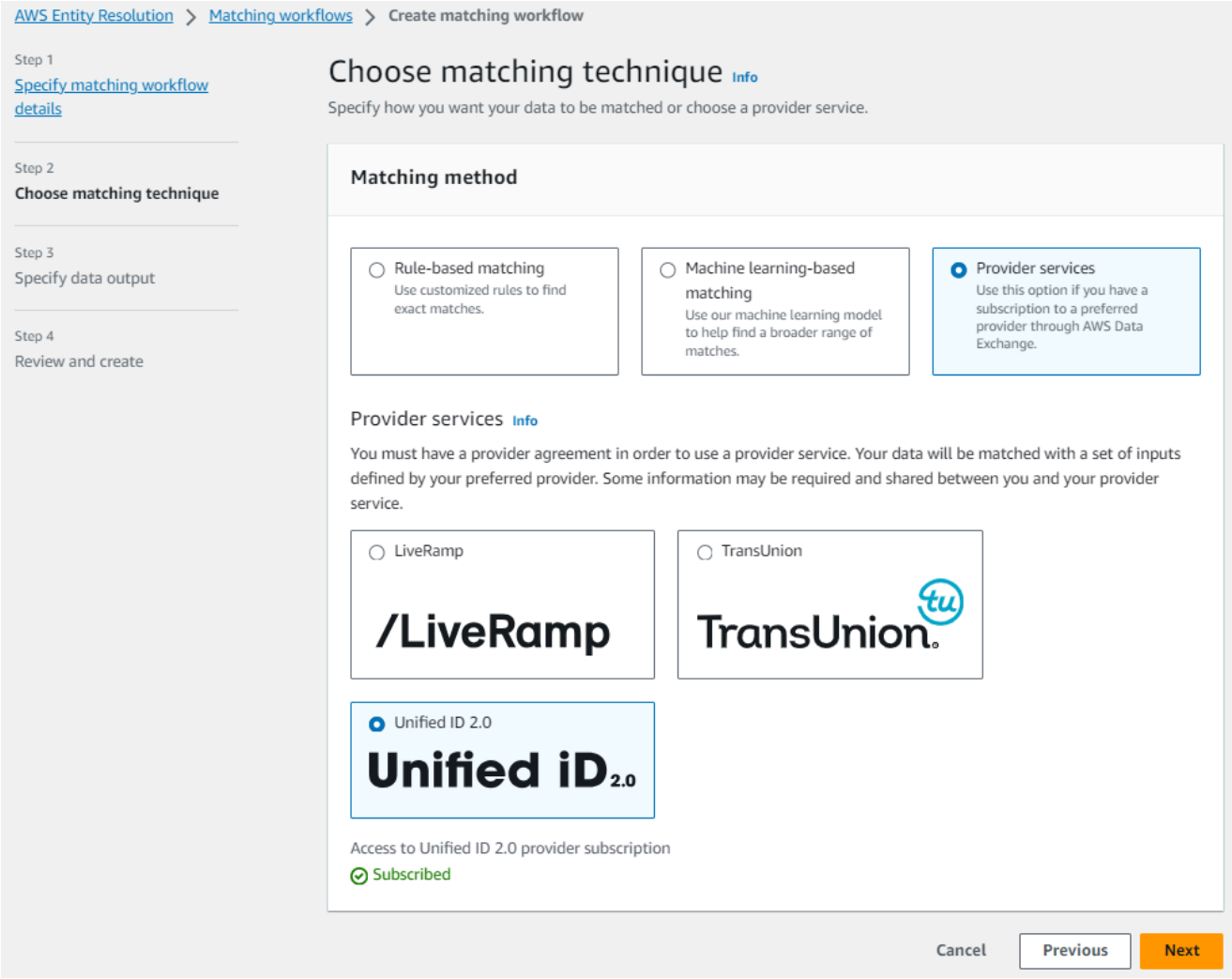
e. (オプション) リソースのタグを有効にするには、新しいタグを追加を選択し、キーと値のペアを入力します。

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、統合 ID 2.0 を選択します。



c. [Next (次へ)] を選択します。

6. ステップ 3: データ出力を指定するには：

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または元のデータのどちらにするかを選択します。

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

c. Unified ID 2.0 で生成された出力を表示します。

これは、UID 2.0 によって生成されたすべての追加情報のリストです。

d. データ出力では、含めるフィールド、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。

目標	推奨されるオプション
フィールドを含める	出力状態を 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、非表示を選択します。
マスクフィールド	出力フィールドを選択し、ハッシュ出力を選択します。
以前の設定をリセットする	[リセット] を選択します。

e. システム生成出力の場合、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: 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」の下に以下を表示します。

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

ジョブ履歴で以前に実行された一致する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. 一致するワークフロージョブが完了したら (ステータスが完了) 、データ出力タブに移動し、Amazon S3 の場所を選択して結果を表示できます。

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と、エンティティ解決プロセスをup-to-date保ち、時間の経過とともに変化する組織の要件に対応できます。エンティティ解決プロセスの精度と効率を向上させるために、一致する基準、手法、またはデータ出力を調整することができます。現在のワークフローの結果で問題やエラーを特定した場合は、編集すると、それらの問題の診断と解決に役立ちます。

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、 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で、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. 一致する手法の選択ページで、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が使用されなくなったり、古くなったりした場合、それを削除するとワークスペースを整理して整理し、整理解除するのに役立ちます。古いワークフローを置き換える改善された新しいワークフローを開発した場合、古いワークフローを削除すると、up-to-dateプロセスのみを使用するようになります。

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 AWS アカウント、 でAWS Entity Resolution コンソールを開きます。まだ開いていない場合は、 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で、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、 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 (ジョブのステータスは完了です)。
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：

状況	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 AWS アカウント、 でAWS Entity Resolution コンソールを開きます。まだ開いていない場合は、 を開きます。
2. 左側のナビゲーションペインのワークフローで、一致を選択します。
3. ルールベースまたは ML ベースのマッチングワークフローを選択します。
4. 一致するワークフローの詳細ページで、アクションドロップダウンリストから一意の IDs の削除を選択します。
5. 削除する一意の ID を一意の IDsセクションに入力します。

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

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

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

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け取りました

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) は名前`jobId`として を持つ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
  - データの行に 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
  - ソース間での重複
  - 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**
>
> 前述の理由でエラーファイルのレコードが作成された場合は、サービスの処理コストが発生するため、料金が発生します。エラーファイルのレコードが内部サーバーエラーによるものである場合、料金は発生しません。

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。これにより、ID マッピングテーブルが生成されます。

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。

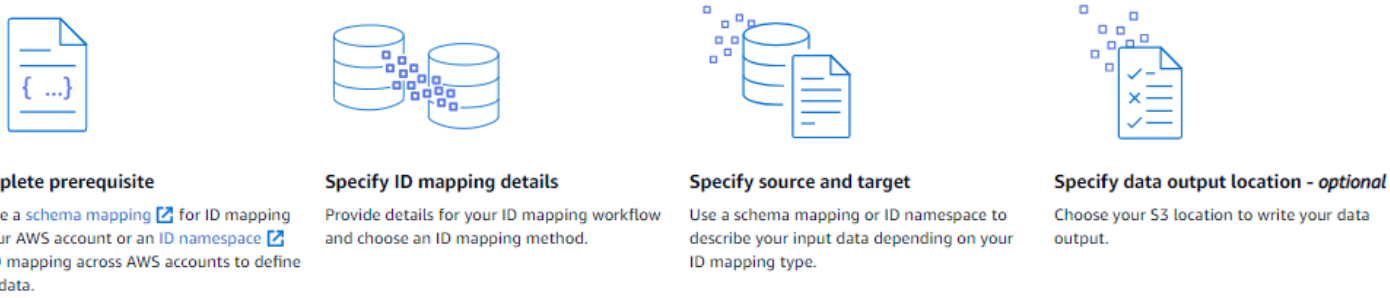
- ルールベースの ID マッピング – 一致するルールを使用して、ソースからターゲットにファーストパーティーデータを変換します。
- プロバイダーサービス ID マッピング – LiveRamp プロバイダーサービスを使用して、ソースからターゲットにサードパーティーデータを変換します。

> **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 LiveRamp と統合されています。LiveRamp サービスのサブスクリプションをお持ちの場合は、LiveRamp を使用して ID マッピングワークフローを作成して、トランスコードを実行できます。LiveRamp トランスコーディングを使用すると、ソース RampIDs のセットを任意のターゲットターゲットターゲット 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、LiveRamp ドキュメントウェブサイトの「ADX による翻訳の実行」を参照してください。

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 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 つのデータセット間で独自の ID マッピングを実行できます AWS アカウント。

ID マッピングワークフローを自分で作成する前に 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 マッピング方法 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、まず以下を実行する必要があります。

- 「AWS エンティティ解決の設定」のタスクを完了します。
- 使用している入力データのタイプに応じて入力データテーブルを準備する、 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) LiveRamp で ID マッピングワークフローを作成する前に、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 ################ を独自の情報に置き換えます。

##########	The Amazon S3 bucket that temporarily stores your data while running a provider service-based workflow.

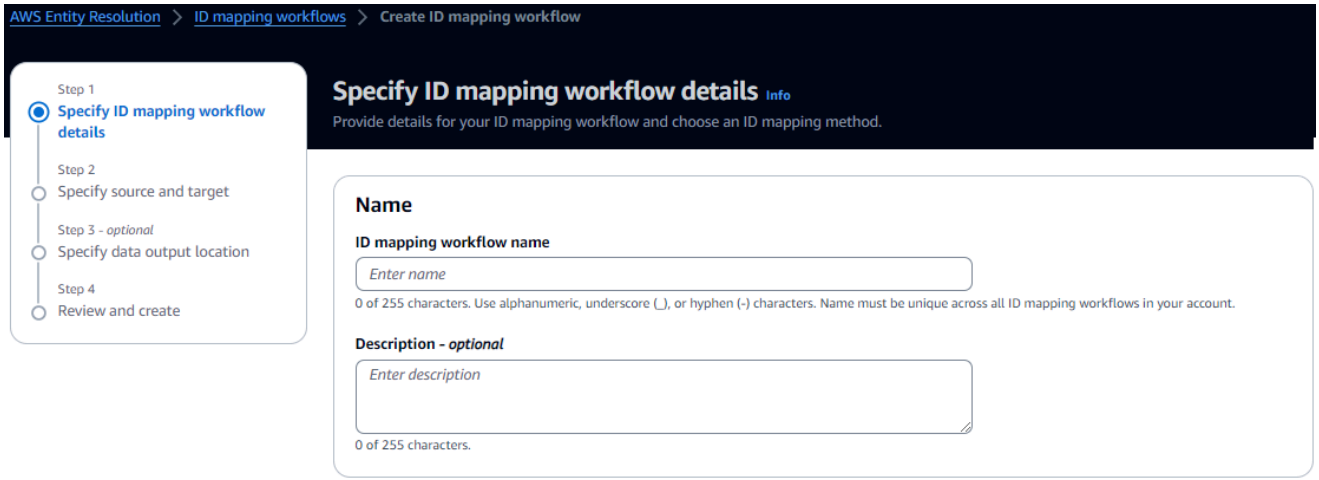
ID マッピングワークフローの作成 (ルールベース)

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 AWS アカウント、まだ AWS Entity Resolution コンソールを開いていない場合は、 で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. [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. Source で、該当するシナリオを選択し、推奨される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、 AWS Glue 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一致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 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. ルールパラメータについては、以下を実行します。

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するが、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. 比較パラメータと一致パラメータの場合、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。

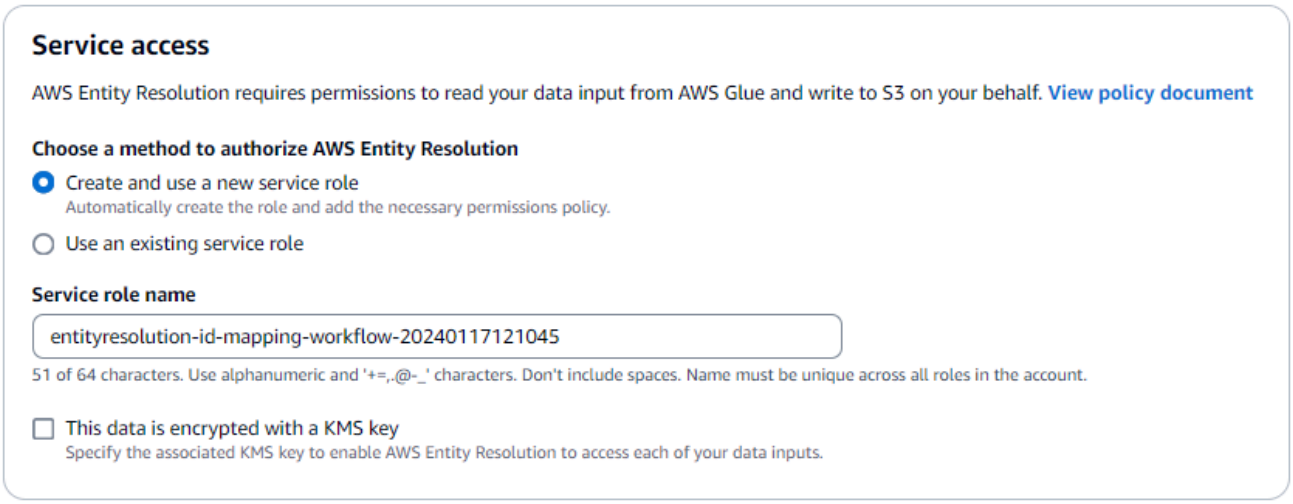
d. 目標に基づいて次のいずれかのオプションを選択して、レコードマッチングタイプを指定します。

目標	推奨されるオプション
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するレコードごとに、一致するレコードを 1 つだけソースに保存します。	1 つのソースから 1 つのターゲットへ

目標	推奨されるオプション
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するレコードごとに、一致するすべてのレコードをソースに保存します。	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 `entityresolution-id-mapping-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	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. [IAM で表示] 外部リンク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。

6. [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. データ出力先については、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. 暗号化では、暗号化設定をカスタマイズすることを選択した場合は、AWS KMS キー ARN を入力するか、 AWS KMS キーの作成を選択します。
   b. [次へ] を選択します。
8. ステップ 4: 確認して作成するには、次の手順を実行します。
   a. 前のステップで選択した内容を確認し、必要に応じて編集します。
   b. [作成] を選択します。

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

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

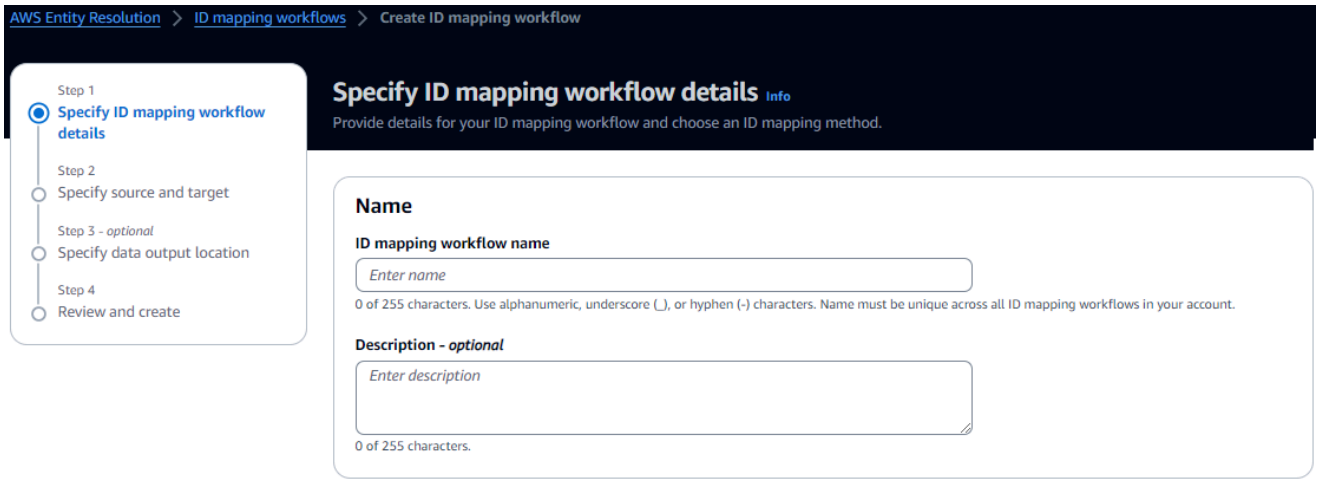
ID マッピングワークフローの作成 (プロバイダーサービス)

このトピックでは、LiveRamp 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、維持された RampIDsまたは派生した RampID を使用して、ソース RampIDs。

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 AWS アカウント、まだ AWS Entity Resolution コンソールを開いていない場合は、 で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。

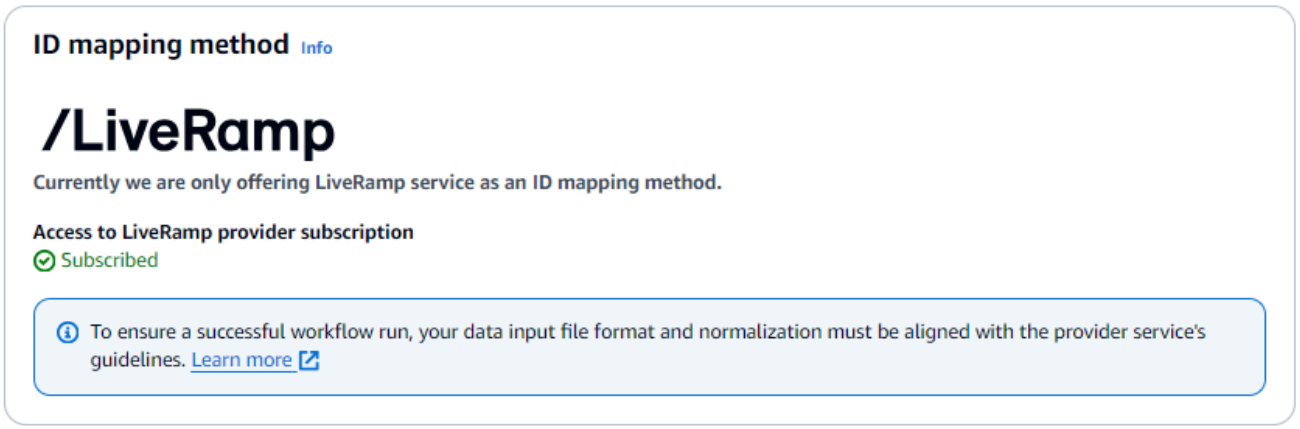
   a. ID マッピングワークフロー名とオプションの 説明を入力します。



   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。LiveRamp のサブスクリプションをお持ちの場合、ステータスは Subscribed と表示されます。LiveRamp をサブスクライブする方法の詳細については、

「」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。



> **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。LiveRamp 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の「ADX による翻訳の実行」を参照してください。

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

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

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

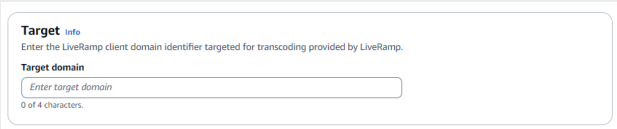
e. [次へ] を選択します。

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。

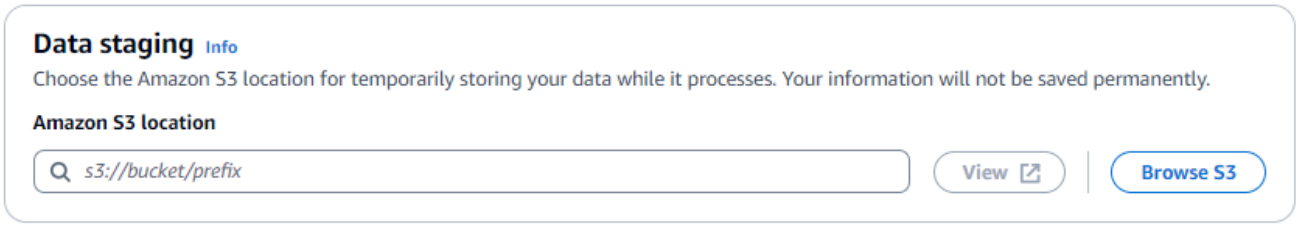
a. Source で、該当するシナリオを選択し、推奨アクションを実行します。

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、 AWS Glue 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一致するワークフローを使用します。	1. 一致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。

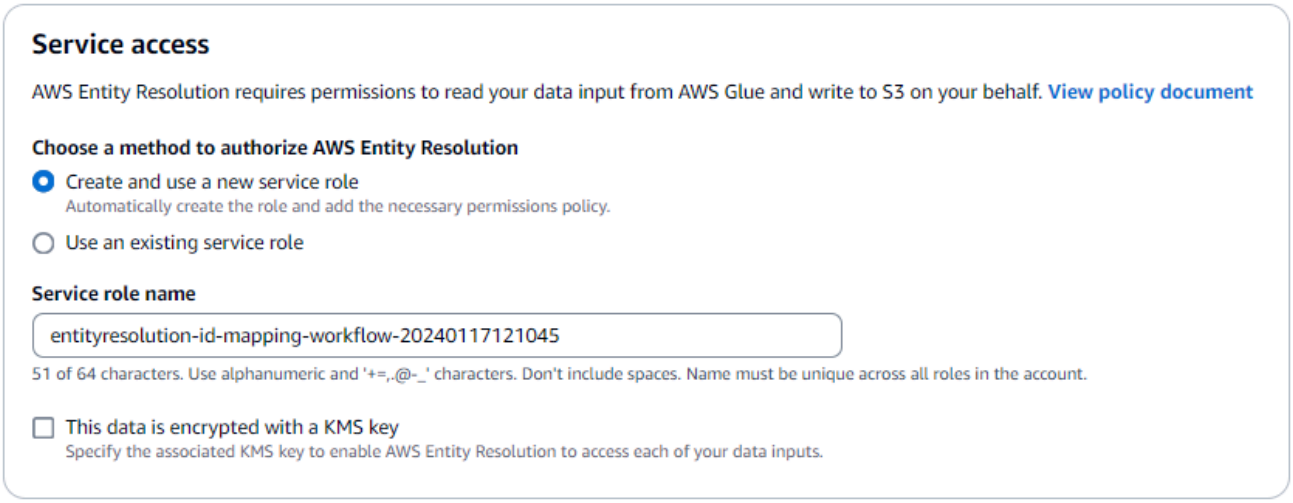
b. ターゲット では、選択した ID マッピング方法に基づいて、次のいずれかのアクションを実行します。

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	LiveRamp がターゲットドメインで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は、ID マッピングワークフロー出力を一時的に書き込む Amazon S3 の場所を選択します。



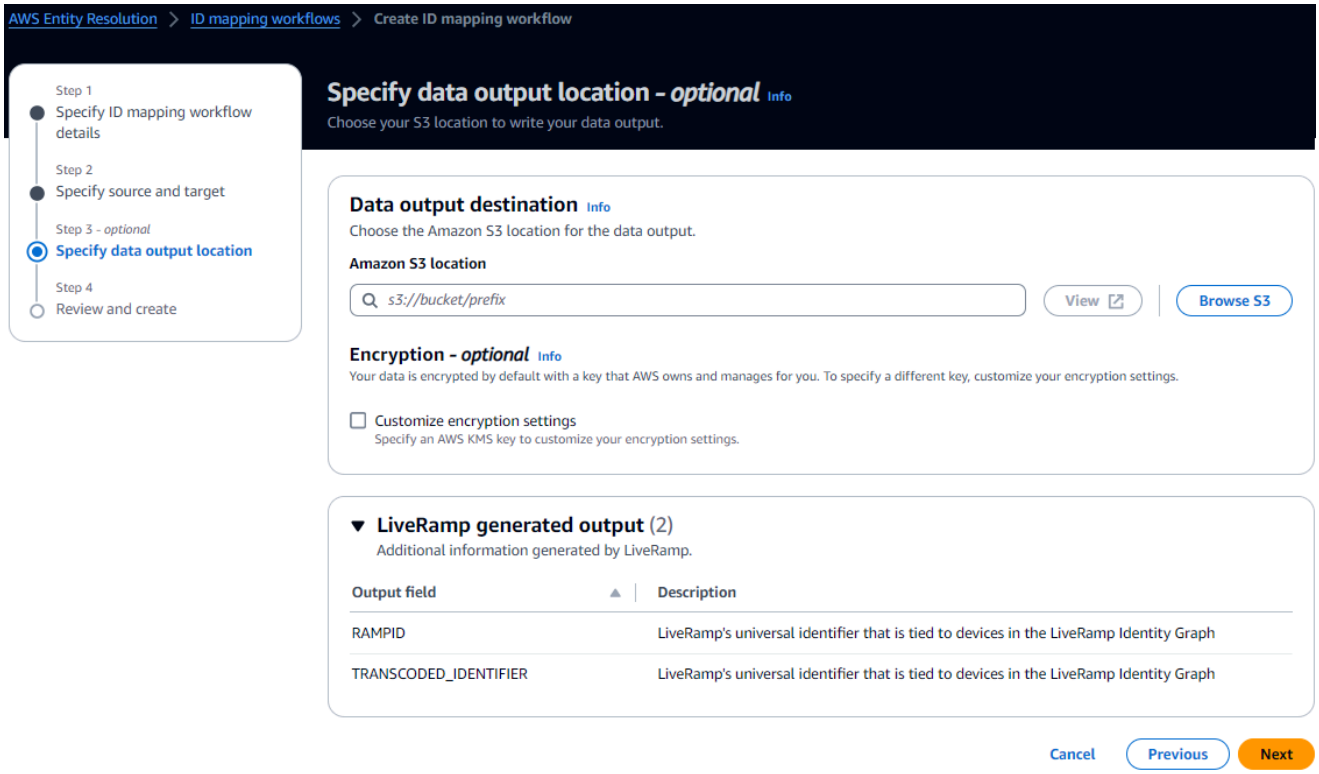
d. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。



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 `entityresolution-id-mapping-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	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. [IAM で表示] 外部リンク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。

6. [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. データ出力先については、次の操作を行います。
      i. データ出力の Amazon S3 の場所を選択します。
      ii. 暗号化で、暗号化設定をカスタマイズする場合は、AWS KMS キー ARN を入力するか、 AWS KMS キーの作成を選択します。
   b. LiveRamp が生成した出力を表示します。
   c. [次へ] を選択します。



8. ステップ 4: 確認して作成するには、次の手順を実行します。

   a. 前のステップで選択した内容を確認し、必要に応じて編集します。

   b. [作成] を選択します。

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

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。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。

たとえば、パブリッシャーは、独自のターゲット ID 名前空間 (独自の AWS アカウント) と広告主のソース ID 名前空間 (別の) 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 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、分析に使用できます。

以下のトピックでは、2 つの 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 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は、ID 名前空間 ARN 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 つの間で ID マッピングワークフローを作成するには、LiveRamp 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するためのアクセス許可 AWS アカウント が必要です。

  LiveRamp 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、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 ################ を独自の情報に置き換えます。

<KMSKeyARN>	The ARN of an AWS KMS customer managed key.

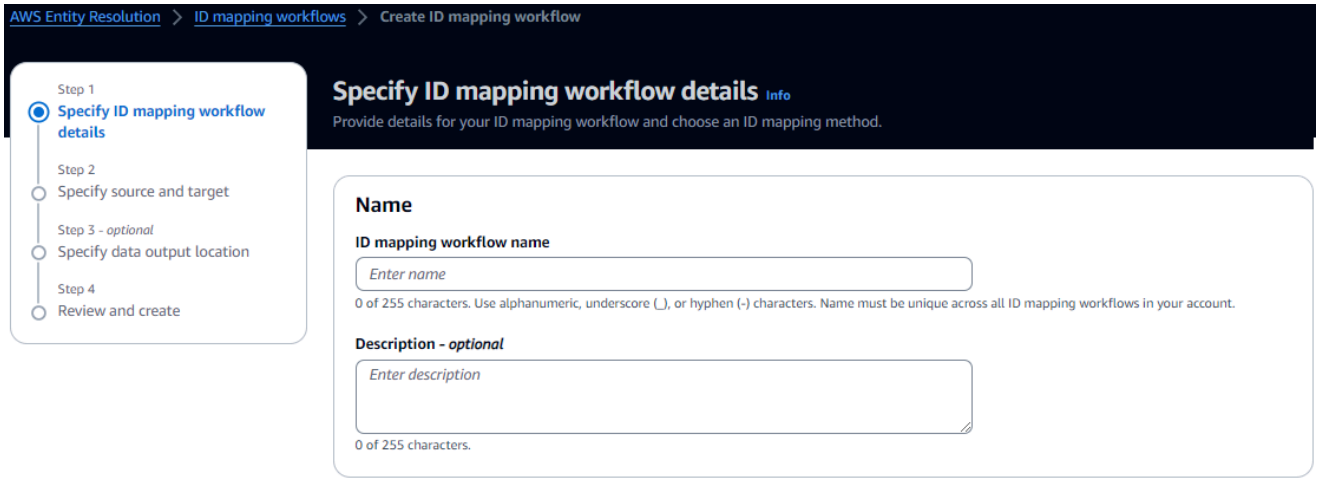
ID マッピングワークフローの作成 (ルールベース)

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 AWS アカウント、まだ AWS Entity Resolution コンソールを開いていない場合は、 で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で、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. [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は、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するが、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. 比較パラメータと一致パラメータについては、以下を実行します。

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	推奨されるオプション
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かかわら	複数の入力フィールド

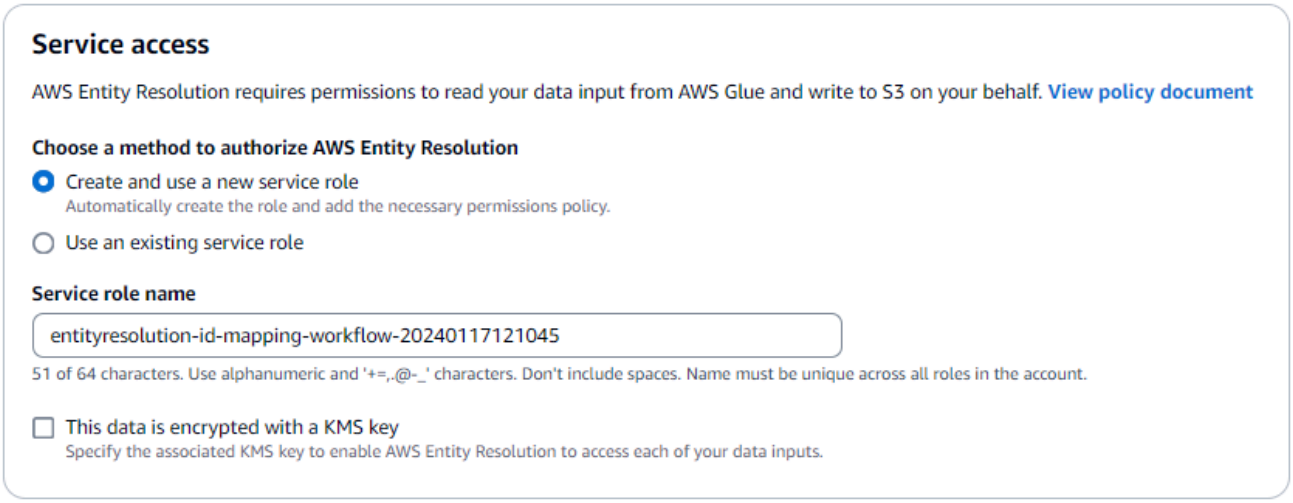
目標	推奨されるオプション
ず、複数の入力フィールドに保存されているデータ間で一致の任意の組み合わせを見つけます。	
複数の入力フィールドに保存されている類似データが一致しない場合、1 つの入力フィールド内の比較を制限します。	単一入力フィールド

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	推奨されるオプション
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するレコードごとに、一致するレコードを 1 つだけソースに保存します。	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するレコードごとに、一致するすべてのレコードをソースに保存します。	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 `entityresolution-id-mapping-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	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. [IAM で表示] 外部リンク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。

6. [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. データ出力先については、以下を実行します。
      i. データ出力の Amazon S3 の場所を選択します。
      ii. 暗号化では、暗号化設定をカスタマイズすることを選択した場合は、AWS KMS キー ARN を入力するか、 AWS KMS キーの作成を選択します。
   b. LiveRamp が生成した出力を表示します。
   c. [次へ] を選択します。
8. ステップ 4: 確認して作成するには、次の手順を実行します。
   a. 前のステップで選択した内容を確認し、必要に応じて編集します。

b. [作成] を選択します。

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

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

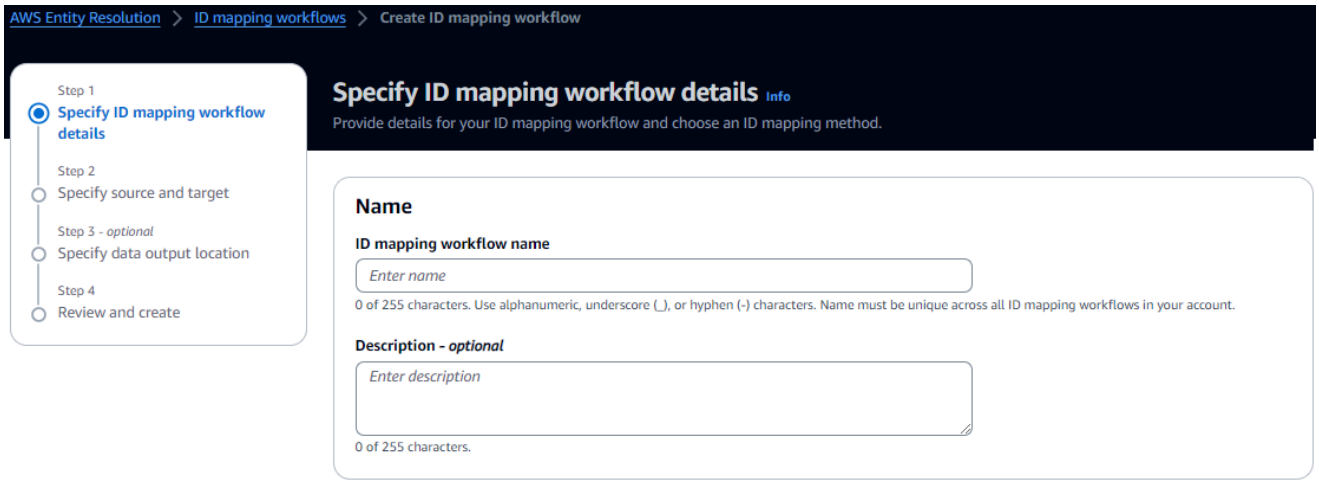
ID マッピングワークフローの作成 (プロバイダーサービス)

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。LiveRamp は、維持された RampIDsまたは派生した RampID を使用して、ソース RampIDs。

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 コンソールを開いていない場合は、 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。

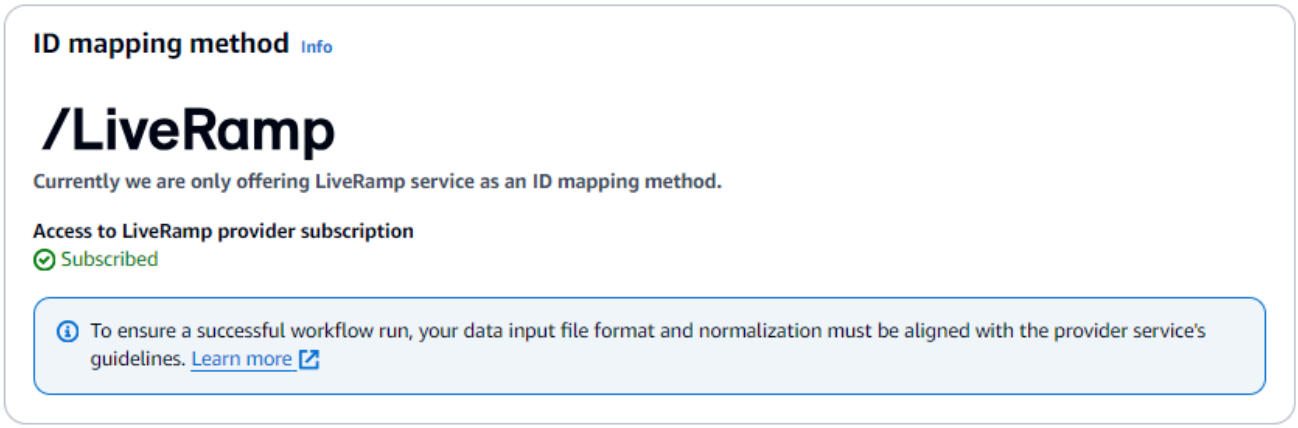
   a. ID マッピングワークフロー名とオプションの 説明を入力します。



   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。LiveRamp のサブスクリプションをお持ちの場合、ステータスは

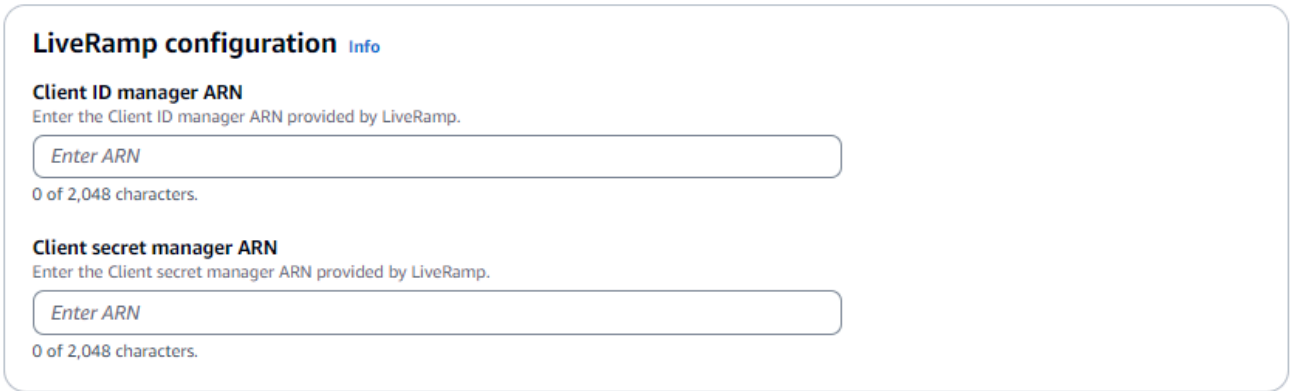
Subscribed と表示されます。LiveRamp をサブスクライブする方法の詳細については、「」を参照してくださいステップ 1: でプロバイダーサービスをサブスクライブする AWS Data Exchange。



> **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。LiveRamp 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の「ADX による翻訳の実行」を参照してください。

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

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



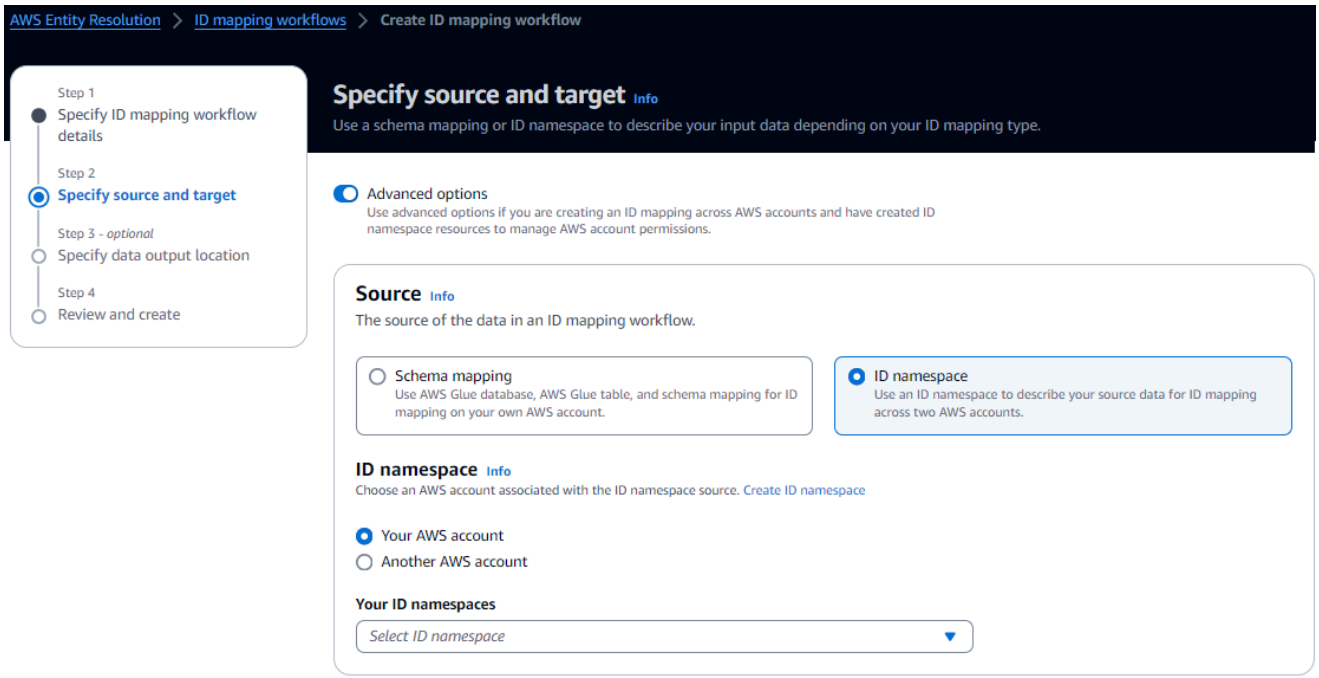
d. （オプション) リソースのタグを有効にするには、新しいタグを追加を選択し、キーと値のペアを入力します。

e. [次へ] を選択します。

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。

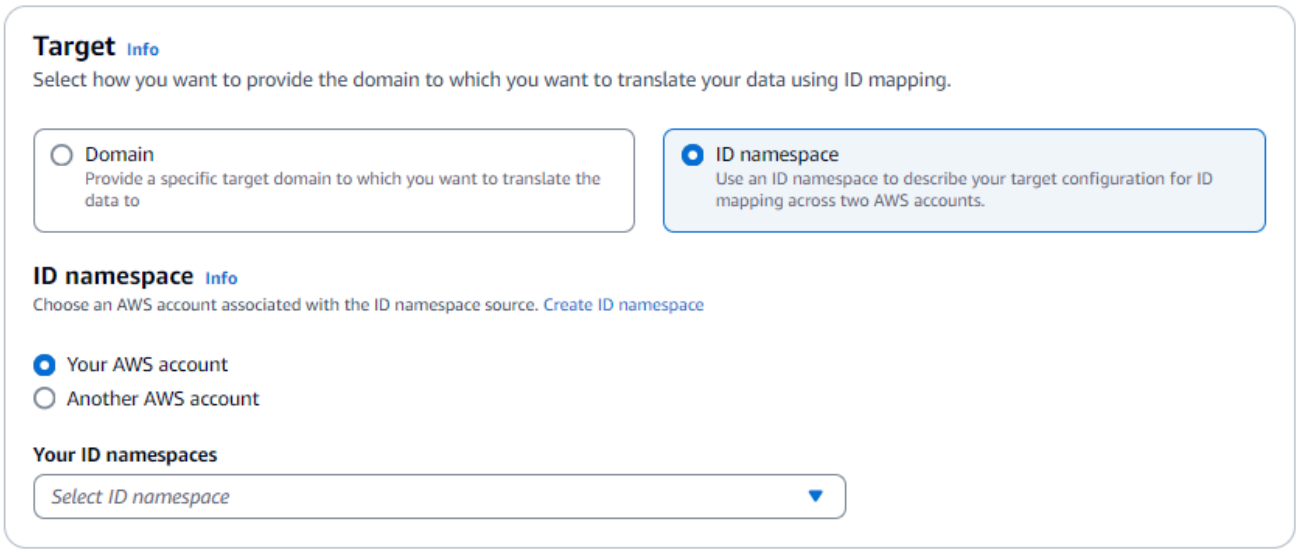
b. Source で、ID 名前空間を選択します。



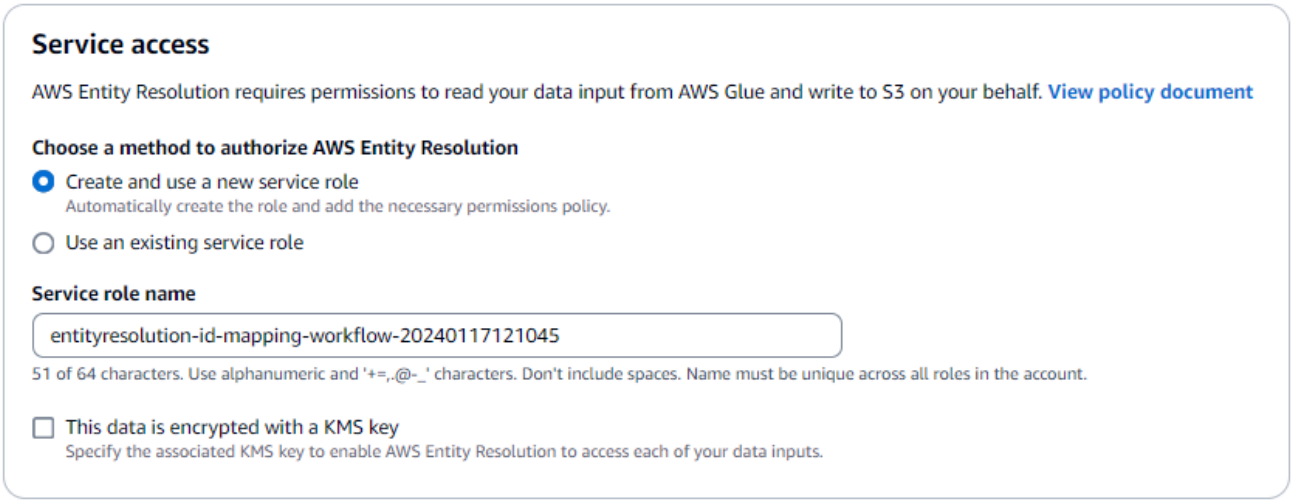
c. ID 名前空間の場合は、ID 名前空間の場所を特定し、推奨されるアクションを実行します。

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. AWS アカウント「」を選択します。 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. Target で、ID 名前空間を選択します。



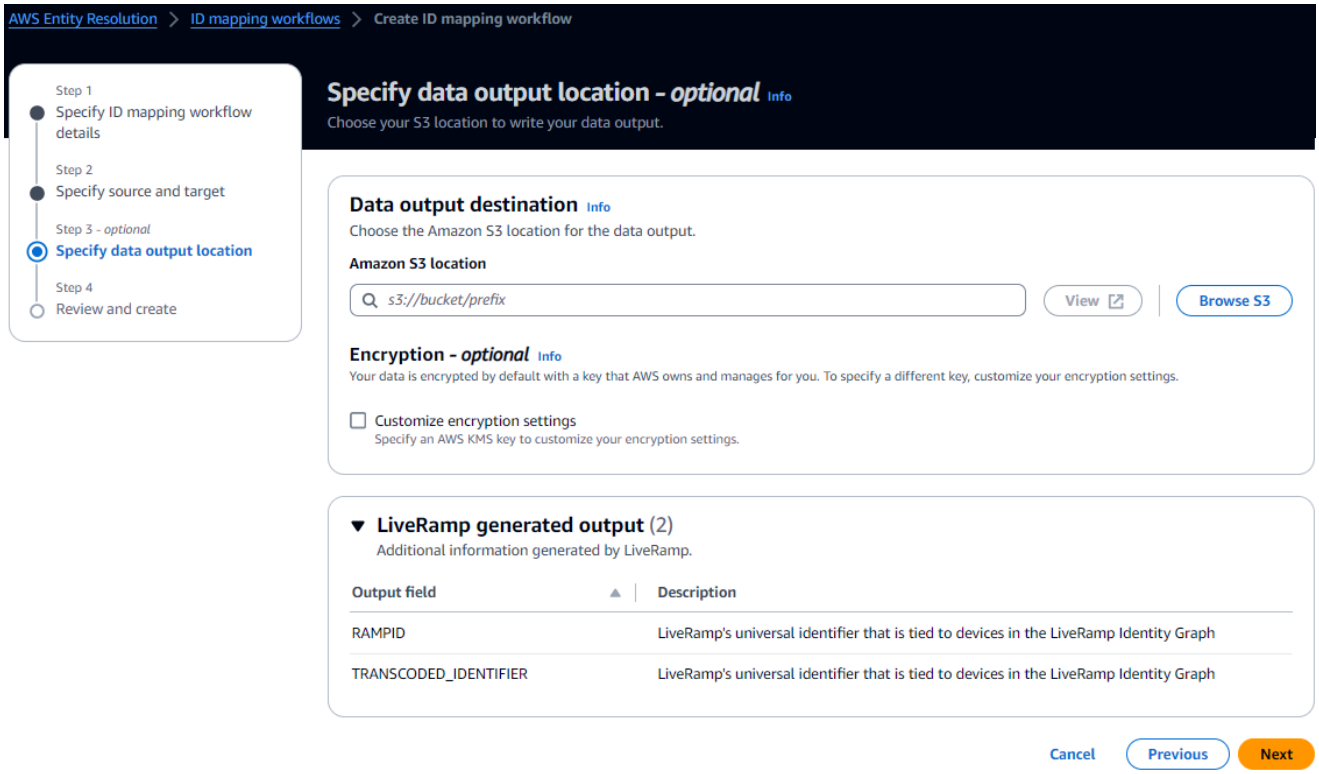
e. サービスアクセス許可を指定するには、 オプションを選択し、推奨アクションを実行します。



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 `entityresolution-id-mapping-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	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. [IAM で表示] 外部リンク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。

6. [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. データ出力先については、以下を実行します。
      i. データ出力の Amazon S3 の場所を選択します。
      ii. 暗号化では、暗号化設定をカスタマイズすることを選択した場合は、AWS KMS キー ARN を入力するか、 AWS KMS キーの作成を選択します。
   b. LiveRamp が生成した出力を表示します。
   c. [次へ] を選択します。



8. ステップ 4: 確認して作成するには、次の手順を実行します。

   a. 前のステップで選択した内容を確認し、必要に応じて編集します。

   b. [作成] を選択します。

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

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

ID マッピングワークフローの実行

1 つの ID マッピングワークフローを作成する AWS アカウントか、2 つの ID マッピングワークフローを作成 AWS アカウントしたら、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 AWS Entity Resolution で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、右上隅で実行を選択します。
5. 一致するワークフローの詳細ページで、メトリクスタブで、Last job metrics の下に以下を表示します。

   - 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
   - 処理されていないレコードの数
   - 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 (ステータスが完了) 、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 ID マッピングワークフローを作成する AWS アカウントか、2 つの 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 の場所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 AWS Entity Resolution コンソールを開いていない場合は、 で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で、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. データ出力先については、以下を実行します。

a. データ出力の Amazon S3 の場所を選択します。

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

6. サービスアクセス許可を指定するには、 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-id-mapping-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	1. ドロップダウンリストから [既存のサービスロール名] を選択します。 ロールを一覧表示するアクセス許可がある場合は、ロールのリストが表示されます。 ロールを一覧表示するアクセス許可がない場合は、使用するロールの Amazon リソースネーム (ARN) を入力できます。 既存のサービスロールがない場合、[既存のサービスロールを使用] オプションは使用できません。 2. [IAM で表示] 外部リンクを選択してサービスロールを表示します。

オプション	推奨されるアクション
	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
   - 処理されていないレコードの数
   - 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と、エンティティ解決機能をup-to-date状態に保ち、進化するビジネスニーズに経時的に一致させることができます。マッピングルール、手法、パラメータを調整し、ワークフローを最適化して、より正確で信頼性の高い ID マッチング結果を提供できます。また、新しいデータソースの追加、マッピングする IDs のタイプの拡大、ワークフローへの追加の一致基準の組み込みを行うこともできます。ID マッピング結果の問題やエラーを特定した場合、ワークフローで編集すると、それらの問題を診断して解決するのに役立ちます。

ID マッピングワークフローを編集するには：

1. にサインイン AWS Management Console し AWS アカウント、まだ AWS Entity Resolution コンソールを開いていない場合は、 で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、右上隅で編集を選択します。
5. ID マッピングワークフローの詳細の指定ページで、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使用しなくなった場合は、削除することでワークフロー管理を効率化できます。さらに、同様の目的を果たす冗長な ID マッピングワークフローや効率の低い ID マッピングワークフローを削除すると、プロセスを統合できます。

ID マッピングワークフローを削除するには：

1. にサインイン AWS Management Console し AWS アカウント、まだ AWS Entity Resolution コンソールを開いていない場合は、 で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、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 AWS Entity Resolution コンソールを開いていない場合は、 で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 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。

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により、お客様は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できます。LiveRamp や TransUnion 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 ID に変換 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、広告ツールや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 AWS Entity Resolution して、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コンシューマー識別子を広告 IDs にエンコードまたはトランスコード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、次の要件を満たす必要があります。

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 OpenAPI 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、AWS Data Exchange (ADX) Product Catalog に製品をリストする必要があります。製品が AWS Data Exchange Product Catalog にリストされると、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。

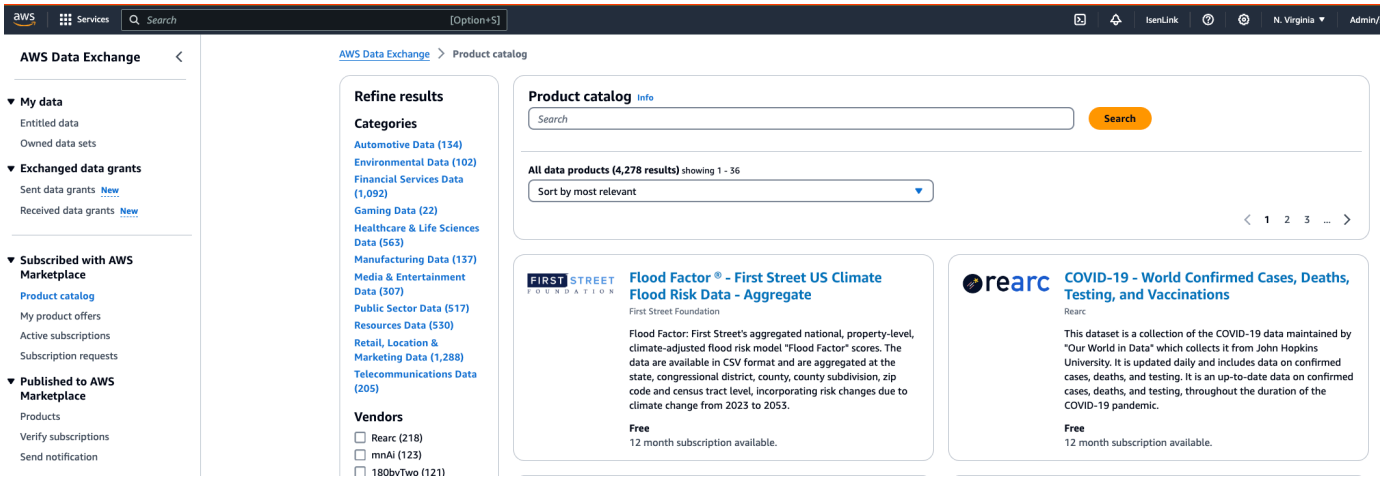
でプロバイダーサービスを一覧表示するには AWS Data Exchange

1. 新しいデータ製品プロバイダーの場合は 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. 「 AWS Data Exchange ユーザーガイドAPIs AWS Data Exchange 」の「API を含む製品の公開方法」セクションの手順に従って、REST API データセットを作成し、 で APIs を含む新しい製品を公開します。このプロセスは、 AWS Data Exchange コンソールまたは を使用して完了できます 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、「 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。 AWS Data Exchange

   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. Product AWS Data Exchange Catalog で製品が利用可能になると、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、「 AWS Data Exchange ユーザーガイド」のAPIs」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

プロバイダー属性を識別するための検証の例を次に示します。

- FirstName または LastName 属性は必須です。
- Email 属性が存在する場合は、ハッシュ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、追加の検証を行う必要があります。

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

AWS Entity Resolution には、プロバイダーとして使用できる OpenAPI 仕様があり、統合に関連する APIs を含むハンドシェイクとして使用できます。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。

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

AWS Entity Resolution OpenAPI 仕様の使用

OpenAPI 仕様は、関連す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ています。

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

- `GET Schema`

OpenAPI 仕様をリクエストするには、 AWS Entity Resolution ビジネス開発チーム <aws-entity-resolution-bd@amazon.com> 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、エンコードとトランスコードの両方の 2 種類の統合をサポートしています。OpenAPI 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。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ます。Amazon S3 リンクは、プロバイダー側で処理し、結果を事前に定義された出力 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、エンコードまたはトランスコーディング、S3 の場所、顧客が提供するスキーマ、必要な追加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。

   この API は を返し`JobId`、ジョブのステータスは `PENDING`、、`READY`、`COMPLETE`、または `IN_PROGRESS`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: この API は、JobId提供された に基づいてジョブを開始することをプロバイダーに通知します。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。

   この API はJobId、、ジョブStatusの 、、statusMessageおよび を返します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: この API は、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を通知します。

   この API はJobId、、ジョブStatusの 、、statusMessageおよび を返します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
}
```

これらの 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 TPS 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方法です。この AWS Entity Resolution ワークフローでは、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実行します。次に、 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 定義のいずれかを使用して有効になります。 は、以下を通じて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: この API は、source_id識別子 を使用して、そのレコードrecordFieldsに関連付けられたデータをプロバイダーに送信します。

この API は を返します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
    }
  ]
}
```

これらの 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する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、 が提供する APIs 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。 AWS Data Exchange はこの ARN を と AWS Entity Resolution 呼んでいます`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の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の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。

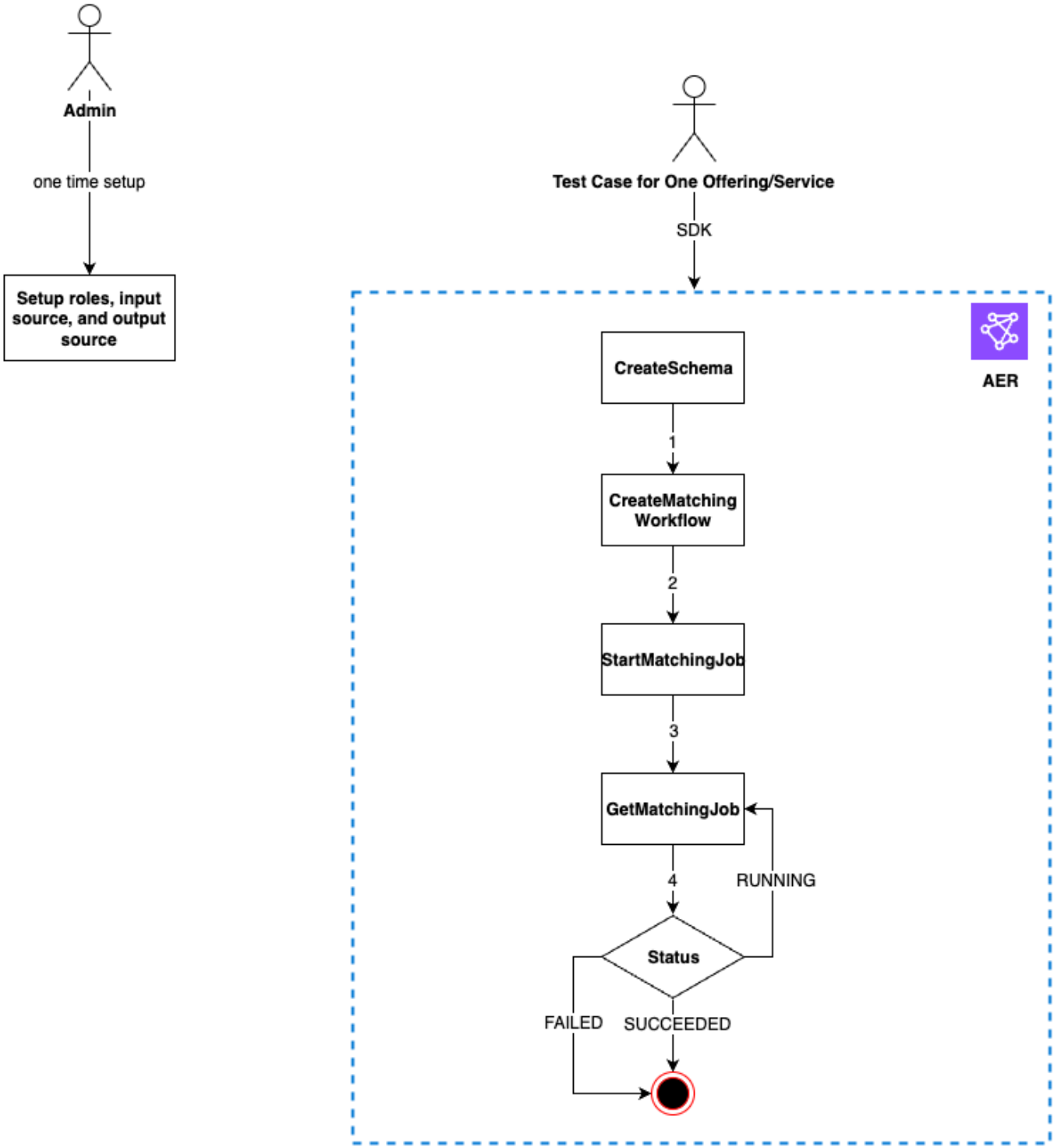
プロバイダーは、テストアカウントと独自のデータを使用して、 AWS Entity Resolution Software Development Kit (SDK) を使用してこれらのend-to-endのテストケースを実行できます。プロバイダーから問題が発生した場合、 は優先エスカレーションパス AWS Entity Resolution を使用して問題をエスカレーションします。さらに、プロバイダーはテスト結果に独自のモニタリングを実装する必要があります。プロバイダーは、これらのテストの実行に使用される AWS アカウント IDsを共有する必要があります AWS Entity Resolution。

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でき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、 が提供する APIs 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、プロバイダーはこれらのワークフローを 1 日 1 回 200 レコードで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 SDK を使用し、テストアカウント AWS Data Exchange を使用して を通じて提供されるサービスに対してend-to-endのテストを実行します。プロバイダーは、サービスまた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`)) を提供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、合格す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の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. (1 回限りのセットアップ) 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 APIs。

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

API

AWS Entity Resolution APIs

1. CreateSchemaMapping API を使用してスキーママッピングを作成します。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、CreateSchemaMapping API 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。

   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 に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、AWS Entity 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 **`id`** と を含むデータソースのスキーママッピングの作成 **`email`**

   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 Java SDK を含むデータソース**id**と Java SDK **email**を使用するデータソースのスキーママッピングの作成

以下は、Java SDK を含むデータソースidと emailを使用するデータソースのスキーママッピングの例です。

```
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. CreateMatchingWorkflow API を使用して一致するワークフローを作成します。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、CreateMatchingWorkflow API 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。

   Example Java SDK を使用して一致するワークフローを作成する

   以下は、Java SDK を使用した一致するワークフローの例です。

```
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. StartMatchingJob API を使用して、一致するワークフローを実行します。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、StartMatchingJob API 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。

   Example Java SDK を使用して一致するワークフローを実行する

   以下は、Java SDK を使用して一致するワークフローを実行する例です。

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

4. GetMatchingJob API 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。

   この API は、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) を返します。

   Example Java SDK を使用した一致するワークフローのモニタリング

   以下は、Java SDK 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。

```
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のテストは完了です。

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 に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 **`id`** と を含むデータソースのスキーママッピング **`email`**

   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。

   一致する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と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. 一致するワークフローページでワークフローのステータスをモニタリングします。

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

   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。
   - 生成された一意の一致 IDs。
   - 入力レコードの数。

   ジョブ履歴で以前に実行された一致する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。

のセキュリティ AWS Entity Resolution

でのクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、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からメリットを得られます。

セキュリティは、 AWS とお客様の間で共有される責任です。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 のサービス で実行される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。 AWS また、 は、お客様が安全に使用できるサービスも提供します。AWS コンプライアンスプログラム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者は定期的にセキュリティの有効性をテストおよび検証。が適用されるコンプライアンスプログラムの詳細については AWS Entity Resolution、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – お客様の責任は AWS のサービス 、使用する によって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、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、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS Entity Resolution。以下のトピックでは、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 AWS Entity Resolution ように を設定する方法について説明します。また、 AWS Entity Resolution リソースのモニタリングや保護 AWS のサービス に役立つ他の 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。ユーザーは、このインフラストラクチャでホストされるコンテンツに

対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR の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 (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」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を、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含めないことを強くお勧めします。これは、コンソール AWS Entity Resolution 、API、または SDK を使用して AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

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

デフォルトでは、保管中のデータを暗号化することで、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 – は、お客様が作成、所有、管理して機密データの暗号化を可能にする対称カスタマーマネージド KMS キーの使用 AWS Entity Resolution をサポートします。この暗号化層はユーザーが完全に制御できるため、次のようなタスクを実行できます。

- キーポリシーの策定と維持
- IAM ポリシーとグラントの策定と維持
- キーポリシーの有効化と無効化
- 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。

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

が で許可 AWS Entity Resolution を使用する方法 AWS KMS

AWS Entity Resolution には、カスタマーマネージドキーを使用するための許可が必要です。カスタマーマネージドキーで暗号化された一致するワークフローを作成すると、 は CreateGrant リクエストを送信してユーザーに代わってグラント AWS Entity Resolution を作成します AWS KMS。の許可 AWS KMS は、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。 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、許可 AWS Entity Resolution が必要です。

- GenerateDataKey リクエストを に送信 AWS KMS して、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キーを生成します。
- 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、それらを使用してデータを暗号化できるようにします。

グラントへのアクセスの取り消しや、カスタマーマネージドキーに対するサービスのアクセスの取り消しは、いつでもできます。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。たとえば、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`エラーを返します。

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は AWS Management Console、、、または AWS KMS APIs を使用して作成できます。

対称カスタマーマネージドキーを作成するには

AWS Entity Resolution は、対称暗号化 KMS キーを使用した暗号化をサポートしています。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KeySpecするのに役立つ などのフィールドが含まれています。また、キーの使用状況 (暗号化、署名、または MACs の生成と検証) 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、 KeyUsage は 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を付与します。これにより、必要な権限付与オペレーション AWS Entity Resolution へのアクセスが可能になります。詳細については、「AWS Key Management Service デベロッパーガイド」の「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。

追加できるポリシーステートメントの例を次に示します AWS Entity Resolution。

```
{
      "Sid" : "Allow access to principals authorized to use AWS Entity Resolution",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "*"
      },
      "Action" : ["kms:DescribeKey","kms:CreateGrant"],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:ViaService" : "entityresolution.region.amazonaws.com",
          "kms:CallerAccount" : "111122223333"
        }
      }
}
```

ユーザーのアクセス許可

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

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

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

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

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

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

```
}
```

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

<KMSKeyARN>	AWS KMS Amazon Resource Name.

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

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

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

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

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

マッチングワークフロー – マッチングワークフローリソースを作成するときに、KMSArn を入力してデータキーを指定できます。KMSArn は、 AWS Entity Resolution を使用してリソースに保存されている識別可能な個人データを暗号化します。

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

2 つの で ID マッピングワークフローを作成または実行している場合は、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とき、または ID マッピングワークフロージョブを開始するときに、KMSArn を入力してデータキーを指定できます。KMSArn は、 AWS Entity Resolution を使用して、リソースに保存されている識別可能な個人データを暗号化します。

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

サービスの暗号化キー AWS Entity Resolution 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と、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 AWS Entity Resolution 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DescribeKeyするための GenerateDataKey、Decrypt、、および 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 作成する権限は、 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、 オペレーション AWS Entity Resolution を使用してRetireGrant、リソースを削除するときにグラントを削除します。

次に、CreateGrant オペレーションを記録するイベントの例を示します。


```
{
    "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": "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。

以下のイベント例では DescribeKey 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": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
    },
```

```
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKey

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

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

```
{
    "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。

以下のイベント例では Decrypt オペレーションを記録しています。

```
{
    "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内のインスタンスは AWS Entity Resolutionにアクセスするためにパブリックアドレスを必要としません。

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「Access AWS のサービス through 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ています。

VPC エンドポイントポリシーがサポートされています 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、 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
```

インターフェース· エンドポイントのプライベートDNSを有効にすると、デフォルトの地域DNS名を使用して AWS Entity Resolution へのAPI要求を行うことができます。例えば、`entityresolution.us-east-1.amazonaws.com` と指定します。

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、リストされた AWS Entity Resolution アクションへのアクセスが許可されます。

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

の Identity and Access Management AWS Entity Resolution

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

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

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、作業内容によって異なります AWS Entity Resolution。

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

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

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

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、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 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して にアクセスすると、間接的 AWS 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、「 AWS サインイン ユーザーガイド」の「 にサインインする方法 AWS アカウント」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」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、 では、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」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 のサービス 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「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

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

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

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

IAM ユーザーとグループ

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

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

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

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロールに切り替えることができます (コンソール) 。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 URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

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

「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

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

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

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

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

アイデンティティベースのポリシー

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

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

リソースベースのポリシー

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

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

アクセスコントロールリスト (ACL)

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

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

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートしています。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ポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の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、ビジネスが所

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

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

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

と IAM の AWS Entity Resolution 連携方法

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

で使用できる IAM の機能 AWS Entity Resolution

IAM 機能	AWS Entity Resolution サポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	はい
ポリシーアクション	はい
ポリシーリソース	あり
ポリシー条件キー	Yes
ACL	いいえ
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	はい
サービスリンクロール	いいえ

AWS Entity Resolution およびその他の AWS のサービスがほとんどの IAM 機能とどのように連携するかの概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

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

アイデンティティベースのポリシーのサポート: あり

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

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

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

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

内のリソースベースのポリシー AWS Entity Resolution

リソースベースのポリシーのサポート: あり

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

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

のポリシーアクション AWS Entity Resolution

ポリシーアクションのサポート:あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可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、「サービス認可リファレンス」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 JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに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。

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

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

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

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

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

のポリシー条件キー AWS Entity Resolution

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに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して、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 IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

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

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

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

ACLs AWS Entity Resolution

ACL のサポート: なし

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

での ABAC AWS Entity Resolution

ABAC (ポリシー内のタグ) のサポート: 一部

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

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

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

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。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。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM

ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

での一時的な認証情報の使用 AWS Entity Resolution

一時的な認証情報のサポート: あり

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

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の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。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。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 AWS を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

の転送アクセスセッション AWS Entity Resolution

転送アクセスセッション (FAS) のサポート: あり

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と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストリクエストを組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FASリクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS Entity Resolutionのサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」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 のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの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、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、「はい」 リンクを選択します。

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

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

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

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

トピック

- ポリシーに関する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

ポリシーに関するベストプラクティス

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

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

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

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

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

AWS Entity Resolution コンソールを使用する

AWS Entity Resolution コンソールにアクセスするには、一連の最小限のアクセス許可が必要です。これらのアクセス許可により、 内の AWS Entity Resolution リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

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

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

自分の権限の表示をユーザーに許可する

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

```
{
    "Version": "2012-10-17",
    "Statement": [
```

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

AWS の マネージドポリシー AWS Entity Resolution

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

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可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) に影響します。 AWS は、新しい AWS のサービス が起動されたとき、または既存のサービスで新しい API オペレーションが利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 マネージドポリシー: AWSEntityResolutionConsoleFullAccess

`AWSEntityResolutionConsoleFullAccess` ポリシーを IAM アイデンティティ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 Glue、 AWS のサービス などの関連 への特定の読み取りアクセスも許可 AWS KMS されるため、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` – 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、ユーザーエクスペリエンスのために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` – タグ付けキーと値の読み取りアクセスを許可します。

- KMSConsoleDisplay – データソースを復号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 – 顧客が使用権限を持っているかサブスクリプションを持っているか AWS Data Exchange を確認するための へのアクセスを許可します。

このポリシーのアクセス許可を確認するには、「 AWS マネージドポリシーリファレンス」のAWSEntityResolutionConsoleFullAccess」を参照してください。

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。

このポリシーのアクセス許可を確認するには、「 AWS マネージドポリシーリファレンス」のAWSEntityResolutionConsoleReadOnlyAccess」を参照してください。

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 AWS Entity Resolution してからの 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通知については、 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	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する ManageEventBridgeRules ADXReadAccess とを追加しました。	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、 と IAM の使用時に発生する可能性がある一般的な問題の診断 AWS Entity Resolution と修正に役立ちます。

トピック

- でアクションを実行する権限がない AWS Entity Resolution
- iam:PassRole を実行する権限がない
- 自分の 以外のユーザーに 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。管理者とは、ユーザーにユーザー名とパスワードを提供した人です。

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

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

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

iam:PassRole を実行する権限がない

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

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

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

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

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

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

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

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

詳細については、以下を参照してください:

- がこれらの機能 AWS Entity Resolution をサポートしているかどうかを確認するには、「」を参照してくださいと IAM の AWS Entity Resolution 連携方法。

- 所有 AWS アカウント する のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント する別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、「IAM ユーザーガイド」の「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

のコンプライアンス検証 AWS Entity Resolution

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、「コンプライアンスAWS のサービス プログラムによる対象範囲内コンプライアンス」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 「 Compliance ProgramsAssurance」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、「Downloading AWS Artifact Reports 」を参照してください。

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

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、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の機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべてが HIPAA 対応 AWS のサービス であるわけではありません。
- 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、お客様の業界と場所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。このガイドは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコント

ロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。

- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、セキュリティ状態を包括的に把握できます 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一覧については、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 – 環境をモニタリングして不審なアクティビティや悪意のあるアクティビティがないか調べることで AWS アカウント、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

AWS Entity Resolution 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。

決済カード業界のデータセキュリティ基準 (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 (DSS) に準拠していることが検証されています。PCI コンプライアンスパッケージのコピーをリクエストする方法など、 AWS PCI DSS の詳細については、「PCI DSS レベル 1」を参照してください。

System and Organization Controls (SOC)

AWS Entity Resolution は、SOC 1、SOC 2、SOC 3 などのシステムおよび組織統制 (SOC) 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統制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 Compliance ウェブサイトで入手できます。ここでは、公開されたレポートを表示して、 AWS 運用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。 は、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、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 には、データの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能が用意されています。

モニタリング AWS Entity Resolution

モニタリングは、 およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する AWS Entity Resolution 上で重要な部分です。 AWS には、監視 AWS Entity Resolution、問題発生時の報告、および必要に応じて自動アクションを実行するための以下のモニタリングツールが用意されています。

- 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。が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、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

トピック

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

AWS Entity Resolution は、ユーザー AWS CloudTrail、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 サービスである と統合されています AWS Entity Resolution。CloudTrail は、 AWS Entity Resolution のすべての API コールをイベントとしてキャプチャします。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、 イベントなど、Amazon S3 バケットへの CloudTrail 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。CloudTrail によって収集された情報を使用して、リクエストの実行元の IP アドレス AWS Entity Resolution、リクエストの実行者、リクエストの実行日時などの詳細を確認できます。

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

AWS Entity Resolution CloudTrail の情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。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イベント履歴の他の AWS サービスイベン

トとともに CloudTrail 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、 CloudTrail イベント履歴での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 ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

すべての AWS Entity Resolution アクションは CloudTrail によってログに記録され、 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) ユーザー認証情報を使用して行われたかどうか。
- 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 エレメント」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

「トレイル」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するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、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

パラメータなどの情報を含みます。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 と統合されています。これは 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を支援するサービスです。必要なすべての AWS リソース (AWS::EntityResolution::MatchingWorkflow、AWS::EntityResolution::SchemaMapping、AWS::EntityResoluti など) 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 Entity Resolution 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、同じリソースを複数の AWS アカウント およびリージョンで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 Entity Resolution および関連サービスのリソースをプロビジョニングおよび設定するには、AWS CloudFormation テンプレートを理解する必要があります。テンプレートは、JSON や YAML でフォーマットされたテキストファイルです。これらのテンプレートは、 AWS CloudFormation スタックでプロビジョニングするリソースを記述します。JSON または YAML に慣れていない場合は、 AWS CloudFormation Designer 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::MatchingWorkflow、AWS::EntityResolution::SchemaMapping、AWS::EntityRes および AWS::EntityResolution::PolicyStatement の作成がサポートされています AWS CloudFormation。AWS::EntityResolution::MatchingWorkflow、AWS::EntityResolution::SchemaMapping、AW の JSON テンプレートと YAML テンプレートの例を含む詳細については、AWS CloudFormation 「 ユーザーガイド」の「AWS エンティティ解決リソースタイプのリファレンス」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、以下の各トピックを参照してください。

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

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

- スキーママッピング

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

  詳細については、以下の各トピックを参照してください。

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

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

- ID マッピングワークフロー

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

  詳細については、以下の各トピックを参照してください。

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

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

- ID 名前空間

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

  詳細については、以下の各トピックを参照してください。

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

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

- PolicyStatement

  `PolicyStatement` オブジェクトを作成します。

  詳細については、以下の各トピックを参照してください。

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

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

の詳細 AWS CloudFormation

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

AWS アカウント には、 ごとに、以前は制限と呼ばれていたデフォルトのクォータがあります AWS のサービス。特に明記していない限り、クォータはリージョン固有です。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ることができません。

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。

AWS アカウント には、 に関連する次のクォータがあります 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、 が一致目的 AWS Entity Resolution に使用する列名と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を含める必要があります。

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	可能	現在の でこの AWS アカウント 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	可能	現在の でこの AWS アカウント 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、出力に含まれる一致するワークフローメタデータの一部です。
ワークフローのマッチング	10	可能	マッチングワークフローの最大数。
`GetMatchId` API リクエストのレート	50	可能	1 秒あたりの `GetCustomerID` API リクエストの最大数。

名前	デフォルト	引き上げ可能	説明
機械学習ベースのワークフローあたりのレコード	250M	はい	機械学習ベースのマッチングワークフローで処理できるレコードの最大数。
ルールベースのマッチングワークフローあたりのレコード	100M	はい	ルールベースのマッチングワークフローで処理できるレコードの最大数。
ワークフローあたりのルール	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。
スキーママッピング	50	可能	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 に指示します。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た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	[Rate limit] (レート制限)	説明
`CreateMatchingWorkflow` リクエストのレート	5 TPS	1 秒あたりの `CreateMatchingWorkflow` API コールの最大数。

リソース	[Rate limit] (レート制限)	説明
DeleteMatchingWorkflow リクエストのレート	5 TPS	1 秒あたりの DeleteMatchingWorkflow API コールの最大数。
GetMatchingWorkflow リクエストのレート	5 TPS	1 秒あたりの GetMatchingWorkflow API コールの最大数。
ListMatchingWorkflows リクエストのレート	5 TPS	1 秒あたりの ListMatchingWorkflows API コールの最大数。
UpdateMatchingWorkflow リクエストのレート	5 TPS	1 秒あたりの UpdateMatchingWorkflow API コールの最大数。
CreateSchemaMapping リクエストのレート	5 TPS	1 秒あたりの CreateSchemaMapping API コールの最大数。
DeleteSchemaMapping リクエストのレート	5 TPS	1 秒あたりの DeleteSchemaMapping API コールの最大数。
GetSchemaMapping リクエストのレート	5 TPS	1 秒あたりの GetSchemaMapping API コールの最大数。
ListSchemaMappings リクエストのレート	5 TPS	1 秒あたりの ListSchemaMappings API コールの最大数。
UpdateSchemaMapping リクエストのレート	5 TPS	1 秒あたりの UpdateSchemaMapping API コールの最大数。

リソース	[Rate limit] (レート制限)	説明
GetPartnerComponent リクエストのレート	5 TPS	1 秒あたりの GetPartnerComponent API コールの最大数。
ListPartnerComponents リクエストのレート	5 TPS	1 秒あたりの ListPartnerComponents API コールの最大数。
TagResource リクエストのレート	5 TPS	1 秒あたりの TagResource API コールの最大数。
UntagResource リクエストのレート	5 TPS	1 秒あたりの UntagResource API コールの最大数。
ListTagsForResource リクエストのレート	5 TPS	1 秒あたりの ListTagsForResource API コールの最大数。
CreateIdMappingWorkflow リクエストのレート	5 TPS	1 秒あたりの CreateIdMappingWorkflow API コールの最大数。
DeleteIdMappingWorkflow リクエストのレート	5 TPS	1 秒あたりの DeleteIdMappingWorkflow API コールの最大数。
GetIdMappingWorkflow リクエストのレート	5 TPS	1 秒あたりの GetIdMappingWorkflow API コールの最大数。
ListIdMappingWorkflow リクエストのレート	5 TPS	1 秒あたりの ListIdMappingWorkflow API コールの最大数。
UpdateIdMappingWorkflow リクエストのレート	5 TPS	1 秒あたりの UpdateIdMappingWorkflow API コールの最大数。

リソース	[Rate limit] (レート制限)	説明
ListProviderServices リクエストのレート	5 TPS	1 秒あたりの ListProviderServices API コールの最大数。
GetProviderService リクエストのレート	5 TPS	1 秒あたりの GetProviderService API コールの最大数。
CreateIdNamespace リクエストのレート	5 TPS	1 秒あたりの CreateIdNamespace API コールの最大数。
DeleteIdNamespace リクエストのレート	5 TPS	1 秒あたりの DeleteIdNamespace API コールの最大数。
GetIdNamespace リクエストのレート	5 TPS	1 秒あたりの GetIdNamespace API コールの最大数。
ListIdNamespaces リクエストのレート	5 TPS	1 秒あたりの ListIdNamespaces API コールの最大数。
UpdateIdNamespace リクエストのレート	5 TPS	1 秒あたりの UpdateIdNamespace API コールの最大数。
AddPolicyStatement リクエストのレート	5 TPS	1 秒あたりの AddPolicyStatement API コールの最大数。
DeletePolicyStatement リクエストのレート	5 TPS	1 秒あたりの DeletePolicyStatement API コールの最大数。

リソース	[Rate limit] (レート制限)	説明
GetPolicy リクエストのレート	5 TPS	1 秒あたりの GetPolicy API コールの最大数。
PutPolicy リクエストのレート	5 TPS	1 秒あたりの PutPolicy API コールの最大数。
GetMatchingJob リクエストのレート	10 TPS	1 秒あたりの GetMatchingJob API コールの最大数。
ListMatchingJobs リクエストのレート	5 TPS	1 秒あたりの ListMatchingJobs API コールの最大数。
StartMatchingJob リクエストのレート	5 TPS	1 秒あたりの StartMatchingJob API コールの最大数。
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。
GetIdMappingJob リクエストのレート	10 TPS	1 秒あたりの GetIdMappingJob API コールの最大数。
ListIdMappingJobs リクエストのレート	5 TPS	1 秒あたりの ListIdMappingJobs API コールの最大数。
StartIdMappingJob リクエストのレート	5 TPS	1 秒あたりの StartIdMappingJob API コールの最大数。
BatchDeleteUniqueId リクエストのレート	5 TPS	1 秒あたりの BatchDeleteUniqueId API コールの最大数。

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

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

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

変更	説明	日付
ID マッピングワークフロー – 更新	ID マッピングワークフローを使用するときに AWS Glue パーティショニングを設定できるようになりました。	2025 年 3 月 25 日
クォータ – 更新	ドキュメントのみの更新。ルールベースのマッチングワークフローは最大 100Mレコードを処理でき、機械学習ベースのマッチングワークフローは最大 250Mレコードを処理できます。制限の引き上げが必要なお客様は、 サービスチームにお問い合わせください。	2025 年 2 月 7 日
スキーママッピング – 更新	フルネーム、フルアドレス、フルフォン属性タイプで正規化がサポートされることを明確にするためのドキュメントのみの更新。	2025年1月17日
プロバイダー統合	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	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翻訳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、データ管理規制に準拠するために、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 は、次のリソースと を追加`AWS::EntityResolution::IdNamespace` `AWS::EntityResolution::PolicyStatement` し、次のリソース を更新しましたAWS::EntityResolution::IdMappingWorkflow 。	2024 年 4 月 2 日
一致 ID の検索	お客様は、処理されたルールベースのワークフローに対応する一致 ID と関連するルール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ベースのマッチングワークフローで PII ベースの RAMPID 割り当てをサポートするようになりました。	2024 年 2 月 12 日
AWS PrivateLink	AWS Entity Resolution では、で追加のデータセキュリティがサポートされるようになりました。 AWS PrivateLink これにより、お客様は でホストされているサービスにプライベートにアクセスできます 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 に 2 つの新しい管理ポリシーが追加されました。	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 AWS Entity Resolution、Amazon Relational Database Service (Amazon RDS) タグ、API コールなど、すべてのでリソースを明確に指定する必要がある場合に必要です。

属性タイプ

入力フィールドの属性のタイプ。スキーママッピングを作成するときは、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のリストから属性タイプを選択します。属性タイプは、提示するデータ AWS Entity Resolution の種類を に伝え、適切に分類および正規化できるようにします。

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ます。これにより、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up-to-date状態になります。

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。

信頼レベル (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。

Encryption

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一致させるのに役立ちます。

例えば、、**first_name**、 **middle_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 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。これを hash. AWS Entity Resolution uses Secure Hash Algorithm 256-bit (SHA256) ハッシュプロトコルと呼び、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の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 現在、 はプロバイダーのサービスベースの ID マッピング方法として LiveRamp をサポートしています。この方法 AWS Data Exchange を使用するには、 を通じて LiveRamp 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。これにより、ID マッピングテーブルが生成されます。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を設定して、独自の AWS アカウント または 2 つの で実行できます AWS アカウント。

ID 名前空間

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

ID 名前空間には、 SOURCEと の 2 種類がありますTARGET。には、ID マッピングワークフローで処理されるソースデータの設定SOURCEが含まれています。には、すべてのソースが解決されるターゲットデータの設定TARGETが含まれています。2 つの にわたって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、ID マッピングワークフローを実行したら、 でコラボレーションに参加 AWS Clean Rooms して、ID マッピングテーブルでマルチテーブル結合を実行し、データを分析できます。

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

入力フィールド

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

入力ソース ARN (InputSourceARN)

AWS Glue テーブル入力用に生成された Amazon リソースネーム (ARN)。これは、出力に含まれる一致するワークフローメタデータの一部です。

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一致を検出します。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、マッチングされたデータセットごとにマッチング ID と信頼レベルを返します。

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。

Many-to-Manyマッチング

Many-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、 `mobile_phone`や など、同じ一致キー「Phonehome_phone」を持つ複数の電話番号入力フィールドがあるとします。many-to-manyマッチングを使用して、`mobile_phone`入力フィールド

のデータとmobile_phone入力フィールドのデータおよびhome_phone入力フィールドのデータを比較します。

一致ルールは、 (または) オペレーションで同じ一致キーを持つ複数の入力フィールドのデータを評価し、one-to-many一致は複数の入力フィールドの値を比較します。つまり、2 つのレコード間でmobile_phoneまたは の組み合わせがhome_phone一致すると、「Phone」一致キーは一致を返します。一致キー「Phone」で一致を検索するには、 `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 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、一致する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、異なる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。

mobile_phone 入力フィールドやhome_phone入力フィールドなど、比較するデータに複数のタイプの電話番号情報がある場合は、両方の一致キー「Phone」を指定できます。次に、ルールベースのマッチングを設定して、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できます (「一致ワークフロー」セクションのOne-to-One のマッチング」およびMany-to-Manyマッチング」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ングキーを作成できます。次に、一致する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一致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から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 (例えば、一致するルールやモデルを通じて) ことに基づいて、どちらが類似しているか、または「一致する」かを判断するプロセス。

マッチングワークフロー

一致する入力データとマッチングの実行方法を指定するようにセットアップしたプロセス。

一致するワークフローの説明

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

一致するワークフロー名

指定した一致するワークフローの名前。

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

ワークフローメタデータの一致

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

正規化 (ApplyNormalization)

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

たとえば、入力フィールドの属性タイプがフルフォンで、入力テーブルの値が の形式である場合(123) 456-7890、 AWS Entity Resolution は値を に正規化します1234567890。

> **Note**
>
> 正規化は、名前、住所、電話番号、E メールのグループタイプでのみサポートされます。

以下のセクションでは、標準の正規化ルールについて説明します。

ML ベースのマッチングについては、「」を参照してください正規化 (ApplyNormalization) – ML ベースのみ。

トピック

- 名前
- E メール
- 電話
- Address
- ハッシュ
- Source_ID

名前

> **Note**
>
> 正規化は、名前グループタイプでのみサポートされます。
> 名前グループタイプは、コンソールにはフルネームとして、API NAME にはフルネームとして表示されます。
> 名前グループタイプのサブタイプを正規化する場合：
>
> - コンソールで、フルネームグループに名、ミドルネーム、姓のサブタイプを割り当てます。

- CreateSchemaMapping API で、NAMEgroupName に次のタイプを割り当てます: NAME_FIRST、NAME_MIDDLE、NAME_LAST。

- TRIM = 先頭と末尾の空白をトリミングする
- LOWERCASE = すべてのアルファ文字を小文字にします
- CONVERT_ACCENT = Covert アクセント付き文字から通常の文字へ
- REMOVE_ALL_NON_ALPHA = 英数字以外の文字をすべて削除します [a-zA-Z]

E メール

> **Note**
>
> 正規化は E メールグループタイプでサポートされています。
> E メールグループタイプは、コンソールには E メールアドレスとして、API EMAIL_ADDRESS には E メールアドレスとして表示されます。

- TRIM = 先頭と末尾の空白をトリミングする
- LOWERCASE = すべてのアルファ文字を小文字にします
- CONVERT_ACCENT = Covert アクセント付き文字から通常の文字へ
- EMAIL_ADDRESS_UTIL_NORM = ユーザー名からドット (.) を削除し、ユーザー名のプラス記号 (+) の後にすべてを削除し、一般的なドメインバリエーションを標準化します。
- REMOVE_ALL_NON_EMAIL_CHARS = non-alpha-numeric文字 [a-zA-Z0-9] と [.@-] をすべて削除します

電話

> **Note**
>
> 正規化は、電話グループタイプでのみサポートされています。
> 電話グループタイプは、コンソールではフルフォンとして、API PHONE では として表示されます。
> 電話グループタイプのサブタイプを正規化する場合：

- コンソールで、電話番号と電話番号の国コードのサブタイプをフルフォングループに割り当てます。
- CreateSchemaMapping API で、次のタイプを PHONE groupName PHONE_NUMBERと に割り当てますPHONE_COUNTRYCODE。

- TRIM = 先頭と末尾の空白をトリミングする
- REMOVE_ALL_NON_NUMERIC = 数値以外の文字をすべて削除します [0-9]
- REMOVE_ALL_LEADING_ZEROES = 先頭のゼロをすべて削除します
- EN"_PREFIX_WITH_MAP, "phonePrefixMap" = 各電話番号を調べ、phonePrefixMap のパターンと照合しようとします。一致が見つかった場合、ルールは電話番号のプレフィックスを追加または変更して、マップで指定された標準化された形式に準拠していることを確認します。

Address

> **Note**
>
> 正規化は、アドレスグループタイプでのみサポートされています。
> アドレスグループタイプは、コンソールにはフルアドレスとして、API ADDRESS　にはフルアドレスとして表示されます。
> Address グループタイプのサブタイプを正規化する場合：
>
> - コンソールで、住所 1、住所 2、住所 3 名、市区町村名、州、国、郵便番号 t のフルアドレスグループに次のサブタイプを割り当てます。
> - CreateSchemaMapping API で、ADDRESSgroupName に次のタイプを割り当てます: ADDRESS_STREET1、ADDRESS_STREET2、ADDRESS_STREET3、、ADDRESS_CITYADDRESS_STA

- TRIM = 先頭と末尾の空白をトリミングする
- LOWERCASE = すべてのアルファ文字を小文字にします
- CONVERT_ACCENT = Covert アクセント付き文字から通常の文字へ
- REMOVE_ALL_NON_ALPHA = 英数字以外の文字をすべて削除します [a-zA-Z]
- ADDRESS_RENAME_WORD_MAP を使用する RENAME_WORDS = Address 文字列の単語を ADDRESS_RENAME_WORD_MAP の単語に置き換えます

- ADDRESS_RENAME_DELIMITER_MAP を使用する RENAME_DELIMITERS = Address 文字列の区切り文字を ADDRESS_RENAME_DELIMITER_MAP の文字列に置き換えます
- ADDRESS_RENAME_DIRECTION_MAP を使用した RENAME_DIRECTIONS= アドレス文字列の区切り文字を ADDRESS_RENAME_DIRECTION_MAP の文字列に置き換えます
- ADDRESS_RENAME_NUMBER_MAP を使用する RENAME_NUMBERS = Address 文字列の数値を ADDRESS_RENAME_NUMBER_MAP の文字列に置き換えます
- ADDRESS_RENAME_ Special_CHAR_MAP を使用する RENAME_ Special_CHARS = Address 文字列の特殊文字を ADDRESS_RENAME_ Special_CHAR_MAP の文字列に置き換えます

ADDRESS_RENAME_WORD_MAP

これらは、アドレス文字列を正規化するときに名前が変更される単語です。

```
"avenue": "ave",
 "bouled": "blvd",
 "circle": "cir",
 "circles": "cirs",
 "court": "ct",
 "centre": "ctr",
 "center": "ctr",
 "drive": "dr",
 "freeway": "fwy",
 "frwy": "fwy",
 "highway": "hwy",
 "lane": "ln",
 "parks": "park",
 "parkways": "pkwy",
 "pky": "pkwy",
 "pkway": "pkwy",
 "pkwys": "pkwy",
 "parkway": "pkwy",
 "parkwy": "pkwy",
 "place": "pl",
 "plaza": "plz",
 "plza": "plz",
 "road": "rd",
 "square": "sq",
 "squ": "sq",
 "sqr": "sq",
 "street": "st",
 "str": "st",
```

```
 "str.": "strasse"
```

ADDRESS_RENAME_DELIMITER_MAP

これらは、アドレス文字列を正規化するときに名前が変更される区切り文字です。

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

ADDRESS_RENAME_DIRECTION_MAP

これらは、アドレス文字列を正規化するときに名前が変更される方向識別子です。

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

ADDRESS_RENAME_NUMBER_MAP

これらは、アドレス文字列を正規化するときに名前が変更される数値文字列です。

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

ADDRESS_RENAME_SPECIAL_CHAR_MAP

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

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

ハッシュ

- TRIM = 先頭と末尾の空白をトリミングする

Source_ID

- TRIM = 先頭と末尾の空白をトリミングする

正規化 (ApplyNormalization) – ML ベースのみ

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、余分なスペースと特殊文字を削除し、小文字の形式に標準化することで、データを標準化します。

たとえば、入力フィールドの属性タイプが でNAME、入力テーブルの値が の形式である場合Johns Smith、 AWS Entity Resolution は値を に正規化しますjohn smith。

以下のセクションでは、機械学習ベースのマッチングワークフローの正規化ルールについて説明します。

トピック

- 名前
- E メール
- 電話

名前

- TRIM = 先頭と末尾の空白をトリミングする
- LOWERCASE = すべてのアルファ文字を小文字にします

E メール

- LOWERCASE = すべてのアルファ文字を小文字にします
- (at)(大文字と小文字を区別) のみを @ 記号に置き換えます
- 値内の任意の場所にあるすべての空白を削除します。
- 存在する"<>"場合、最初の の外部にあるものをすべて削除します

電話

- TRIM = 先頭と末尾の空白をトリミングする
- REMOVE_ALL_NON_NUMERIC = 数値以外の文字をすべて削除します [0-9]
- REMOVE_ALL_LEADING_ZEROES = 先頭のゼロをすべて削除します
- EN"_PREFIX_WITH_MAP, "phonePrefixMap" = 各電話番号を調べ、phonePrefixMap のパターンと照合しようとします。一致が見つかった場合、ルールは電話番号のプレフィックスを追加または変更して、マップで指定された標準化された形式に準拠していることを確認します。

One-to-Oneマッチング

One-to-one のマッチングは、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、 mobile_phoneや など、同じ一致キー「Phonehome_phone」を持つ複数の電話番号入力フィールドがあるとします。one-to-oneのマッチングを使用して、mobile_phone入力フィールド内のデータとmobile_phone入力フィールド内のデータを比較し、home_phone入力フィールド内のデータとhome_phone入力フィールド内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 がhome_phone一致すると、「電話」一致キーは一致を返します。一致を見つけるための一致キー「Phone」の場合は、Record One mobile_phone = Record Two mobile_phoneまたは Record One home_phone = Record Two home_phone。

一致ルールは、 (および) オペレーションを使用して、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ングキーを作成できます。

ルールで両方の一致キーを使用して一致を検索する場合は、 `Record One mobile_phone = Record Two mobile_phone` AND `Record One home_phone = Record Two home_phone`。

Output

OutputAttribute オブジェクトのリスト。各オブジェクトには名前とハッシュ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。

OutputS3Path

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

OutputSourceConfig

OutputSource オブジェクトのリスト。各オブジェクトには OutputS3PathApplyNormalization、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とライセンスされた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、次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、ウォーターフォールマッチングルールの階層的なセットであり、入力したデータに基づいて提案され AWS Entity Resolution、ユーザーが完全に設定可能です。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。

たとえば、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見つけるには、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

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

スキーマの説明

入力できるスキーマのオプションの説明。説明は、スキーママッピングを複数作成する場合に、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 に指示するプロセスです。一致するワークフローに AWS Entity Resolution 読み込む入力データテーブルのスキーマを定義します。

スキーママッピング ARN

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

一意の ID

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

Example

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

一意の ID 列は必須です。

一意の ID は、単一のテーブル内の一意の識別子である必要があります。

一意の ID は、次のパターンを満たす必要があります。 `[a-zA-Z0-9_-]`

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 が次の場合、レコードは拒否されます。

- が指定されていません
- は同じテーブル内で一意ではありません
- は、ソース間で属性名の点で重複しています。
- が 38 文字を超えています (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。