Guide de l’utilisateur

Résolution des entités AWS

Résolution des entités AWS: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est Résolution des entités AWS ?

Résolution des entités AWS est un service qui vous permet de faire correspondre, de lier et d'améliorer les enregistrements connexes stockés dans de multiples applications, canaux et magasins de données. Vous pouvez commencer à utiliser des flux de travail de résolution d'entités flexibles, évolutifs et capables de vous connecter à vos applications et fournisseurs de services de données existants.

Résolution des entités AWS propose des techniques de correspondance avancées, telles que la correspondance basée sur des règles, la correspondance basée sur l'apprentissage automatique (correspondance ML) et la correspondance dirigée par le fournisseur de services de données. Ces techniques peuvent vous aider à relier et à améliorer plus précisément les enregistrements connexes d'informations sur les clients, de codes de produits ou de codes de données commerciales.

Vous pouvez l'utiliser Résolution des entités AWS pour créer une vue unifiée des interactions avec les clients en associant les événements récents (tels que les clics sur les annonces, les abandons de panier et les achats) aux signaux pseudonymisés de vos fournisseurs de services de données sous forme d'un identifiant d'entité unique. Vous pouvez également mieux suivre les produits qui utilisent des codes différents (par exempleSKU,UPC) dans vos boutiques. Vous pouvez l'utiliser Résolution des entités AWS pour contrôler la précision des correspondances et mieux protéger la sécurité des données tout en minimisant les mouvements de données.

Rubriques

Vous en êtes un Résolution des entités AWS utilisateur pour la première fois ?

Si vous utilisez pour la première fois Résolution des entités AWS, nous vous recommandons de commencer par lire les sections suivantes :

- Caractéristiques de Résolution des entités AWS

- Accès Résolution des entités AWS
- Configurez Résolution des entités AWS

Caractéristiques de Résolution des entités AWS

Résolution des entités AWS inclut les fonctionnalités suivantes :

- Préparation des données flexible et personnalisable

  Résolution des entités AWS lit vos données AWS Glue pour les utiliser comme entrées pour le traitement des correspondances. Vous pouvez spécifier un maximum de 20 entrées de données. Résolution des entités AWS traite chaque ligne de la table d'entrée de données comme un enregistrement, une entité unique servant de clé primaire. Résolution des entités AWS peut fonctionner sur des ensembles de données chiffrés. Définissez d'abord le mappage du schéma Résolution des entités AWS pour comprendre quels champs de saisie vous souhaitez utiliser dans votre flux de travail correspondant. Vous pouvez apporter votre propre schéma de données, ou plan, à partir d'une entrée de AWS Glue données existante. Vous pouvez également créer votre schéma personnalisé à l'aide d'une interface utilisateur interactive ou d'un JSON éditeur. Par défaut, normalise Résolution des entités AWS également les entrées de données avant la mise en correspondance afin d'améliorer le traitement des correspondances, par exemple en supprimant les caractères spéciaux et les espaces supplémentaires, et en formatant le texte en minuscules. Si votre saisie de données est déjà normalisée, vous pouvez désactiver la normalisation. Nous fournissons également une GitHub bibliothèque que vous pouvez utiliser pour personnaliser davantage le processus de normalisation des données en fonction de vos besoins.
- Flux de travail configurables correspondant aux entités

  Un flux de travail de correspondance d'entités est une séquence d'étapes que vous configurez pour indiquer Résolution des entités AWS comment faire correspondre vos données d'entrée et où écrire les données de sortie consolidées. Vous pouvez configurer un ou plusieurs flux de travail de correspondance pour comparer différentes entrées de données et utiliser différentes techniques de correspondance, telles que la correspondance basée sur des règles, la correspondance par apprentissage automatique ou la correspondance dirigée par le fournisseur de services de données sans aucune expérience en matière de résolution d'entités ni d'apprentissage automatique. Vous pouvez également consulter l'état des tâches des flux de travail correspondants et des indicateurs existants, tels que le nombre de ressources, le nombre d'enregistrements traités et le nombre de correspondances trouvées.

  - Correspondance basée sur des eady-to-use règles R

Cette technique de correspondance inclut un ensemble de ready-to-use règles dans le AWS Management Console ou AWS Command Line Interface (AWS CLI). Vous pouvez utiliser ces règles pour rechercher des enregistrements connexes en fonction de vos champs de saisie. Vous pouvez également personnaliser les règles en ajoutant ou en supprimant des champs de saisie pour chaque règle, en supprimant des règles, en réorganisant la priorité des règles et en créant de nouvelles règles. Vous pouvez également réinitialiser les règles pour rétablir leur configuration d'origine. Les données de sortie de votre compartiment Amazon Simple Storage Service (Amazon S3) contiennent des groupes Résolution des entités AWS de correspondance générés à l'aide de la technique de correspondance basée sur des règles. Chaque groupe de match possède le numéro de règle utilisé pour générer cette correspondance qui lui est associé afin de vous aider à comprendre la correspondance. Par exemple, le numéro de règle peut démontrer la précision de chaque groupe de correspondance, de telle sorte que la première règle soit plus précise que la règle deux.

- Correspondance préconfigurée basée sur l'apprentissage automatique (correspondance ML)

  Cette technique de correspondance inclut un modèle de machine learning préconfiguré pour trouver des correspondances entre toutes vos entrées de données, en particulier les enregistrements basés sur les consommateurs. Le modèle utilise tous les champs de saisie associés au nom, à l'adresse e-mail, au numéro de téléphone, à l'adresse et aux types de données de date de naissance. Le modèle génère des groupes de correspondance d'enregistrements connexes avec un score de confiance dans chaque groupe expliquant la qualité de la correspondance par rapport aux autres groupes de correspondance. Le modèle prend en compte les champs de saisie manquants et analyse l'ensemble de l'enregistrement pour représenter une entité. Les données de sortie de votre compartiment Amazon S3 contiennent des groupes de correspondance Résolution des entités AWS générés à l'aide de la correspondance ML. C'est là que chaque groupe de correspondance est associé à un score de confiance de 0,0-1,0, qui indique la précision de la correspondance.

- Mise en correspondance des enregistrements avec les fournisseurs de services de données

  Résolution des entités AWS Vous pouvez ainsi associer, lier et améliorer vos enregistrements avec ceux des principaux fournisseurs de services de données et des ensembles de données sous licence afin de renforcer votre capacité à comprendre, atteindre et servir vos clients. Par exemple, vous pouvez ajouter des attributs à vos données pour améliorer vos enregistrements, ou vous pouvez améliorer l'interopérabilité des systèmes et des plateformes avec lesquels vous travaillez pour atteindre vos objectifs commerciaux. Vous pouvez utiliser ce flux de travail correspondant en quelques clics, ce qui vous évite de devoir créer et gérer des intégrations

propriétaires complexes. Vous devez avoir un contrat de licence avec ces fournisseurs de services de données pour tirer parti de cette technique de mise en correspondance.

- Traitement manuel en vrac et traitement incrémentiel automatique

  Vous pouvez utiliser le traitement des données pour convertir vos entrées ou entrées de données en une table de sortie de données consolidée contenant des enregistrements similaires dotés d'un identifiant de correspondance commun généré à l'aide de configurations de flux de travail de correspondance d'entités. À l'aide du API et AWS Management Console ou du AWS CLI, vous pouvez exécuter un traitement manuel en masse à la demande, sur la base de votre pipeline de données d'extraction, de transformation et de chargement (ETL) existant, qui retraite toutes les données pour toute nouvelle correspondance et mise à jour des correspondances existantes. En outre, pour les scénarios de correspondance basés sur des règles, vous pouvez lancer un traitement incrémentiel automatique afin que, dès que de nouvelles données sont disponibles dans votre compartiment Amazon S3, le service lise ces nouveaux enregistrements et les compare aux enregistrements existants. Cela permet de tenir vos correspondances à jour en fonction de toute modification apportée aux données Amazon S3.

- Recherche en temps quasi réel

  La recherche de n'importe quel champ d'entité par le biais de l'Résolution des entités AWS GetMatchId APIopération vous permet de récupérer de manière synchrone un identifiant de match existant. Vous pouvez appeler Résolution des entités AWS avec des informations personnellement identifiables (PII), des attributs obtenus par le biais de différentes sources et canaux. Résolution des entités AWS hache ces attributs à des fins de protection des données et récupère l'ID de correspondance correspondant pour lier et associer le client. Par exemple, vous pouvez vous inscrire sur le Web avec un nom, une adresse e-mail et une adresse postale associés. Utilisez cette Résolution des entités AWS GetMatchId API opération pour savoir si ce client ou cette entité existe déjà dans vos résultats correspondants stockés dans votre compartiment S3, ainsi que l'ID de correspondance d'entité correspondant qui lui est associé. Une fois que vous avez obtenu l'identifiant de correspondance de l'entité, vous pouvez trouver les informations transactionnelles qui y sont associées dans vos applications sources, telles que vos systèmes de gestion de la relation client (CRM) ou de plateforme de données clients (CDP).

- Protection des données et régionalisation dès la conception

  Résolution des entités AWS propose une fonctionnalité de chiffrement par défaut qui peut vous aider à protéger vos données et vous fournit une clé de chiffrement pour chaque entrée de données dans le service. Par exemple, vous Résolution des entités AWS donne la flexibilité d'intégrer des données chiffrées et hachées côté serveur pour exécuter des flux de travail

de correspondance basés sur des règles. Résolution des entités AWS prend en charge la régionalisation, ce qui signifie que vos flux de travail correspondants sont exécutés pour traiter vos données Région AWS de la même manière que celle où vous utilisez le service. Vous pouvez également chiffrer et hacher les données de sortie dans Amazon S3 avant d'utiliser vos données résolues dans d'autres applications.

- Transcodage multipartite

  Résolution des entités AWS vous aide à définir vos sources de données et à faire correspondre les configurations entre plusieurs parties souhaitant utiliser une collaboration de données, comme dans AWS Clean Rooms.

Services connexes

Les éléments suivants Services AWS sont liés à Résolution des entités AWS :

- Amazon S3

  Stockez les données que vous importez Résolution des entités AWS dans Amazon S3.

  Pour plus d'informations, consultez Qu'est-ce qu'Amazon S3 ? dans le guide de l'utilisateur d'Amazon Simple Storage Service.

- AWS Glue

  Créez des AWS Glue tables à partir de vos données dans Amazon S3 pour les utiliser dans Résolution des entités AWS.

  Pour plus d'informations, voir Qu'est-ce que c'est AWS Glue ? dans le Guide AWS Glue du développeur.

- AWS CloudTrail

  Résolution des entités AWS Utilisez-le avec CloudTrail les journaux pour améliorer votre analyse de Service AWS l'activité.

  Pour de plus amples informations, veuillez consulter Journalisation des appels Résolution des entités AWS d'API à l'aide AWS CloudTrail.

- AWS CloudFormation

Créez les ressources suivantes dans AWS CloudFormation : AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace et AWS::EntityResolution::PolicyStatement

Pour de plus amples informations, veuillez consulter Créez des ressources de résolution d'AWSentités avec AWS CloudFormation.

Accès Résolution des entités AWS

Vous pouvez y accéder Résolution des entités AWS par le biais des options suivantes :

- Directement via la Résolution des entités AWS console à l'adresse https://console.aws.amazon.com/entityresolution/.
- Programmatiquement par le biais du. Résolution des entités AWS API Pour plus d'informations, consultez la Résolution des entités AWS APIréférence.
  - Si vous prévoyez d'appeler le Résolution des entités AWS API dans AWS Lambda Runtime, créez votre propre package de déploiement et incluez la version souhaitée de la AWS SDK bibliothèque. Pour plus d'informations, consultez les exemples suivants dans le guide du AWS Lambda développeur :
    - Déployez des fonctions Java Lambda avec des archives .zip ou de fichiers JAR
    - Utilisation d'archives de fichiers .zip pour les fonctions Lambda en Python

Tarification pour Résolution des entités AWS

Pour de plus amples informations sur la tarification, veuillez consulter Résolution des entités AWS Pricing (français non garanti).

Configurez Résolution des entités AWS

Avant de l'utiliser Résolution des entités AWS pour la première fois, inscrivez-vous AWS et créez un utilisateur administrateur pour créer des rôles.

S'inscrire à AWS

Si vous en avez déjà un Compte AWS, ignorez cette étape.

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

Création d'un utilisateur administrateur

Afin de créer un utilisateur administrateur, choisissez l'une des options suivantes :

Choisissez un moyen de gérer votre administrateur	Pour	Par	Vous pouvez également
Dans IAM Identity Center (Recommandé)	Utiliser des identifiants à court terme pour accéder à AWS. Telles sont les meilleures pratiques en matière de sécurité. Pour plus d'informations sur les meilleures pratiques, consultez la section Bonnes pratiques en matière de sécurité IAM dans le guide de IAM l'utilisateur.	Suivre les instructions de la section Mise en route dans le AWS IAM Identity Center Guide de l'utilisateur.	Configurez l'accès par programmation en configurant le AWS CLI à utiliser AWS IAM Identity Center dans le guide de l'AWS Command Line Interface utilisateur.
Dans IAM (Non recommandé)	Utiliser des identifiants à long terme pour accéder à AWS.	Suivez les instructions de la section Créer un IAM utilisateur pour un accès d'urgence dans le guide de IAM l'utilisateur.	Configurez l'accès programmatique en gérant les clés d'accès pour IAM les utilisateurs dans le guide de IAM l'utilisateur.

Création d'un IAM rôle pour un utilisateur de console

Effectuez la procédure suivante si vous utilisez la Résolution des entités AWS console.

Pour créer un rôle IAM

1. Connectez-vous à la IAM console (https://console.aws.amazon.com/iam/) avec votre compte administrateur.
2. Sous Access Management (Gestion des accès), choisissez Roles (Rôles).

   Vous pouvez utiliser les rôles pour créer des informations d'identification à court terme, ce qui est recommandé pour renforcer la sécurité. Vous pouvez également sélectionner Utilisateurs pour créer des informations d'identification à long terme.
3. Sélectionnez Créer un rôle.
4. Dans l'assistant de création de rôle, pour Type d'entité fiable, sélectionnez Compte AWS.
5. Conservez l'option Ce compte sélectionnée, puis choisissez Suivant.
6. Pour Ajouter des autorisations, choisissez Create Policy.

   Un nouvel onglet s'ouvre.

   a. Sélectionnez l'JSONonglet, puis ajoutez des politiques en fonction des capacités accordées à l'utilisateur de la console. Résolution des entités AWS propose les politiques gérées suivantes basées sur des cas d'utilisation courants :

      - AWS politique gérée : AWSEntityResolutionConsoleFullAccess
      - AWS politique gérée : AWSEntityResolutionConsoleReadOnlyAccess

   b. Choisissez Suivant : Balises, ajoutez des balises (facultatif), puis choisissez Suivant : Révision.

   c. Pour la politique de révision, entrez un nom et une description, puis consultez le résumé.

   d. Choisissez Create Policy (Créer une politique).

      Vous avez créé une politique pour un membre de la collaboration.

   e. Retournez à votre onglet d'origine et sous Ajouter des autorisations, entrez le nom de la politique que vous venez de créer. (Vous devrez peut-être recharger la page.)

   f. Cochez la case à côté du nom de la politique que vous avez créée, puis choisissez Next.
7. Dans Nom, révision et création, entrez le nom et la description du rôle.

   a. Passez en revue Sélectionnez les entités de confiance, saisissez le Compte AWS nom de la ou des personnes qui assumeront le rôle (si nécessaire).

b. Passez en revue les autorisations dans Ajouter des autorisations et modifiez-les si nécessaire.

c. Passez en revue les balises et ajoutez-y des balises si nécessaire.

d. Sélectionnez Créer un rôle.

Création d'un rôle de travail dans le flux de travail pour Résolution des entités AWS

Résolution des entités AWS utilise un rôle de tâche de flux de travail pour exécuter un flux de travail. Vous pouvez créer ce rôle à l'aide de la console si vous disposez des IAM autorisations nécessaires. Si vous n'êtes pas `CreateRole` autorisé, demandez à votre administrateur de créer le rôle.

Pour créer un rôle de travail dans le flux de travail pour Résolution des entités AWS

1. Connectez-vous à la IAM console à l'https://console.aws.amazon.com/iam/aide de votre compte administrateur.
2. Sous Access Management (Gestion des accès), choisissez Roles (Rôles).

   Vous pouvez utiliser les rôles pour créer des informations d'identification à court terme, ce qui est recommandé pour renforcer la sécurité. Vous pouvez également sélectionner Utilisateurs pour créer des informations d'identification à long terme.
3. Sélectionnez Créer un rôle.
4. Dans l'assistant de création de rôle, pour Type d'entité fiable, choisissez Politique de confiance personnalisée.
5. Copiez et collez la politique de confiance personnalisée suivante dans l'JSONéditeur.

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

```
        }
    ]
}
```

6. Choisissez Suivant.
7. Pour Ajouter des autorisations, choisissez Create Policy.

   Un nouvel onglet apparaît.

   a. Copiez et collez la politique suivante dans l'JSONéditeur.

> **Note**
>
> L'exemple de politique suivant prend en charge les autorisations nécessaires pour lire les ressources de données correspondantes, telles qu'Amazon S3 et AWS Glue. Toutefois, il se peut que vous deviez modifier cette politique en fonction de la manière dont vous avez configuré vos sources de données.
> Vos AWS Glue ressources et les ressources Amazon S3 sous-jacentes doivent être identiques Région AWS à Résolution des entités AWS.
> Il n'est pas nécessaire d'accorder AWS KMS des autorisations si vos sources de données ne sont ni chiffrées ni déchiffrées.

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

```
}
```

Remplacez chacun *{{user input placeholder}}* avec vos propres informations.

aws-region	Région AWS de vos ressources. Vos AWS Glue ressources, les ressources sous-jacentes d'Amazon S3 et les AWS KMS ressources doivent être identiques Région AWS à`Résolution des entités AWS` .
accountId	Votre Compte AWS carte d'identité.
input-buckets	Des compartiments Amazon S3 qui contiennent les objets de données sous-jacents de AWS Glue Where `Résolution des entités AWS` will read from.
output-buckets	Des compartiments Amazon S3 dans lesquels `Résolution des entités AWS` seront générées les données de sortie.
input-databases	AWS Glue bases de données d'où je `Résolution des entités AWS` vais lire.

b. (Facultatif) Si le compartiment Amazon S3 d'entrée est chiffré à l'aide de la KMS clé du client, ajoutez ce qui suit :

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

Remplacez chacun *{{user input placeholder}}* avec vos propres informations.

aws-region	Région AWS de vos ressources. Vos AWS Glue ressources, les ressources sous-jacentes d'Amazon S3 et les AWS KMS ressources doivent être identiques Région AWS à`Résolution des entités AWS` .
accountId	Votre Compte AWS carte d'identité.
inputKeys	Clés gérées entrées AWS Key Management Service. Si vos sources d'entrée sont cryptées, vous `Résolution des entités AWS` devez déchiffrer vos données à l'aide de votre clé.

c. (Facultatif) Si les données écrites dans le compartiment Amazon S3 de sortie doivent être chiffrées, ajoutez ce qui suit :

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

Remplacez chacun *{{user input placeholder}}* avec vos propres informations.

aws-region	Région AWS de vos ressources. Vos AWS Glue ressources, les ressources sous-jacentes d'Amazon S3 et les AWS KMS ressources doivent être identiques Région AWS à`Résolution des entités AWS` .

accountId	Votre Compte AWS carte d'identité.
outputKeys	Clés gérées entrées AWS Key Management Service. Si vous avez besoin de chiffrer vos sources de sortie, vous `Résolution des entités AWS` devez chiffrer les données de sortie à l'aide de votre clé.

d. (Facultatif) Si vous avez souscrit un abonnement auprès d'un fournisseur de services et que vous souhaitez utiliser un rôle existant pour un flux de travail basé sur les services du fournisseur, ajoutez ce qui suit : AWS Data Exchange

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

Remplacez chacun *{{user input placeholder}}* avec vos propres informations.

aws-region	L' Région AWS endroit où la ressource du fournisseur est accordée. Vous pouvez trouver cette valeur dans l'actif ARN de la AWS Data Exchange console. Par exemple : `arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc64444examplef3bc15cf0b2346b/assets/546468b8dexamplea37bfc73b8f79fefa`
datasetId	L'ID de l'ensemble de données, qui se trouve sur la AWS Data Exchange console.

revisionId	Révision de l'ensemble de données, disponible sur la AWS Data Exchange console.
assetId	L'ID de la ressource, qui se trouve sur la AWS Data Exchange console.

8. Retournez à votre onglet d'origine et sous Ajouter des autorisations, entrez le nom de la politique que vous venez de créer. (Vous devrez peut-être recharger la page.)
9. Cochez la case à côté du nom de la politique que vous avez créée, puis choisissez Next.
10. Dans Nom, révision et création, entrez le nom et la description du rôle.

> **Note**
>
> Le nom du rôle doit correspondre au modèle des `passRole` autorisations accordées au membre qui peut les transmettre `workflow job role` pour créer un flux de travail correspondant.
> Par exemple, si vous utilisez la politique `AWSEntityResolutionConsoleFullAccess` gérée, n'oubliez pas de l'inclure `entityresolution` dans le nom de votre rôle.

    a. Passez en revue Sélectionnez les entités fiables et modifiez-les si nécessaire.
    b. Passez en revue les autorisations dans Ajouter des autorisations et modifiez-les si nécessaire.
    c. Passez en revue les balises et ajoutez-y des balises si nécessaire.
    d. Sélectionnez Créer un rôle.

Le rôle de tâche de flux de travail pour Résolution des entités AWS a été créé.

Préparer des tableaux de données d'entrée

Entrée Résolution des entités AWS, chacune de vos tables de données d'entrée contient des enregistrements source. Ces dossiers contiennent des identifiants de consommateurs tels que le prénom, le nom de famille, l'adresse e-mail ou le numéro de téléphone. Ces enregistrements source peuvent être mis en correspondance avec d'autres enregistrements source que vous fournissez dans la même table de données ou dans d'autres tables de données d'entrée. Chaque enregistrement doit avoir un identifiant d'enregistrement unique (Identifiant unique) et vous devez le définir comme clé primaire lors de la création d'un mappage de schéma dans Résolution des entités AWS.

Chaque tableau de données d'entrée est disponible sous forme de AWS Glue table soutenue par Amazon S3. Vous pouvez utiliser vos données de première partie déjà présentes dans Amazon S3 ou importer des tables de données provenant d'autres fournisseurs de SaaS tiers dans Amazon S3. Après avoir chargé les données sur Amazon S3, vous pouvez utiliser un AWS Glue crawler pour créer une table de données dans le AWS Glue Data Catalog. Vous pouvez ensuite utiliser le tableau de données comme entrée pour Résolution des entités AWS.

Les sections suivantes décrivent comment préparer des données de première partie et des données de tiers.

Rubriques

Préparation des données d'entrée de première partie

Les étapes suivantes décrivent comment préparer des données de première partie à utiliser dans un flux de travail de correspondance basé sur des règles, un flux de travail de correspondance basé sur le machine learning ou un flux de travail de mappage d'identifiants.

Étape 1 : Enregistrez votre tableau de données d'entrée dans un format de données pris en charge

Si vous avez déjà enregistré vos données d'entrée internes dans un format de données pris en charge, vous pouvez ignorer cette étape.

Pour utiliser Résolution des entités AWS, les données d'entrée doivent être dans un format qui Résolution des entités AWS soutient. Résolution des entités AWS prend en charge les formats de données suivants :

- valeur séparée par des virgules () CSV
- Parquet

Étape 2 : Chargez votre table de données d'entrée sur Amazon S3

Si vous disposez déjà de votre table de données propriétaire dans Amazon S3, vous pouvez ignorer cette étape.

> **Note**
>
> Les données d'entrée doivent être stockées dans Amazon Simple Storage Service (Amazon S3) dans le même Compte AWS and Région AWS dans lequel vous souhaitez exécuter le flux de travail correspondant.

Pour télécharger votre tableau de données d'entrée sur Amazon S3

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Buckets, puis choisissez un bucket pour stocker votre table de données.
3. Choisissez Upload, puis suivez les instructions.
4. Choisissez l'onglet Objets pour afficher le préfixe dans lequel vos données sont stockées. Notez le nom du dossier.

   Vous pouvez sélectionner le dossier pour afficher le tableau de données.

Étape 3 : Création d'un AWS Glue table

Les données d'entrée dans Amazon S3 doivent être cataloguées dans AWS Glue et représenté sous la forme d'un AWS Glue table. Pour plus d'informations sur la création d'un AWS Glue tableau avec Amazon S3 en entrée, voir Travailler avec des robots d'exploration sur le AWS Glue console dans le AWS Glue Guide du développeur.

> **Note**
>
> Résolution des entités AWS ne prend pas en charge les tables partitionnées.

Au cours de cette étape, vous allez configurer un crawler dans AWS Glue qui analyse tous les fichiers de votre compartiment S3 et crée un AWS Glue table.

> **Note**
>
> Résolution des entités AWS ne prend actuellement pas en charge les sites Amazon S3 enregistrés auprès de AWS Lake Formation.

Pour créer un AWS Glue table

1. Connectez-vous au AWS Management Console et ouvrez le AWS Glue console à https://console.aws.amazon.com/glue/.
2. Dans la barre de navigation, sélectionnez Crawlers.
3. Sélectionnez votre compartiment S3 dans la liste, puis choisissez Ajouter un robot d'exploration.
4. Sur la page Ajouter un robot d'exploration, entrez un nom de robot, puis choisissez Suivant.
5. Parcourez la page Ajouter un robot d'exploration en spécifiant les détails.
6. Sur la page Choisir un IAM rôle, choisissez Choisir un IAM rôle existant, puis cliquez sur Suivant.

   Vous pouvez également choisir Créer un IAM rôle ou demander à votre administrateur de créer le IAM rôle si nécessaire.
7. Pour Créer un calendrier pour ce robot d'exploration, conservez la fréquence par défaut (Exécuter à la demande), puis choisissez Next.
8. Pour Configurer la sortie du robot d'exploration, entrez AWS Glue base de données, puis choisissez Next.
9. Vérifiez tous les détails, puis choisissez Terminer.
10. Sur la page Crawlers, cochez la case à côté de votre compartiment S3, puis choisissez Run crawler.
11. Une fois que le crawler a fini de fonctionner, sur le AWS Glue dans la barre de navigation, choisissez Bases de données, puis choisissez le nom de votre base de données.
12. Sur la page Base de données, sélectionnez Tables dans {nom de votre base de données}.

a. Consultez les tableaux dans le AWS Glue base de données.
b. Pour afficher le schéma d'une table, sélectionnez une table spécifique.
c. Prenez note du AWS Glue nom de la base de données et AWS Glue nom de la table.

Vous êtes maintenant prêt à créer un mappage de schéma. Pour de plus amples informations, veuillez consulter Création d'un mappage de schéma.

Préparation de données d'entrée tierces

Les services de données tiers fournissent des identifiants qui peuvent être mis en correspondance avec vos identifiants connus.

Résolution des entités AWS prend actuellement en charge les services de fournisseurs de données tiers suivants :

Services de fournisseurs de données

Nom de l'entreprise	Disponible Régions AWS	Identifiant
LiveRamp	USA Est (Virginie du Nord) (us-east-1), USA Est (Ohio) (us-east-2) et USA Ouest (Oregon) (us-west-2)	Identifiant de la rampe
TransUnion	USA Est (Virginie du Nord) (us-east-1), USA Est (Ohio) (us-east-2) et USA Ouest (Oregon) (us-west-2)	TransUnion Individuel et ménage IDs
Unified ID 2.0	USA Est (Virginie du Nord) (us-east-1), USA Est (Ohio) (us-east-2) et USA Ouest (Oregon) (us-west-2)	brut UID 2

Les étapes suivantes décrivent comment préparer des données tierces pour utiliser un flux de travail de correspondance basé sur le service du fournisseur ou un flux de travail de mappage des identifiants basé sur le service du fournisseur.

Rubriques

Étape 1 : Abonnez-vous à un service fournisseur sur AWS Data Exchange

Si vous avez souscrit un abonnement auprès d'un fournisseur de services via AWS Data Exchange, vous pouvez exécuter un flux de travail de mise en correspondance avec l'un des fournisseurs de services suivants afin de faire correspondre vos identifiants connus à ceux de votre fournisseur préféré. Vos données seront mises en correspondance avec un ensemble d'entrées définies par votre fournisseur préféré.

Pour souscrire au service d'un fournisseur sur AWS Data Exchange

1. Consultez la liste des fournisseurs sur AWS Data Exchange. Les listes de fournisseurs suivantes sont disponibles :

   - LiveRamp
     - LiveRampRésolution d'identité
     - LiveRampTranscodage
   - TransUnion
     - TransUnion TruAudience Résolution et enrichissement de l'identité sans transfert
     - TransUnion TruAudience Résolution d'identité sans transfert
   - Unified ID 2.0
     - Résolution d'identité Unified ID 2.0
2. Effectuez l'une des étapes suivantes, en fonction de votre type d'offre.

   - Offre privée — Si vous entretenez déjà une relation avec un fournisseur, suivez la procédure relative aux produits et offres privés dans le AWS Data Exchange Guide de l'utilisateur pour accepter une offre privée sur AWS Data Exchange.
   - Apportez votre propre abonnement — Si vous avez déjà un abonnement de données auprès d'un fournisseur, suivez la procédure relative aux offres Bring Your Own Subscription (BYOS)

décrite dans le AWS Data Exchange Guide de l'utilisateur pour accepter une BYOS offre sur AWS Data Exchange.

3. Après avoir souscrit à un service de fournisseur sur AWS Data Exchange, vous pouvez ensuite créer un flux de travail correspondant ou un flux de travail de mappage d'identifiants avec ce service fournisseur.

Pour plus d'informations sur la façon d'accéder à un produit fournisseur contenantAPIs, voir Accès à un API produit dans le AWS Data Exchange Guide de l'utilisateur

Étape 2 : Préparation de tables de données tierces

Chaque service tiers dispose d'un ensemble différent de recommandations et de directives pour garantir un flux de travail de correspondance réussi.

Pour préparer des tableaux de données tiers, consultez le tableau suivant :

Directives relatives aux services des fournisseurs de données

Service du fournisseur	Vous avez besoin d'un identifiant unique ?	Actions
LiveRamp	Oui	Vérifiez les points suivants : • L'identifiant unique peut être votre propre identifiant pseudonyme ou un identifiant de ligne. • Le format et la normalisation de votre fichier d'entrée de données sont conformes aux LiveRamp directives. Pour plus d'informations sur les directives de formatage des fichiers d'entrée pour le flux de travail correspondant, voir Perform Identity Resolution ADX Through dans la LiveRamp documentation. Pour plus d'informations sur les directive s de formatage des fichiers d'entrée pour le flux de travail de mappage d'identifiants,

Service du fournisseur	Vous avez besoin d'un identifiant unique ?	Actions
		voir Perform Transcoding Through ADX dans la LiveRamp documentation.

Service du fournisseur	Vous avez besoin d'un identifiant unique ?	Actions

TransUnion	Oui	Vérifiez les points suivants :
		• Il existe un identifiant unique pour l'enrichissement TransUnion des données.
		Note
		Les attributs de transmission sont autorisés à persister en entrée et en sortie vers TransUnion. Les touches E domestiques HHID sont spécifiques à l'espace de noms du client.
		• **`Phone number`** doit comporter 10 chiffres, sans caractères spéciaux tels que des espaces ou des tirets.
		• **`Addresses`** doit être scindé en
		  • une seule ligne d'adresse (combinez les lignes d'adresse 1 et 2, le cas échéant)
		  • city
		  • zip (ou zip plus4), sans caractères spéciaux tels que des espaces ou des tirets
		  • État, spécifié sous la forme d'un code à 2 lettres 3
		• **`Email addresses`** doit être en texte clair.
		• **`First Name`** peuvent être en minuscules ou en majuscules, les surnoms sont pris en charge, mais les titres et suffixes doivent être exclus.

Service du fournisseur	Vous avez besoin d'un identifiant unique ?	Actions
		• **`Last Name`**peuvent être en minuscules ou en majuscules, les initiales du milieu étant exclues.

Service du fournisseur	Vous avez besoin d'un identifiant unique ?	Actions
Unified ID 2.0	Oui	Vérifiez les points suivants : • L'identifiant unique ne peut pas être un hachage. • UID2prend en charge à la fois le courrier électronique et le numéro de téléphone pour UID2 la génération. Toutefois, si les deux valeurs sont présentes dans le mappage du schéma, le flux de travail duplique chaque enregistrement de la sortie. Un enregistrement utilise l'e-mail pour la UID2 génération et le second un numéro de téléphone. Si vos données incluent un mélange d'e-mails et de numéros de téléphone et que vous ne souhaitez pas que ces enregistrements soient dupliqués dans la sortie, la meilleure approche consiste à créer un flux de travail distinct pour chacun, avec des mappages de schéma distincts. Dans ce scénario, suivez les étapes deux fois : créez un flux de travail pour les e-mails et un autre pour les numéros de téléphone. **Note** Un e-mail ou un numéro de téléphone spécifique, à un moment donné, donne la même UID2 valeur brute, quelle que soit la personne qui a fait la demande. UID2sLes produits bruts sont créés en ajoutant des sels provenant de seaux

Service du fournisseur	Vous avez besoin d'un identifiant unique ?	Actions
		à sel qui sont alternés environ une fois par an, ce qui permet de UID2 faire également tourner le brut avec celui-ci. Les différents seaux à sel changent à différents moments de l'année. Résolution des entités AWS ne tient actuellement pas compte de la rotation des seaux à sel et du sel brutUID2s. Il est donc recommand é de régénérer le sel brut UID2s tous les jours. Pour plus d'informa tions, voir À quelle fréquence faut-il actualiser les mises UID2s à jour pour les mises à jour incrémentielles ? dans la documentation UID 2.0.

Étape 3 : Enregistrez votre tableau de données d'entrée dans un format de données pris en charge

Si vous avez déjà enregistré vos données d'entrée tierces dans un format de données pris en charge, vous pouvez ignorer cette étape.

Pour utiliser Résolution des entités AWS, les données d'entrée doivent être dans un format qui Résolution des entités AWS soutient. Résolution des entités AWS prend en charge les formats de données suivants :

- valeur séparée par des virgules () CSV

> **Note**
>
> LiveRamp ne prend en charge que CSV les fichiers.

- Parquet

Étape 4 : Chargez votre table de données d'entrée sur Amazon S3

Si vous avez déjà votre table de données tierce dans Amazon S3, vous pouvez ignorer cette étape.

> **Note**
>
> Les données d'entrée doivent être stockées dans Amazon Simple Storage Service (Amazon S3) dans le même Compte AWS and Région AWS dans lequel vous souhaitez exécuter le flux de travail correspondant.

Pour télécharger votre tableau de données d'entrée sur Amazon S3

1. Connectez-vous au AWS Management Console et ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Buckets, puis choisissez un bucket pour stocker votre table de données.
3. Choisissez Upload, puis suivez les instructions.
4. Choisissez l'onglet Objets pour afficher le préfixe dans lequel vos données sont stockées. Notez le nom du dossier.

   Vous pouvez sélectionner le dossier pour afficher le tableau de données.

Étape 5 : Création d'un AWS Glue table

Les données d'entrée dans Amazon S3 doivent être cataloguées dans AWS Glue et représenté sous la forme d'un AWS Glue table. Pour plus d'informations sur la création d'un AWS Glue tableau avec Amazon S3 en entrée, voir Travailler avec des robots d'exploration sur le AWS Glue console dans le AWS Glue Guide du développeur.

> **Note**
>
> Résolution des entités AWS ne prend pas en charge les tables partitionnées.

Au cours de cette étape, vous allez configurer un crawler dans AWS Glue qui analyse tous les fichiers de votre compartiment S3 et crée un AWS Glue table.

> **Note**
>
> Résolution des entités AWS ne prend actuellement pas en charge les sites Amazon S3 enregistrés auprès de AWS Lake Formation.

Pour créer un AWS Glue table

1. Connectez-vous au AWS Management Console et ouvrez le AWS Glue console à https://console.aws.amazon.com/glue/.
2. Dans la barre de navigation, sélectionnez Crawlers.
3. Sélectionnez votre compartiment S3 dans la liste, puis choisissez Ajouter un robot d'exploration.
4. Sur la page Ajouter un robot d'exploration, entrez un nom de robot, puis choisissez Suivant.
5. Parcourez la page Ajouter un robot d'exploration en spécifiant les détails.
6. Sur la page Choisir un IAM rôle, choisissez Choisir un IAM rôle existant, puis cliquez sur Suivant.

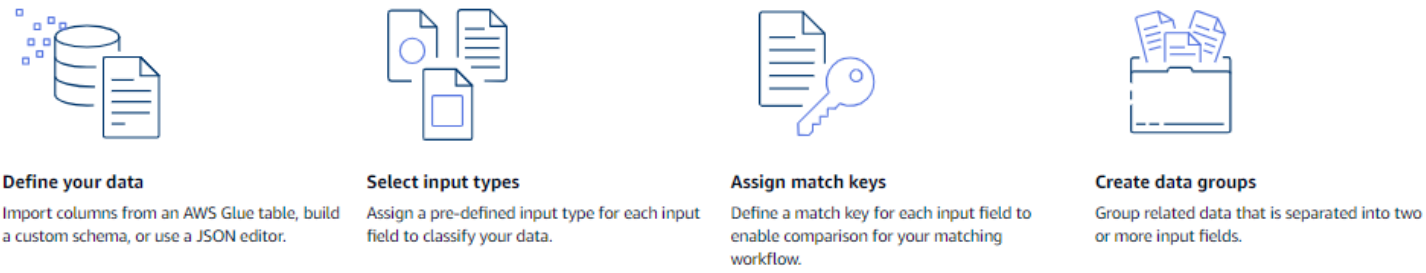
   Vous pouvez également choisir Créer un IAM rôle ou demander à votre administrateur de créer le IAM rôle si nécessaire.
7. Pour Créer un calendrier pour ce robot d'exploration, conservez la fréquence par défaut (Exécuter à la demande), puis choisissez Next.
8. Pour Configurer la sortie du robot d'exploration, entrez AWS Glue base de données, puis choisissez Next.
9. Passez en revue tous les détails, puis choisissez Terminer.
10. Sur la page Crawlers, cochez la case à côté de votre compartiment S3, puis choisissez Run crawler.
11. Une fois que le crawler a fini de fonctionner, sur le AWS Glue dans la barre de navigation, choisissez Bases de données, puis choisissez le nom de votre base de données.
12. Sur la page Base de données, sélectionnez Tables dans {nom de votre base de données}.

    a. Consultez les tableaux dans le AWS Glue base de données.
    b. Pour afficher le schéma d'une table, sélectionnez une table spécifique.
    c. Prenez note du AWS Glue nom de la base de données et AWS Glue nom de la table.

Définition des données d'entrée à l'aide du mappage de schéma

Un mappage de schéma définit les données d'entrée que vous souhaitez résoudre. Il fournit également des métadonnées sur les données d'entrée, telles que les types d'attributs des colonnes (types d'entrée) et les colonnes sur lesquelles effectuer la correspondance.

Lorsque vous créez un mappage de schéma, vous définissez d'abord vos champs de saisie et vos types d'entrée, puis vous définissez vos clés de correspondance et les données relatives aux groupes. Le schéma suivant explique comment créer un mappage de schéma.



Avant de créer un mappage de schéma, vous devez d'abord configurer Résolution des entités AWS et préparez vos tableaux de données. Pour plus d'informations, consultez Configurez Résolution des entités AWS et Préparer des tableaux de données d'entrée.

Après avoir créé un mappage de schéma, vous pouvez effectuer l'une des opérations suivantes :

- Créez un flux de travail correspondant pour trouver des correspondances entre les différentes entrées de données.
- Créez une source d'espace de noms d'ID que vous pouvez utiliser dans un flux de travail de mappage d'identifiants pour traduire les données d'une source vers une cible.
- Créez un flux de travail de mappage d'identifiants dans le même Compte AWSen utilisant votre mappage de schéma comme source.

Rubriques

- Création d'un mappage de schéma
- Clonage d'un mappage de schéma
- Modification d'un mappage de schéma

- Supprimer un mappage de schéma

Création d'un mappage de schéma

Cette procédure décrit le processus de création d'un mappage de schéma à l'aide du Résolution des entités AWS console.

Il existe trois méthodes pour créer un mappage de schéma :

- Importez des données d'entrée existantes à l'aide de l'option Importer depuis AWS Glueoption — Utilisez cette méthode de création pour définir des champs de saisie en commençant par des colonnes préremplies provenant d'un AWS Glue table utilisant un flux guidé.
- Définition manuelle des données d'entrée à l'aide de l'option Créer un schéma personnalisé : utilisez cette méthode de création pour définir manuellement les champs de saisie à l'aide d'un flux guidé.
- Création manuelle à l'aide de l'option Utiliser l'JSONéditeur : utilisez un JSON éditeur pour créer, utiliser un échantillon ou importer manuellement des données d'entrée existantes.

> **Note**
>
> Les champs d'identifiant unique et de saisie ne sont pas disponibles avec cette option.

Import from AWS Glue

Pour créer un mappage de schéma en important des données d'entrée existantes depuis AWS Glue

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez Schema mappings.
3. Sur la page des mappages de schéma, dans le coin supérieur droit, choisissez Créer un mappage de schéma.
4. Pour l'étape 1 : Spécifier les détails du schéma, procédez comme suit :

a. Dans Nom et méthode de création, entrez un nom de mappage de schéma et une description facultative.

b. Pour la méthode de création, choisissez Importer depuis AWS Glue.

c. Cliquez sur le bouton AWS Glue base de données dans le menu déroulant, puis sélectionnez AWS Glue tableau dans le menu déroulant.

   Pour créer une nouvelle table, rendez-vous sur AWS Glue console https://console.aws.amazon.com/glue/. Pour plus d'informations, consultez .AWS Glue tables dans le AWS Glue Guide de l'utilisateur.

d. Pour ID unique, spécifiez la colonne qui fait référence de manière distincte à chaque ligne de vos données.

   Example

   Par exemple : **`Primary_key`**, **`Row_ID`** ou **`Record_ID`**.

   > **Note**
   >
   > La colonne Unique ID est obligatoire. L'identifiant unique doit être un identifiant unique au sein d'une même table. Cependant, dans les différentes tables, l'identifiant unique peut comporter des valeurs dupliquées. Si l'identifiant unique n'est pas spécifié, n'est pas unique au sein de la même source ou se chevauche en termes de noms d'attributs entre les sources, alors Résolution des entités AWS rejette l'enregistrement lorsque le flux de travail correspondant est exécuté. Si vous utilisez ce mappage de schéma dans un flux de travail de correspondance basé sur des règles, l'identifiant unique ne doit pas dépasser 38 caractères.

e. Pour les champs de saisie, choisissez les colonnes que vous souhaitez utiliser pour la correspondance et pour le transfert facultatif.

   Vous pouvez choisir un maximum de 34 colonnes au total pour la correspondance et le transfert.

   i. Sous Correspondance, choisissez les colonnes que vous souhaitez utiliser comme champs de saisie pour la mise en correspondance.

      Vous pouvez choisir un maximum de 24 colonnes pour la correspondance.

ii. Sélectionnez Ajouter des colonnes à transmettre si vous souhaitez spécifier les colonnes qui ne sont pas utilisées pour la correspondance.

iii. (Facultatif) Sous Transférer, choisissez les colonnes à inclure en tant que colonnes intermédiaires.

f. (Facultatif) Si vous souhaitez activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

g. Choisissez Suivant.

5. Pour l'étape 2 : mapper les champs de saisie, définissez les champs de saisie que vous souhaitez utiliser pour la correspondance et pour le transfert facultatif.

   a. Pour les champs de saisie à mettre en correspondance, pour chaque champ de saisie, spécifiez le type de saisie, la clé de correspondance et le statut de hachage.

      Le type d'entrée vous permet de classer les données. La touche Match permet de comparer les champs de saisie à votre flux de travail correspondant. L'état de hachage indique si la valeur de colonne de ce champ de saisie est hachée ou en texte clair.

      > **Note**
      >
      > Si vous créez un mappage de schéma à utiliser avec la technique de correspondance basée sur les services du LiveRamp fournisseur, vous pouvez :
      >
      > - Spécifiez le type d'entrée en tant qu'LiveRampID.
      > - Spécifiez le champ de nom sous la forme de plusieurs champs (tels que**`first_name`**,**`last_name`**) ou d'un seul champ.
      > - Spécifiez le champ d'adresse postale sous la forme de plusieurs champs (tels que**`address1`**,**`address2`**) ou d'un seul champ.
      >
      >   En cas de correspondance avec une adresse, un code postal est requis.
      > - Incluez un e-mail ou un téléphone avec le nom, et ces champs peuvent correspondre à l'adresse postale.

> **Note**
>
> Si vous créez un mappage de schéma à utiliser avec le flux de travail de correspondance basé sur l'apprentissage automatique, votre ensemble de données doit contenir au moins l'un des attributs suivants :**`phonenumber`**,**`emailaddress`**, **`fullnameaddresses`**, ou. **`birthdate`**
> Ne spécifiez le type d'entrée pour aucun de ces attributs sous forme de chaîne personnalisée.

b. (Facultatif) Pour les champs de saisie à transmettre, ajoutez les champs de saisie qui ne seront pas mis en correspondance et leur statut de hachage correspondant.

   L'état de hachage indique si la valeur de colonne de ce champ de saisie est hachée ou en texte clair.

c. Choisissez Suivant.

6. Pour l'étape 3 : Grouper les données, procédez comme suit :

   a. Choisissez les champs de nom associés, puis entrez le nom du groupe et la clé de correspondance.

      Example

      Par exemple, choisissez les champs de saisie **`First nameMiddle name`**, et**`Last name`**. Entrez ensuite un nom de groupe appelé « **`Full name`** » et une clé de correspondance appelée « **`Full name`** » pour permettre la comparaison.

   b. Choisissez les champs d'adresse associés, puis entrez le nom du groupe et la clé de correspondance.

      Example

      Par exemple, choisissez les champs de saisie **`Home street address 1Home street address 2`**, et**`Home city`**. Entrez ensuite un nom de groupe appelé « **`Shipping address`** » et une clé de correspondance appelée « **`Shipping address`** » pour permettre la comparaison.

c. Choisissez les champs de numéro de téléphone correspondants, puis entrez le nom du groupe et la clé de correspondance.

Example

Par exemple, choisissez les champs de saisie **`Home phone 1`** **`Home phone 2`**, et **`Cell phone`**. Entrez ensuite un nom de groupe appelé « **`Shipping phone number`** » et une clé de correspondance appelée « **`Shipping phone number`** » pour permettre la comparaison.

Si vous disposez de plusieurs types de données, vous pouvez ajouter d'autres groupes.

d. Choisissez Suivant.

7. Pour l'étape 4 : révision et création, procédez comme suit :

a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

b. Choisissez Créer un mappage de schéma.

> **Note**
>
> Vous ne pouvez pas modifier un mappage de schéma après l'avoir associé à un flux de travail. Vous pouvez cloner un mappage de schéma si vous souhaitez utiliser une configuration existante pour créer un nouveau mappage de schéma.

Après avoir créé le mappage du schéma, vous êtes prêt à créer un flux de travail correspondant ou à créer un espace de noms d'identification.

Build custom schema

Pour créer un mappage de schéma à l'aide de l'option Créer un schéma personnalisé

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez Schema mappings.
3. Sur la page des mappages de schéma, dans le coin supérieur droit, choisissez Créer un mappage de schéma.

4. Pour l'étape 1 : Spécifier les détails du schéma, procédez comme suit :

   a. Pour le nom et la méthode de création, entrez un nom de mappage de schéma et une description facultative.

   b. Pour Méthode de création, choisissez Créer un schéma personnalisé.

   c. Dans le champ Identifiant unique, entrez un identifiant unique pour identifier chaque ligne de vos données.

      Example

      Par exemple : **`Primary_key`**, **`Row_ID`** ou **`Record_ID`**.

      > **Note**
      >
      > La colonne Unique ID est obligatoire. L'identifiant unique doit être un identifiant unique au sein d'une même table. Cependant, dans les différentes tables, l'identifiant unique peut comporter des valeurs dupliquées. Si l'identifiant unique n'est pas spécifié, n'est pas unique au sein de la même source ou se chevauche en termes de noms d'attributs entre les sources, alors Résolution des entités AWS rejette l'enregistrement lorsque le flux de travail correspondant est exécuté. Si vous utilisez ce mappage de schéma dans un flux de travail de correspondance basé sur des règles, l'identifiant unique ne doit pas dépasser 38 caractères.

   d. (Facultatif) Si vous souhaitez activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

   e. Choisissez Suivant.

5. Pour l'étape 2 : mapper les champs de saisie, définissez les champs de saisie que vous souhaitez utiliser pour la correspondance et pour le transfert facultatif.

   Vous pouvez définir un maximum de 34 colonnes au total pour la correspondance et le transfert.

   a. Pour les champs de saisie à mettre en correspondance, ajoutez un champ de saisie, ainsi que le type de saisie, la clé de correspondance et le statut de hachage correspondants.

Vous pouvez ajouter un maximum de 24 champs de saisie à des fins de correspondance.

Le type d'entrée vous permet de classer les données. La touche Match permet de comparer les champs de saisie à votre flux de travail correspondant. L'état de hachage indique si la valeur de colonne de ce champ de saisie est hachée ou en texte clair.

> **Note**
>
> Si vous créez un mappage de schéma à utiliser avec la technique de correspondance basée sur le service du LiveRamp fournisseur, vous pouvez spécifier le type d'entrée comme LiveRamp ID. Si vous souhaitez inclure PII des données dans la sortie, vous devez spécifier le type d'entrée en tant que chaîne personnalisée.

> **Note**
>
> Si vous créez un mappage de schéma à utiliser avec le flux de travail de correspondance basé sur l'apprentissage automatique, votre ensemble de données doit contenir au moins l'un des attributs suivants :**`phonenumber`**,**`emailaddress`**, **`fullnameaddresses`**, ou. **`birthdate`**
> Ne spécifiez le type d'entrée pour aucun de ces attributs sous forme de chaîne personnalisée.

b. (Facultatif) Pour les champs de saisie à transmettre, ajoutez les champs de saisie qui ne seront pas mis en correspondance et leur statut de hachage correspondant.

c. Choisissez Suivant.

6. Pour l'étape 3 : Données de groupe :

a. Choisissez les champs de nom associés, puis entrez le nom du groupe et la clé de correspondance.

Example

Par exemple, choisissez les champs de saisie **`First nameMiddle name`**, et**`Last name`**. Entrez ensuite un nom de groupe appelé « **`Full name`** » et une clé de correspondance appelée « **`Full name`** » pour permettre la comparaison.

b. Choisissez les champs d'adresse associés, puis entrez le nom du groupe et la clé de correspondance.

Example

Par exemple, choisissez les champs de saisie **`Home street address 1Home street address 2`**, et**`Home city`**. Entrez ensuite un nom de groupe appelé « **`Shipping address`** » et une clé de correspondance appelée « **`Shipping address`** » pour permettre la comparaison.

c. Choisissez les champs de numéro de téléphone correspondants, puis entrez le nom du groupe et la clé de correspondance.

Example

Par exemple, choisissez les champs de saisie **`Home phone 1Home phone 2`**, et**`Cell phone`**. Entrez ensuite un nom de groupe appelé « **`Shipping phone number`** » et une clé de correspondance appelée « **`Shipping phone number`** » pour permettre la comparaison.

Si vous disposez de plusieurs types de données, vous pouvez ajouter d'autres groupes.

d. Choisissez Suivant.

7. Pour l'étape 4 : révision et création, procédez comme suit :

a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

b. Choisissez Créer un mappage de schéma.

> **Note**
>
> Vous ne pouvez pas modifier un mappage de schéma après l'avoir associé à un flux de travail. Vous pouvez cloner un mappage de schéma si vous souhaitez utiliser une configuration existante pour créer un nouveau mappage de schéma.

Après avoir créé le mappage du schéma, vous êtes prêt à créer un flux de travail correspondant ou à créer un espace de noms d'identification.

Use JSON editor

Pour créer un mappage de schéma à l'aide de l'JSONéditeur

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez Schema mappings.
3. Sur la page des mappages de schéma, dans le coin supérieur droit, choisissez Créer un mappage de schéma.
4. Pour l'étape 1 : Spécifier les détails du schéma, procédez comme suit :
   a. Pour le nom et la méthode de création, entrez un nom de mappage de schéma et une description facultative.
   b. Pour Méthode de création, choisissez Utiliser l'JSONéditeur.
   c. (Facultatif) Si vous souhaitez activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
   d. Choisissez Suivant.
5. Pour l'étape 2 : Spécifier le mappage :
   a. Commencez à créer le schéma dans l'JSONéditeur ou choisissez l'une des options suivantes en fonction de votre objectif :

Votre objectif	Option recommandée
Commencez à créer votre mappage de schéma	Insérez un échantillon, JSON puis modifiez les informations si nécessaire.
Utiliser un JSON fichier existant	Importer depuis un fichier

   b. Choisissez Suivant.
6. Pour l'étape 3 : révision et création :

a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

b. Choisissez Créer un mappage de schéma.

> **Note**
>
> Vous ne pouvez pas modifier un mappage de schéma après l'avoir associé à un flux de travail. Vous pouvez cloner un mappage de schéma si vous souhaitez utiliser une configuration existante pour créer un nouveau mappage de schéma.

Après avoir créé le mappage du schéma, vous êtes prêt à créer un flux de travail correspondant ou à créer un espace de noms d'identification.

Clonage d'un mappage de schéma

Vous pouvez cloner un mappage de schéma si vous souhaitez utiliser une configuration existante pour créer un nouveau mappage de schéma.

Pour cloner un mappage de schéma :

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez Schema mappings.
3. Choisissez le mappage du schéma.
4. Choisissez Clone (Cloner).
5. Sur la page Spécifier les détails du schéma, apportez les modifications nécessaires, puis choisissez Suivant.
6. Sur la page Choisir une technique de correspondance, apportez les modifications nécessaires, puis choisissez Suivant.
7. Sur la page des champs de saisie de la carte, apportez les modifications nécessaires, puis choisissez Next.
8. Sur la page Données du groupe, apportez les modifications nécessaires, puis choisissez Suivant.

9. Sur la page Réviser et enregistrer, apportez les modifications nécessaires, puis choisissez Cloner le mappage du schéma.

Modification d'un mappage de schéma

Vous ne pouvez modifier un mappage de schéma qu'avant de l'associer à un flux de travail. Une fois que vous avez associé un mappage de schéma à un flux de travail, vous ne pouvez pas le modifier. Vous pouvez cloner un mappage de schéma si vous souhaitez utiliser une configuration existante pour créer un nouveau mappage de schéma.

Pour modifier un mappage de schéma :

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez Schema mappings.
3. Choisissez le mappage du schéma.
4. Choisissez Modifier.
5. Sur la page Spécifier les détails du schéma, apportez les modifications nécessaires, puis choisissez Suivant.
6. Sur la page Choisir une technique de correspondance, apportez les modifications nécessaires, puis choisissez Suivant.
7. Sur la page des champs de saisie de la carte, apportez les modifications nécessaires, puis choisissez Next.
8. Sur la page Données du groupe, apportez les modifications nécessaires, puis choisissez Suivant.
9. Sur la page Réviser et enregistrer, apportez les modifications nécessaires, puis choisissez Modifier le mappage du schéma.

Supprimer un mappage de schéma

Vous ne pouvez pas supprimer un mappage de schéma lorsqu'il est associé à un flux de travail correspondant. Vous devez d'abord supprimer le mappage de schéma de tous les flux de travail correspondants associés avant de pouvoir le supprimer.

Pour supprimer un mappage de schéma :

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez Schema mappings.
3. Choisissez le mappage du schéma.
4. Sélectionnez Delete (Supprimer).
5. Confirmez la suppression, puis choisissez Supprimer.

Définir les données d'entrée à l'aide d'un espace de noms ID

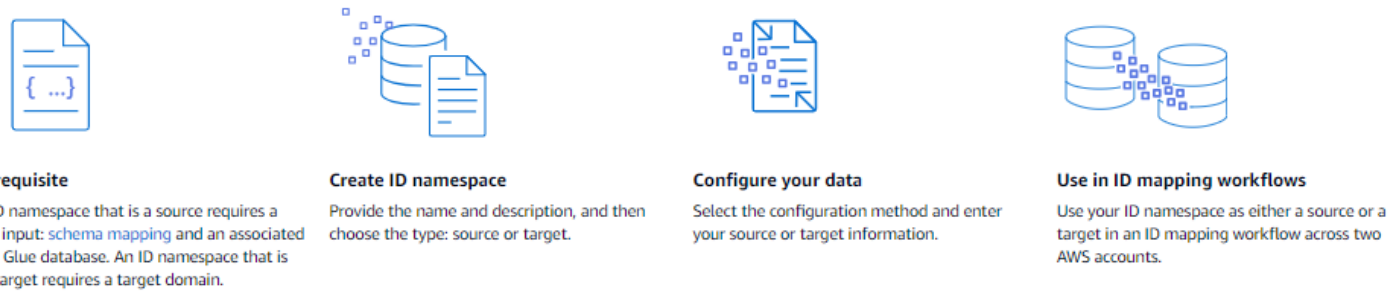
Un espace de noms d'ID est une enveloppe entourant votre table de données d'entrée. Vous utilisez un espace de noms d'identification pour fournir des métadonnées expliquant vos données d'entrée et les techniques de correspondance, ainsi que la façon de les utiliser dans un flux de travail de mappage d'identifiants.

Il existe deux types d'espaces de noms d'ID : source et cible.

- La source contient des configurations pour les données sources qui Résolution des entités AWS processus dans un flux de travail de mappage d'identifiants.
- La cible contient une configuration des données cibles vers laquelle toutes les sources sont résolues.

Vous pouvez définir les données d'entrée que vous souhaitez résoudre entre deux Comptes AWS dans un flux de travail de mappage d'identifiants. Un participant crée une source d'espace de noms ID et un autre participant crée une cible d'espace de noms d'ID. Une fois que les participants ont créé la source et la cible, vous pouvez exécuter un flux de travail de mappage d'identifiants pour traduire les données de la source vers la cible.

Le schéma suivant explique comment créer un espace de noms d'ID à utiliser dans un flux de travail de mappage d'ID.



Les sections suivantes décrivent comment créer une source d'espace de noms ID et une cible d'espace de noms ID.

Rubriques

- Source de l'espace de noms ID
- ID : espace de noms cible
- Modification d'un espace de noms d'ID

- Supprimer un espace de noms d'ID
- Ajouter ou mettre à jour une politique de ressources pour un espace de noms d'ID

Source de l'espace de noms ID

La source de l'espace de noms ID est la source des données dans un flux de travail de mappage d'ID.

Avant de créer une source d'espace de noms d'ID, vous devez d'abord créer un mappage de schéma ou un flux de travail correspondant, selon votre cas d'utilisation. Pour plus d'informations, consultez Création d'un mappage de schéma et Associez les données d'entrée à l'aide d'un flux de travail correspondant.

Après avoir créé une source d'espace de noms d'ID, vous pouvez l'utiliser avec une cible d'espace de noms d'ID dans un flux de travail de mappage d'ID. Pour de plus amples informations, veuillez consulter Mapper les données d'entrée à l'aide d'un flux de travail de mappage.

Il existe deux manières de créer une source d'espace de noms d'ID dans Résolution des entités AWS console : la méthode basée sur des règles ou la méthode des services du fournisseur.

Rubriques

- Création d'une source d'espace de noms d'identification (basée sur des règles)
- Création d'une source d'espace de noms ID (services du fournisseur)

Création d'une source d'espace de noms d'identification (basée sur des règles)

Cette rubrique décrit le processus de création d'une source d'espace de noms d'identification à l'aide de la méthode basée sur des règles. Cette méthode utilise des règles de correspondance pour traduire les données de première partie d'une source vers une cible dans un flux de travail de mappage d'identifiants.

> **Note**
>
> Si les données d'entrée sont la source, elles doivent avoir un mappage de schéma et un AWS Glue base de données.

Pour créer une source d'espace de noms d'identification (basée sur des règles)

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez les espaces de noms ID.
3. Sur la page des espaces de noms d'identification, dans le coin supérieur droit, choisissez Create ID namespace.
4. Pour plus de détails, procédez comme suit :

   a. Pour le nom de l'espace de noms ID, entrez un nom unique.

   b. (Facultatif) Dans Description, entrez une description facultative.

   c. Pour le type d'espace de noms ID, choisissez Source.
5. Pour la méthode de l'espace de noms ID, choisissez Rule-based.
6. Pour la saisie de données, choisissez le type d'entrée que vous souhaitez utiliser, puis prenez les mesures recommandées.

Service du fournisseur	Actions recommandées
Un mappage de schéma existant	1. Choisissez le mappage du schéma. 2. Cliquez sur le bouton AWS Glue base de données, le AWS Glue table et le mappage du schéma dans la liste déroulante. Vous pouvez ajouter jusqu'à 20 entrées de données.
Un flux de travail de correspondance existant	1. Choisissez le flux de travail correspondant. 2. Choisissez le compte associé à l'espace de noms ID : soit votre Compte AWSou un autre Compte AWS. 3. Selon le type de compte, sélectionnez le nom du flux de travail correspondant

Service du fournisseur	Actions recommandées
	ou entrez le flux de travail correspondant ARN.

7. Pour les paramètres de règle, procédez comme suit.

   a. Spécifiez les contrôles de règle en choisissant l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Autoriser les règles provenant à la fois de la source et de la cible	Aucune préférence
Choisissez si une source, une cible ou les deux peuvent fournir des règles dans un flux de travail de mappage d'identifiants	Règles limitées

   Les contrôles de règles doivent être compatibles entre la source et la cible pour être utilisés dans un flux de travail de mappage d'identifiants. Par exemple, si un espace de noms d'ID source limite les règles à la cible mais que l'espace de noms d'ID cible limite les règles à la source, cela entraîne une erreur.

   b. Spécifiez les règles de correspondance en choisissant l'une des options suivantes en fonction de votre type de saisie de données.

Type de saisie de données	Action recommandée
Cartographie du schéma	Choisissez Ajouter une autre règle pour ajouter une règle correspondante. Vous pouvez appliquer jusqu'à 25 règles de correspondance pour définir vos critères de correspondance.
Flux de travail correspondant	Choisissez Utiliser les règles du flux de travail correspondant ou Fournir de

Type de saisie de données	Action recommandée
	nouvelles règles pour définir vos règles de correspondance.

8. Pour les paramètres de comparaison et de correspondance, procédez comme suit.

   a. Spécifiez le type de comparaison en choisissant l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Autorisez l'utilisation de n'importe quel type de comparaison lorsque vous créez le flux de travail de mappage des identifiants.	Aucune préférence
Trouvez n'importe quelle combinaison de correspondances entre les données stockées dans plusieurs champs de saisie, que les données se trouvent dans le même champ de saisie ou dans un champ différent.	Plusieurs champs de saisie
Limitez la comparaison au sein d'un seul champ de saisie, lorsque des données similaires stockées dans plusieurs champs de saisie ne doivent pas être mises en correspondance.	Champ de saisie unique

   b. Spécifiez le type de correspondance des enregistrements en choisissant l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Autorisez l'utilisation de n'importe quel type de comparaison lorsque vous créez le flux de travail de mappage des identifiants.	Aucune préférence

Votre objectif	Option recommandée
Limitez le type de correspondance d'enregistrements afin de ne stocker qu'un seul enregistrement correspondant dans la source pour chaque enregistrement correspondant dans la cible lorsque vous créez le flux de travail de mappage d'identifiants.	Correspondance d'enregistrements limitée and Une source pour une cible
Limitez le type de correspondance d'enregistrements afin de stocker tous les enregistrements correspondants dans la source pour chaque enregistrement correspondant dans la cible lorsque vous créez le flux de travail de mappage d'identifiants.	Correspondance d'enregistrements limitée and De nombreuses sources pour une seule cible

> **Note**
>
> Vous devez spécifier des limites compatibles pour les espaces de noms d'ID source et cible. Par exemple, si un espace de noms d'ID source limite les règles à la cible mais que l'espace de noms d'ID cible limite les règles à la source, cela entraîne une erreur.

9. Spécifiez les autorisations d'accès au service en choisissant un nom de rôle de service existant dans la liste déroulante.
10. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
11. Choisissez Create ID namespace.

La source de l'espace de noms ID est créée. Vous êtes maintenant prêt à créer une cible d'espace de noms ID.

Création d'une source d'espace de noms ID (services du fournisseur)

Cette rubrique décrit le processus de création d'une source d'espace de noms ID à l'aide de la méthode Provider services. Cette méthode utilise un service fournisseur appelé LiveRamp. LiveRamp traduit les données codées par des tiers d'une source vers une cible au cours d'un flux de travail de mappage d'identifiants.

> **Note**
>
> Si les données d'entrée sont la source, elles doivent avoir un mappage de schéma et un AWS Glue base de données.

Pour créer une source d'espace de noms ID (services du fournisseur)

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez les espaces de noms ID.
3. Sur la page des espaces de noms d'identification, dans le coin supérieur droit, choisissez Create ID namespace.
4. Pour plus de détails, procédez comme suit :
   a. Pour le nom de l'espace de noms ID, entrez un nom unique.
   b. (Facultatif) Dans Description, entrez une description facultative.
   c. Pour le type d'espace de noms ID, choisissez Source.
5. Pour la méthode d'espace de noms ID, choisissez Provider services.

> **Note**
>
> Résolution des entités AWS propose actuellement le service du LiveRamp fournisseur en tant que méthode d'espace de noms d'identification. Si vous êtes abonné à LiveRamp, le statut apparaît comme Abonné. Pour plus d'informations sur la façon de s'abonner à LiveRamp, consultezÉtape 1 : Abonnez-vous à un service fournisseur sur AWS Data Exchange.

6. Pour la saisie des données, choisissez AWS Glue base de données, le AWS Glue table et le mappage du schéma dans la liste déroulante.

   Vous pouvez ajouter jusqu'à 20 entrées de données.

7. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.

Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut est `entityresolution-id-mapping-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite un AWS KMS clé utilisée pour déchiffrer vos données saisies.
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser.

Option	Action recommandée
	S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

8. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
9. Choisissez Create ID namespace.

La source de l'espace de noms ID est créée. Vous êtes maintenant prêt à créer une cible d'espace de noms ID.

ID : espace de noms cible

La cible de l'espace de noms d'identification est la cible des données d'un flux de travail de mappage d'identifiants. Toutes les sources sont résolues vers la cible.

Avant de créer une cible d'espace de noms d'ID, vous devez d'abord créer un flux de travail correspondant ou être abonné à un service fournisseur (LiveRamp), selon votre cas d'utilisation. Pour plus d'informations, consultez Associez les données d'entrée à l'aide d'un flux de travail correspondant et Étape 1 : Abonnez-vous à un service fournisseur sur AWS Data Exchange.

Après avoir créé une cible d'espace de noms d'ID, vous pouvez l'utiliser avec une source d'espace de noms d'ID dans un flux de travail de mappage d'ID. Pour de plus amples informations, veuillez consulter Mapper les données d'entrée à l'aide d'un flux de travail de mappage.

Il existe deux manières de créer une cible d'espace de noms ID dans Résolution des entités AWS console : la méthode basée sur des règles ou la méthode des services du fournisseur.

Rubriques

Création d'une cible d'espace de noms ID (méthode basée sur des règles)

Cette rubrique décrit le processus de création d'une cible d'espace de noms ID à l'aide de la méthode basée sur des règles. Cette méthode utilise des règles de correspondance pour traduire les données de première partie d'une source vers une cible au cours d'un flux de travail de mappage d'identifiants.

Pour créer une cible d'espace de noms ID (basée sur des règles)

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez les espaces de noms ID.
3. Sur la page des espaces de noms d'identification, dans le coin supérieur droit, choisissez Create ID namespace.
4. Pour plus de détails, procédez comme suit :
    a. Pour le nom de l'espace de noms ID, entrez un nom unique.
    b. (Facultatif) Dans Description, entrez une description facultative.
    c. Pour le type d'espace de noms ID, choisissez Target.
5. Pour la méthode de l'espace de noms ID, choisissez Rule-based.
6. Pour la saisie de données, sous Processus de mise en correspondance, procédez comme suit.
    a. Choisissez le compte associé à l'espace de noms ID : soit votre Compte AWSou un autre Compte AWS.
    b. Selon le type de compte, sélectionnez le nom du flux de travail correspondant ou entrez le flux de travail correspondant ARN.
7. Pour les paramètres de règle, procédez comme suit.
    a. Spécifiez les contrôles de règle en choisissant l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Autoriser les règles provenant à la fois de la source et de la cible	Aucune préférence
Choisissez si une source, une cible ou les deux peuvent fournir des règles dans un flux de travail de mappage d'identifiants	Règles limitées

Les contrôles de règles doivent être compatibles entre la source et la cible pour être utilisés dans un flux de travail de mappage d'identifiants. Par exemple, si un espace de noms d'ID source limite les règles à la cible mais que l'espace de noms d'ID cible limite les règles à la source, cela entraîne une erreur.

b. Pour les règles de correspondance, Résolution des entités AWS ajoute automatiquement les règles du flux de travail correspondant.

8. Pour les paramètres de comparaison et de correspondance, procédez comme suit.

a. Spécifiez le type de comparaison en choisissant l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Autorisez l'utilisation de n'importe quel type de comparaison lorsque vous créez le flux de travail de mappage des identifiants.	Aucune préférence
Trouvez n'importe quelle combinaison de correspondances entre les données stockées dans plusieurs champs de saisie, que les données se trouvent dans le même champ de saisie ou dans un champ différent.	Plusieurs champs de saisie
Limitez la comparaison au sein d'un seul champ de saisie, lorsque des données	Champ de saisie unique

Votre objectif	Option recommandée
similaires stockées dans plusieurs champs de saisie ne doivent pas être mises en correspondance.	

b. Spécifiez le type de correspondance des enregistrements en choisissant l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Autorisez l'utilisation de n'importe quel type de comparaison lorsque vous créez le flux de travail de mappage des identifiants.	Aucune préférence
Limitez le type de correspondance d'enregistrements afin de ne stocker qu'un seul enregistrement correspondant dans la source pour chaque enregistrement correspondant dans la cible lorsque vous créez le flux de travail de mappage d'identifiants.	Correspondance d'enregistrements limitée and Une source pour une cible
Limitez le type de correspondance d'enregistrements afin de stocker tous les enregistrements correspondants dans la source pour chaque enregistrement correspondant dans la cible lorsque vous créez le flux de travail de mappage d'identifiants.	Correspondance d'enregistrements limitée and De nombreuses sources pour une seule cible

> **Note**
>
> Vous devez spécifier des limites compatibles pour les espaces de noms d'ID source et cible. Par exemple, si un espace de noms d'ID source limite les règles à la cible

mais que l'espace de noms d'ID cible limite les règles à la source, cela entraîne une erreur.

9. Spécifiez les autorisations d'accès au service en choisissant un nom de rôle de service existant dans la liste déroulante.
10. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
11. Choisissez Create ID namespace.

La cible de l'espace de noms ID est créée. Après avoir créé les espaces de noms d'identification (source et cible) requis pour un flux de travail de mappage d'identifiants, vous êtes prêt à créer un flux de travail de mappage d'identifiants.

Création d'une cible d'espace de noms ID (méthode des services du fournisseur)

Cette rubrique décrit le processus de création d'une cible d'espace de noms ID à l'aide de la méthode Provider services. Cette méthode utilise un service fournisseur appelé LiveRamp. LiveRamp traduit les données codées par des tiers d'une source vers une cible au cours d'un flux de travail de mappage d'identifiants.

Pour créer une cible d'espace de noms ID (services du fournisseur)

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez les espaces de noms ID.
3. Sur la page des espaces de noms d'identification, dans le coin supérieur droit, choisissez Create ID namespace.
4. Pour plus de détails, procédez comme suit :
   a. Pour le nom de l'espace de noms ID, entrez un nom unique.
   b. (Facultatif) Dans Description, entrez une description facultative.
   c. Pour le type d'espace de noms ID, choisissez Target.
5. Pour la méthode de l'espace de noms ID, choisissez Provider services.

> **Note**
>
> Résolution des entités AWS propose actuellement le service du LiveRamp fournisseur en tant que méthode d'espace de noms d'identification.
> Si vous êtes abonné à LiveRamp, le statut apparaît comme Abonné.
> Pour plus d'informations sur la façon de s'abonner à LiveRamp, consultezÉtape 1 : Abonnez-vous à un service fournisseur sur AWS Data Exchange.

6. Pour le domaine cible, entrez l'identifiant de domaine LiveRamp client ciblé pour le transcodage qui LiveRamp fournit.
7. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
8. Choisissez Create ID namespace.

La cible de l'espace de noms ID est créée. Après avoir créé les espaces de noms d'identification (source et cible) requis pour un flux de travail de mappage d'identifiants, vous êtes prêt à créer le flux de travail de mappage d'identifiants.

Modification d'un espace de noms d'ID

Vous pouvez uniquement modifier un espace de noms d'ID avant de l'associer à un flux de travail de mappage d'ID. Une fois que vous avez associé un espace de noms d'ID à un flux de travail de mappage d'ID, vous ne pouvez pas le modifier.

Pour modifier un espace de noms d'ID, procédez comme suit :

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS (si vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez les espaces de noms ID.
3. Choisissez l'espace de noms ID.
4. Choisissez Modifier.
5. Sur la page Modifier l'espace de noms ID, apportez les modifications nécessaires, puis choisissez Enregistrer.

Supprimer un espace de noms d'ID

Vous ne pouvez pas supprimer un espace de noms d'ID lorsqu'il est associé à un flux de travail de mappage d'ID. Vous devez d'abord supprimer le mappage de schéma de tous les flux de travail de mappage d'ID associés avant de pouvoir le supprimer.

Pour supprimer un espace de noms d'ID, procédez comme suit :

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS (si vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, sous Préparation des données, choisissez les espaces de noms ID.
3. Choisissez l'espace de noms ID.
4. Sélectionnez Delete (Supprimer).
5. Confirmez la suppression, puis choisissez Supprimer.

Ajouter ou mettre à jour une politique de ressources pour un espace de noms d'ID

Une politique de ressources permet au créateur de la ressource de mappage d'identifiants d'accéder à votre ressource d'espace de noms d'identification.

Pour ajouter ou mettre à jour une politique de ressources

1. Connectez-vous au AWS Management Console et ouvrez le Résolution des entités AWS console avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez les espaces de noms ID.
3. Choisissez l'espace de noms ID.
4. Sur la page de détails de l'espace de noms d'ID, choisissez l'onglet Autorisations.
5. Dans la section Politique en matière de ressources, choisissez Modifier.
6. Ajoutez ou mettez à jour la politique dans l'JSONéditeur.
7. Sélectionnez Enregistrer les modifications.

Associez les données d'entrée à l'aide d'un flux de travail correspondant

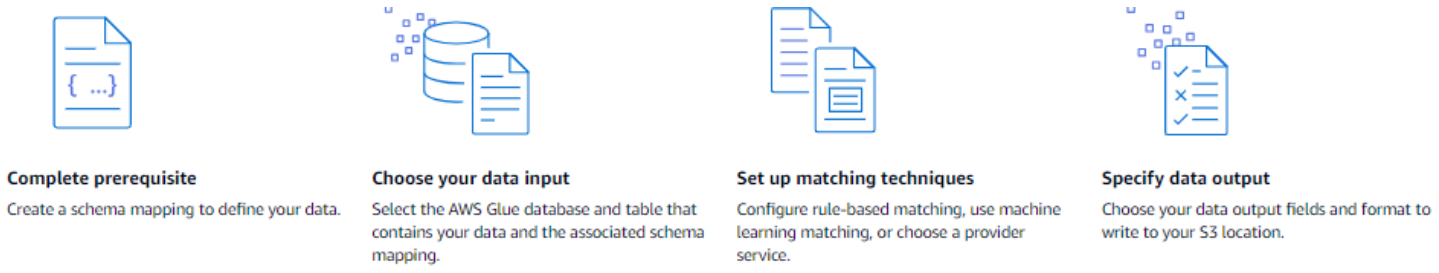
Un flux de travail de correspondance est une tâche de traitement des données qui combine et compare les données provenant de différentes sources d'entrée et détermine laquelle correspond en fonction de différentes techniques de correspondance. Il produit une table de sortie de données.

Lorsque vous créez un flux de travail de correspondance, vous spécifiez d'abord les entrées de données, les étapes de normalisation, puis vous choisissez les techniques de correspondance et les sorties de données souhaitées. Résolution des entités AWS lit vos données à partir de l'emplacement ou des emplacements que vous avez spécifiés et trouve une correspondance entre deux ou plusieurs enregistrements de vos données. Il attribue ensuite un identifiant de correspondance aux enregistrements de l'ensemble de données correspondant. Résolution des entités AWS écrit ensuite les fichiers de sortie de données à l'emplacement de votre choix. Vous pouvez l'utiliser Résolution des entités AWS pour hacher les données de sortie si vous le souhaitez, ce qui vous permet de garder le contrôle de vos données.

Un flux de travail correspondant peut comporter plusieurs exécutions et les résultats (réussites ou erreurs) sont écrits dans un dossier portant le `jobId` nom.

La sortie de données contient à la fois un fichier pour les correspondances réussies et un fichier pour les erreurs. La sortie de données peut contenir plusieurs champs. Les résultats positifs sont écrits `success` dans un dossier contenant plusieurs fichiers, et chaque fichier contient un sous-ensemble des enregistrements réussis. De même, les erreurs sont enregistrées `error` dans un dossier contenant plusieurs champs, chacun contenant un sous-ensemble des enregistrements d'erreurs. Pour plus d'informations sur la résolution des erreurs, consultezRésolution des problèmes liés aux workflows correspondants.

Le schéma suivant explique comment créer un flux de travail correspondant.



Avant de créer un flux de travail correspondant, vous devez d'abord créer un mappage de schéma. Pour de plus amples informations, veuillez consulter Création d'un mappage de schéma.

Il existe trois méthodes pour créer un flux de travail correspondant, basé sur des techniques de correspondance : basé sur des règles, basé sur l'apprentissage automatique ou basésur les services des fournisseurs.

Après avoir créé et exécuté un flux de travail correspondant, vous pouvez effectuer les opérations suivantes :

- Affichez les résultats dans l'emplacement S3 que vous avez spécifié. Les flux de travail correspondants sont générés une IDs fois les données indexées.
- Utilisez les résultats de la mise en correspondance basée sur des règles ou de l'apprentissage automatique (ML) comme entrée pour la mise en correspondance basée sur les services des fournisseurs ou inversement pour répondre aux besoins de votre entreprise.

Par exemple, pour réduire les coûts d'abonnement des fournisseurs, vous pouvez d'abord exécuter une correspondance basée sur des règles pour trouver des correspondances dans vos données. Vous pouvez ensuite envoyer un sous-ensemble d'enregistrements sans correspondance au jumelage basé sur les services du fournisseur.

Rubriques

- Création d'un flux de travail de correspondance basé sur des règles
- Création d'un flux de travail de correspondance basé sur le machine learning
- Création d'un flux de travail de correspondance basé sur les services des fournisseurs
- Modification d'un flux de travail correspondant
- Supprimer un flux de travail correspondant
- Trouver un identifiant de correspondance pour un flux de travail de correspondance basé sur des règles
- Suppression d'enregistrements d'un flux de travail de correspondance basé sur des règles ou basé sur le ML
- Résolution des problèmes liés aux workflows correspondants

Création d'un flux de travail de correspondance basé sur des règles

La correspondance basée sur des règles est un ensemble hiérarchique de règles de correspondance en cascade, suggérées par Résolution des entités AWS, en fonction des données que vous saisissez et que vous pouvez entièrement configurer. Le flux de correspondance basé sur des règles vous permet de comparer des données en texte clair ou hachées pour trouver des correspondances exactes en fonction de critères que vous personnalisez.

Lorsqu'il Résolution des entités AWS trouve une correspondance entre deux ou plusieurs enregistrements de vos données, il attribue :

- Un identifiant de correspondance avec les enregistrements de l'ensemble de données correspondant
- La règle de correspondance qui a généré la correspondance.

Pour créer un flux de travail de correspondance basé sur des règles

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS (si vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, sous Workflows, choisissez Matching.
3. Sur la page des flux de travail correspondants, dans le coin supérieur droit, choisissez Créer un flux de travail correspondant.
4. Pour l'étape 1 : Spécifier les détails du flux de travail correspondants, procédez comme suit :

    a. Entrez un nom de flux de travail correspondant et une description facultative.

    b. Pour la saisie de données, choisissez une AWS Glue base de données dans la liste déroulante, sélectionnez la AWS Glue table, puis le mappage de schéma correspondant.

    Vous pouvez ajouter jusqu'à 19 entrées de données.

    c. L'option Normaliser les données est sélectionnée par défaut, afin que les entrées de données soient normalisées avant la mise en correspondance. Si vous ne souhaitez pas normaliser les données, désélectionnez l'option Normaliser les données.

    d. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.

Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut est `entityresolution-matching-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.

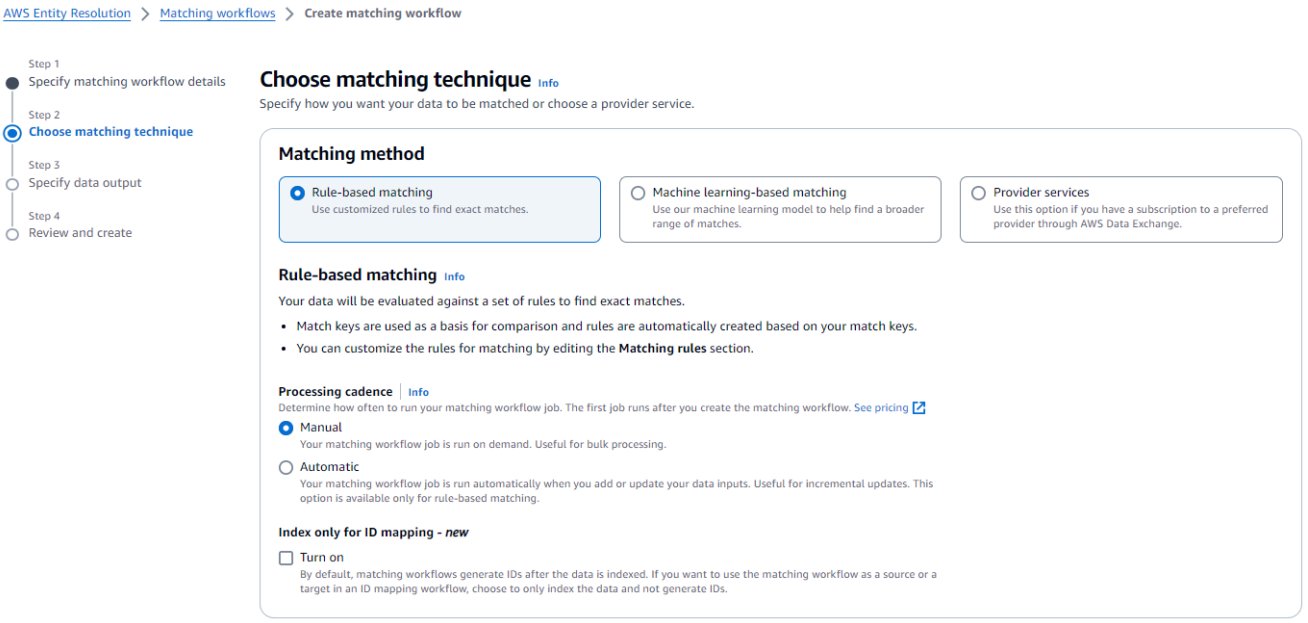
Option	Action recommandée
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

e. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

f. Choisissez Suivant.

5. Pour l'étape 2 : Choisissez la technique de correspondance :

   a. Pour Méthode de correspondance, choisissez Correspondance basée sur des règles.



b. Pour Processing cadence, choisissez l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Exécuter un flux de travail à la demande pour une mise à jour groupée	Manuel
Exécutez un flux de travail dès que de nouvelles données se trouvent dans votre compartiment S3	Automatique

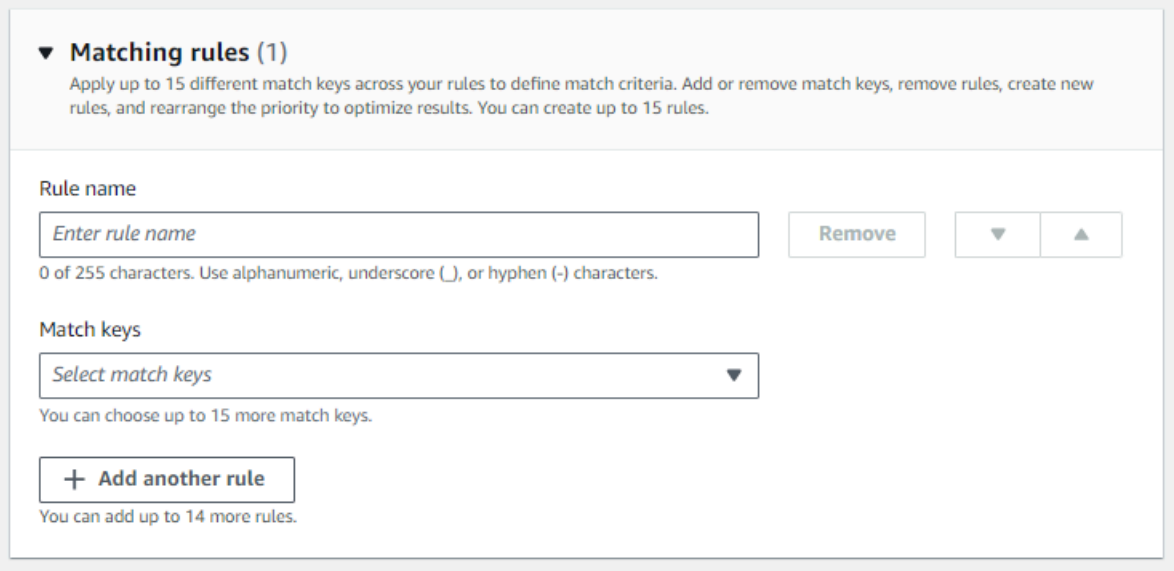
> **Note**
>
> Si vous choisissez Automatique, assurez-vous que EventBridge les notifications Amazon sont activées pour votre compartiment S3. Pour obtenir des instructions sur l'activation EventBridge d'Amazon à l'aide de la console S3, consultez la section Activation d'Amazon EventBridge dans le guide de l'utilisateur Amazon S3.

c. (Facultatif) Pour Index uniquement pour le mappage des identifiants, vous pouvez choisir d'activer la possibilité d'indexer uniquement les données et de ne pas les générerIDs.

Par défaut, les flux de travail correspondants sont générés une IDs fois les données indexées.

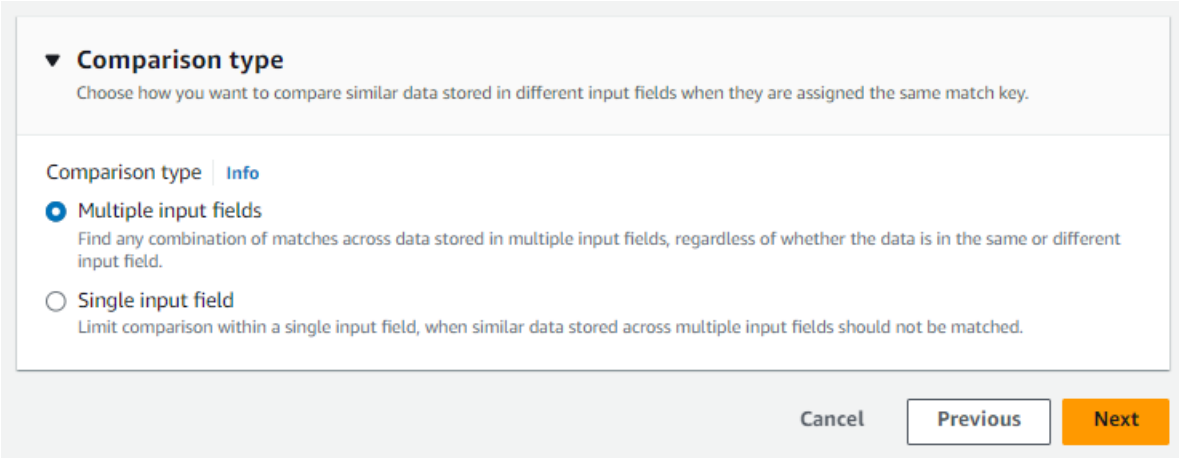
d. Pour les règles de correspondance, entrez un nom de règle, puis choisissez les clés de correspondance pour cette règle.

   Vous pouvez créer jusqu'à 15 règles et appliquer jusqu'à 15 clés de correspondance différentes à vos règles pour définir des critères de correspondance.



e. Pour le type de comparaison, choisissez l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Trouvez n'importe quelle combinaison de correspondances entre les données stockées dans plusieurs champs de saisie	Plusieurs champs de saisie
Limiter la comparaison à un seul champ de saisie	Champ de saisie unique



f. Choisissez Suivant.

6. Pour l'étape 3 : Spécifier la sortie et le format des données :

   a. Pour la destination et le format de sortie des données, choisissez l'emplacement Amazon S3 pour la sortie des données et indiquez si le format des données sera des données normalisées ou des données d'origine.

   b. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS cléARN.

   c. Affichez la sortie générée par le système.

   d. Pour la sortie de données, choisissez les champs que vous souhaitez inclure, masquer ou masquer, puis prenez les mesures recommandées en fonction de vos objectifs.

Votre objectif	Option recommandée
Inclure les champs	Conservez l'état de sortie sur Inclus.
Masquer les champs (exclure de la sortie)	Choisissez le champ de sortie, puis choisissez Masquer.
Champs de masque	Choisissez le champ Sortie, puis choisissez Hash output.
Réinitialisez les paramètres précédents	Choisissez Réinitialiser.

   e. Choisissez Suivant.

7. Pour l'étape 4 : révision et création :

a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

b. Choisissez Créer et exécuter.

   Un message apparaît, indiquant que le flux de travail correspondant a été créé et que le travail a commencé.

8. Sur la page des détails du flux de travail correspondant, sous l'onglet Mesures, consultez les informations suivantes sous Dernières mesures de travail :

   - Le Job ID.
   - État de la tâche de flux de travail correspondante : En file d'attente, en cours, terminée, échouée
   - Durée d'exécution de la tâche de flux de travail.
   - Le nombre d'enregistrements traités.
   - Le nombre d'enregistrements non traités.
   - La correspondance unique IDs générée.
   - Le nombre d'enregistrements en entrée.

   Vous pouvez également consulter les statistiques des tâches correspondant aux tâches de flux de travail précédemment exécutées dans l'historique des tâches.

9. Une fois la tâche de flux de travail correspondante terminée (le statut est terminé), vous pouvez accéder à l'onglet Sortie de données, puis sélectionner votre site Amazon S3 pour afficher les résultats.

10. (Type de traitement manuel uniquement) Si vous avez créé un flux de travail de correspondance basé sur des règles avec le type de traitement manuel, vous pouvez exécuter le flux de travail correspondant à tout moment en choisissant Exécuter le flux de travail sur la page de détails du flux de travail correspondant.

Création d'un flux de travail de correspondance basé sur le machine learning

La mise en correspondance basée sur l'apprentissage automatique est un processus prédéfini qui tente de faire correspondre les enregistrements à toutes les données que vous saisissez. Le

flux de travail de correspondance basé sur l'apprentissage automatique vous permet de comparer des données en texte clair pour trouver un large éventail de correspondances à l'aide d'un modèle d'apprentissage automatique.

> **Note**
>
> Le modèle d'apprentissage automatique ne prend pas en charge la comparaison de données hachées.

Lorsqu'il Résolution des entités AWS trouve une correspondance entre deux ou plusieurs enregistrements de vos données, il attribue :

- Un identifiant de correspondance avec les enregistrements de l'ensemble de données correspondant
- Le pourcentage du niveau de confiance du match.

Vous pouvez utiliser le résultat d'un flux de travail de correspondance basé sur le ML comme entrée pour le rapprochement des fournisseurs de services de données, ou vice-versa pour atteindre vos objectifs spécifiques. Par exemple, vous pouvez exécuter une correspondance basée sur le ML pour trouver d'abord des correspondances entre vos sources de données sur vos propres enregistrements. Si un sous-ensemble n'a pas été mis en correspondance, vous pouvez ensuite exécuter une correspondance basée sur le service du fournisseur pour trouver des correspondances supplémentaires.

Pour créer un flux de travail de correspondance basé sur le ML :

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS (si vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, sous Workflows, choisissez Matching.
3. Sur la page des flux de travail correspondants, dans le coin supérieur droit, choisissez Créer un flux de travail correspondant.
4. Pour l'étape 1 : Spécifier les détails du flux de travail correspondants, procédez comme suit :
    a. Entrez un nom de flux de travail correspondant et une description facultative.
    b. Pour la saisie de données, choisissez une AWS Glue base de données dans la liste déroulante, sélectionnez la AWS Glue table, puis le mappage de schéma correspondant.

Vous pouvez ajouter jusqu'à 20 entrées de données.

c. L'option Normaliser les données est sélectionnée par défaut, afin que les entrées de données soient normalisées avant la mise en correspondance. Si vous ne souhaitez pas normaliser les données, désélectionnez l'option Normaliser les données.

   La correspondance basée sur l'apprentissage automatique ne fait que normaliserNom, Téléphone et. E-mails

d. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.

Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut `estentityresolution-matching-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.

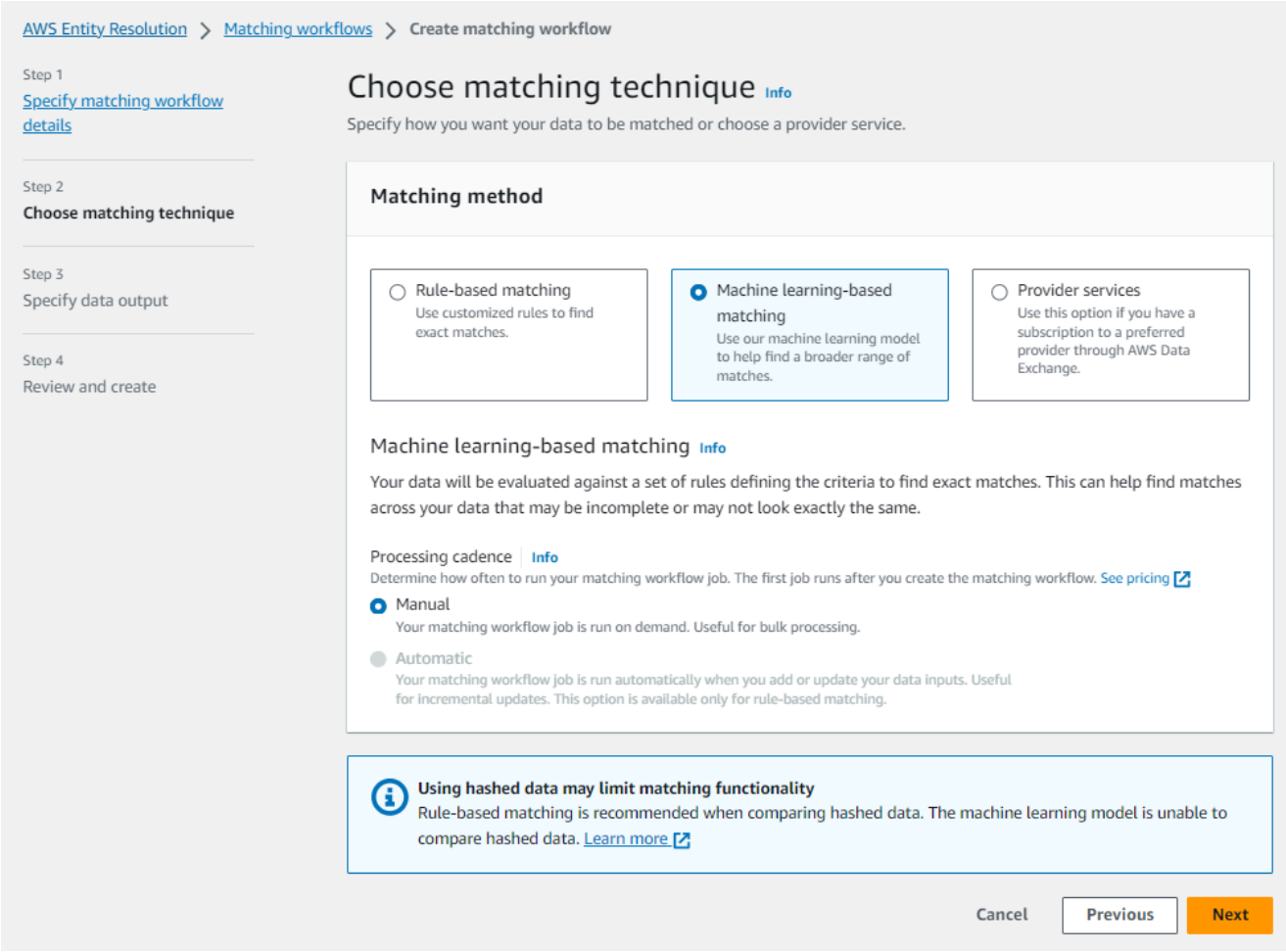
Option	Action recommandée
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

e. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

f. Choisissez Suivant.

5. Pour l'étape 2 : Choisissez la technique de correspondance :

   a. Pour la méthode de correspondance, choisissez la correspondance basée sur l'apprentissage automatique.



b. Pour Processing cadence, l'option Manuel est sélectionnée.

   Cette option vous permet d'exécuter un flux de travail à la demande pour une mise à jour groupée.

c. Choisissez Suivant.

6. Pour l'étape 3 : Spécifier la sortie et le format des données :

   a. Pour la destination et le format de sortie des données, choisissez l'emplacement Amazon S3 pour la sortie des données et indiquez si le format des données sera des données normalisées ou des données d'origine.

   b. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS cléARN.

   c. Affichez la sortie générée par le système.

   d. Pour la sortie de données, choisissez les champs que vous souhaitez inclure, masquer ou masquer, puis prenez les mesures recommandées en fonction de vos objectifs.

Votre objectif	Option recommandée
Inclure les champs	Conservez l'état de sortie sur Inclus.
Masquer les champs (exclure de la sortie)	Choisissez le champ de sortie, puis choisissez Masquer.
Champs de masque	Choisissez le champ Sortie, puis choisissez Hash output.
Réinitialisez les paramètres précédents	Choisissez Réinitialiser.

e. Choisissez Suivant.

7. Pour l'étape 4 : révision et création :

   a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

   b. Choisissez Créer et exécuter.

      Un message apparaît, indiquant que le flux de travail correspondant a été créé et que le travail a commencé.

8. Sur la page des détails du flux de travail correspondant, sous l'onglet Mesures, consultez les informations suivantes sous Dernières mesures de travail :

   - Le Job ID.
   - État de la tâche de flux de travail correspondante : En file d'attente, en cours, terminée, échouée
   - Durée d'exécution de la tâche de flux de travail.
   - Le nombre d'enregistrements traités.
   - Le nombre d'enregistrements non traités.
   - La correspondance unique IDs générée.
   - Le nombre d'enregistrements en entrée.

   Vous pouvez également consulter les statistiques des tâches correspondant aux tâches de flux de travail précédemment exécutées dans l'historique des tâches.

9. Une fois la tâche de flux de travail correspondante terminée (le statut est terminé), vous pouvez accéder à l'onglet Sortie de données, puis sélectionner votre site Amazon S3 pour afficher les résultats.
10. (Type de traitement manuel uniquement) Si vous avez créé un flux de travail de correspondance basé sur le machine learning avec le type de traitement manuel, vous pouvez exécuter le flux de travail correspondant à tout moment en choisissant Exécuter le flux de travail sur la page des détails du flux de travail correspondant.

Création d'un flux de travail de correspondance basé sur les services des fournisseurs

La mise en correspondance basée sur les services du fournisseur vous permet de faire correspondre vos identifiants connus à votre fournisseur de services de données préféré.

Résolution des entités AWS prend actuellement en charge les services de fournisseurs de données suivants :

- LiveRamp
- TransUnion
- Unified ID 2.0

Pour plus d'informations sur les services des fournisseurs pris en charge, consultezPréparation de données d'entrée tierces.

Vous pouvez utiliser un abonnement public pour ces fournisseurs AWS Data Exchange ou négocier une offre privée directement avec le fournisseur de données. Pour plus d'informations sur la création d'un nouvel abonnement ou la réutilisation d'un abonnement existant auprès d'un fournisseur de services, consultezÉtape 1 : Abonnez-vous à un service fournisseur sur AWS Data Exchange.

Les sections suivantes décrivent comment créer un flux de travail de correspondance basé sur le fournisseur.

Rubriques

- Création d'un flux de travail correspondant avec LiveRamp
- Création d'un flux de travail correspondant avec TransUnion
- Création d'un flux de travail correspondant avec UID 2.0

Création d'un flux de travail correspondant avec LiveRamp

Si vous êtes abonné au LiveRamp service, vous pouvez créer un flux de travail correspondant au LiveRamp service pour effectuer la résolution d'identité.

Le LiveRamp service fournit un identifiant appelé RAMPid. Le RamPid est l'un des plus couramment utilisés sur IDs les plateformes axées sur la demande pour créer une audience pour une campagne publicitaire. À l'aide d'un flux de travail correspondant avec LiveRamp, vous pouvez résoudre les adresses e-mail hachées enRAMPIDs.

> **Note**
>
> Résolution des entités AWS supporte l'attribution RampID PII basée sur le support.

Ce flux de travail nécessite un compartiment de transfert de données Amazon S3 dans lequel vous souhaitez que la sortie du flux de travail correspondante soit temporairement écrite. Avant de créer un flux de travail de mappage d'identifiants avec LiveRamp, ajoutez les autorisations suivantes au bucket de transit des données.

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

Remplacez chacun *<user input placeholder>* avec vos propres informations.

staging-bucket	Compartiment Amazon S3 qui stocke temporairement vos données lors de l'exécution d'un flux de travail basé sur les services d'un fournisseur.

Pour créer un flux de travail correspondant avec LiveRamp :

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS (si vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, sous Workflows, choisissez Matching.
3. Sur la page des flux de travail correspondants, dans le coin supérieur droit, choisissez Créer un flux de travail correspondant.
4. Pour l'étape 1 : Spécifier les détails du flux de travail correspondants, procédez comme suit :

    a. Entrez un nom de flux de travail correspondant et une description facultative.

    b. Pour la saisie de données, choisissez une AWS Glue base de données dans la liste déroulante, sélectionnez la AWS Glue table, puis sélectionnez le mappage de schéma correspondant.

Vous pouvez ajouter jusqu'à 20 entrées de données.

c. L'option Normaliser les données est sélectionnée par défaut, afin que les entrées de données soient normalisées avant la mise en correspondance.

   Si vous utilisez le processus de résolution par e-mail uniquement, désélectionnez l'option Normaliser les données, car seuls les e-mails hachés sont utilisés pour les données d'entrée.

d. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.

Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut `estentityresolution-matching-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.

Option	Action recommandée
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

e. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

f. Choisissez Suivant.

5. Pour l'étape 2 : Choisissez la technique de correspondance :

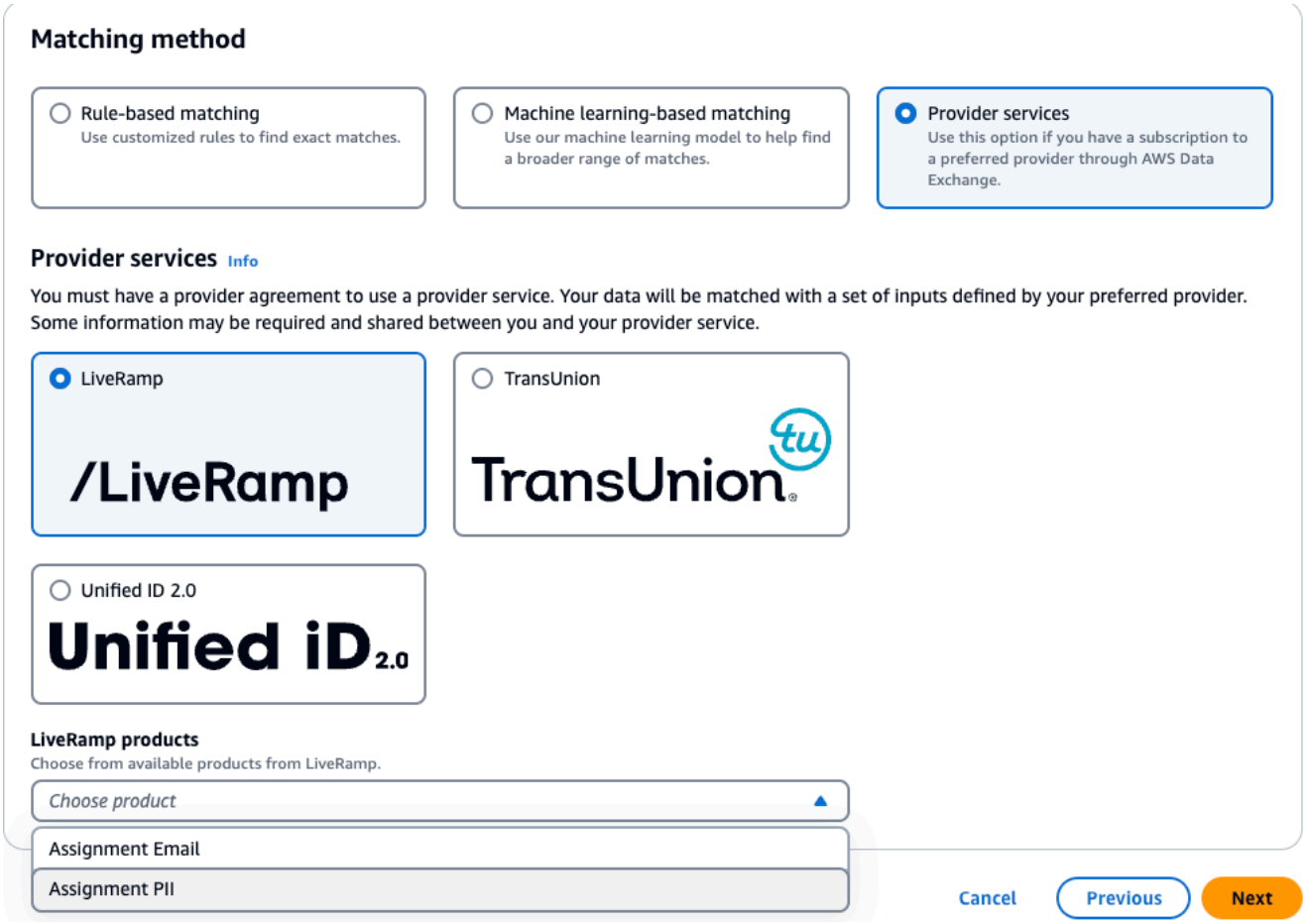
   a. Pour Méthode de correspondance, choisissez Provider services.

   b. Pour les services du fournisseur, sélectionnez LiveRamp.

> **Note**
>
> Assurez-vous que le format et la normalisation de votre fichier d'entrée de données sont conformes aux directives du fournisseur de services.

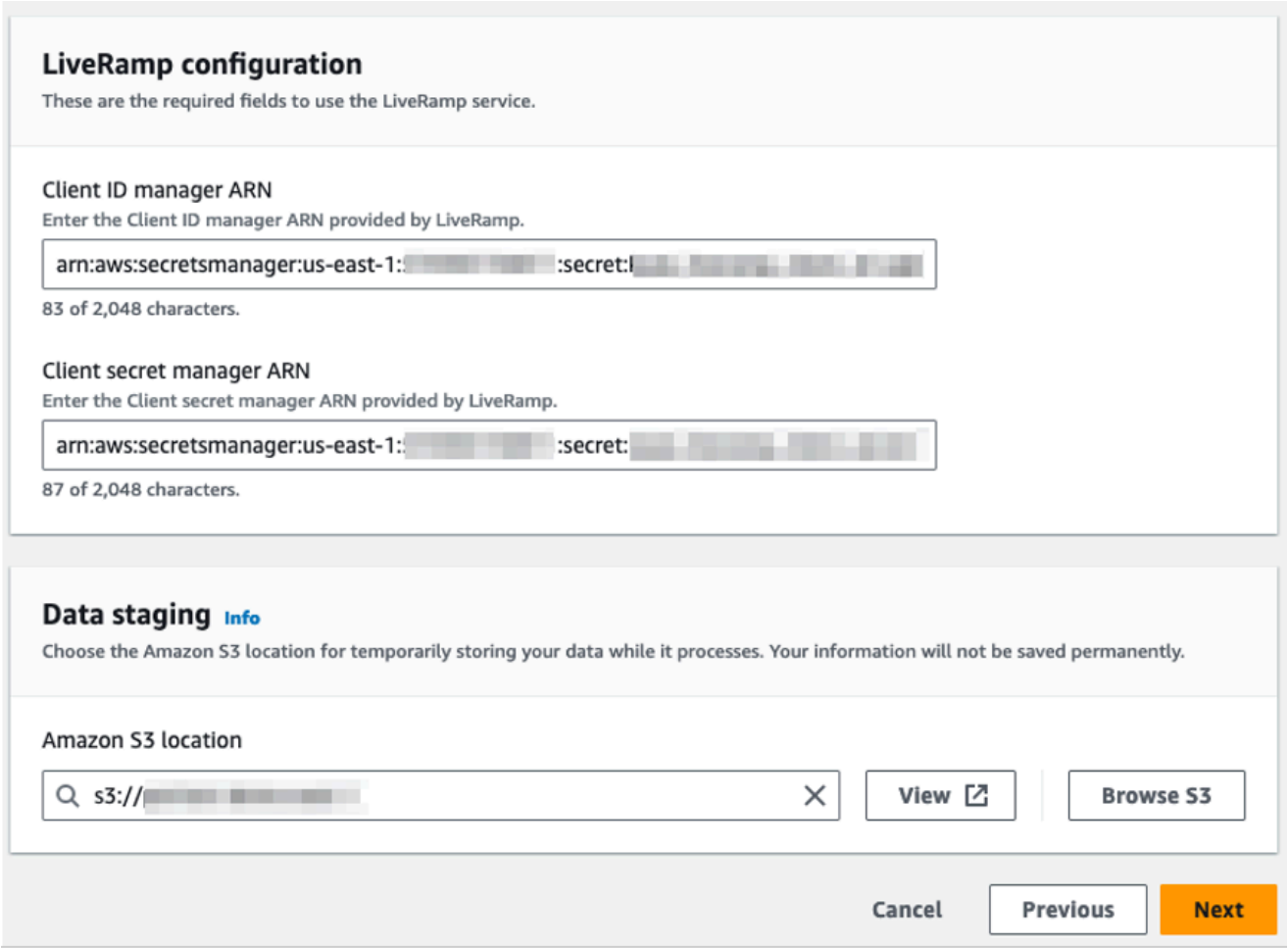
Pour plus d'informations sur les directives de formatage des fichiers d'entrée pour le flux de travail correspondant, voir Perform Identity Resolution ADX Through dans la LiveRamp documentation.

c. Pour les LiveRamp produits, choisissez-en un dans la liste déroulante.



> **Note**
>
> Si vous choisissez AffectationPII, vous devez fournir au moins une colonne sans identifiant lors de la résolution d'entités. Par exemple,GENDER.

d. Pour LiveRamp la configuration, entrez un gestionnaire d'ID client ARN et un gestionnaire de secret client ARN.



e. Pour le stockage des données, choisissez l'emplacement Amazon S3 pour le stockage temporaire de vos données pendant leur traitement.

   Vous devez être autorisé à transférer les données sur le site Amazon S3. Pour de plus amples informations, veuillez consulter Création d'un rôle de travail dans le flux de travail pour Résolution des entités AWS.

f. Choisissez Suivant.

6. Pour l'étape 3 : Spécifier les données de sortie :

   a. Pour la destination et le format de sortie des données, choisissez l'emplacement Amazon S3 pour la sortie des données et indiquez si le format des données sera des données normalisées ou des données d'origine.

   b. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS cléARN.

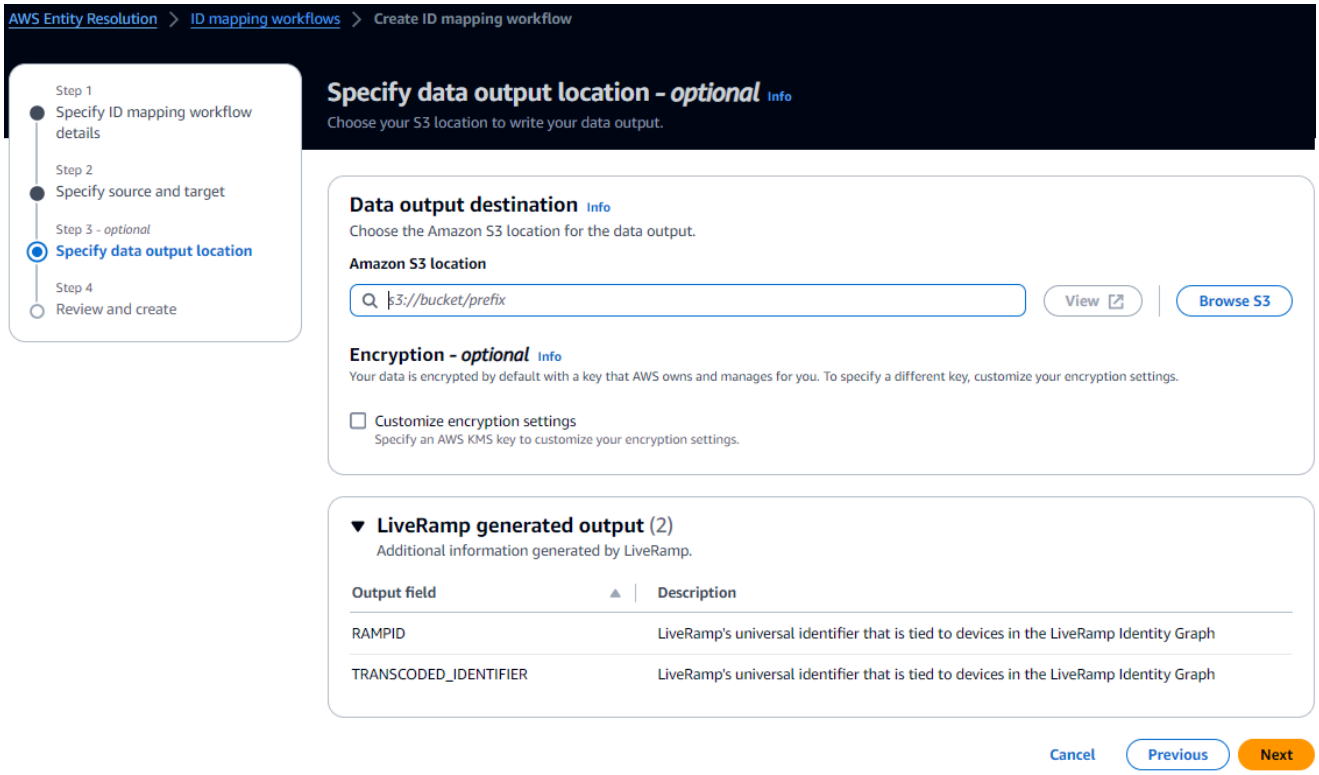
   c. Affichez le résultat LiveRamp généré.

Il s'agit des informations supplémentaires générées par LiveRamp.

d. Pour la sortie de données, choisissez les champs que vous souhaitez inclure, masquer ou masquer, puis prenez les mesures recommandées en fonction de vos objectifs.

> **Note**
>
> Si vous avez choisi LiveRamp, en raison des filtres de LiveRamp confidentialité qui suppriment les informations personnelles identifiables (PII), certains champs afficheront l'état de sortie Non disponible.

Votre objectif	Option recommandée
Inclure les champs	Conservez l'état de sortie sur Inclus.
Masquer les champs (exclure de la sortie)	Choisissez le champ de sortie, puis choisissez Masquer.
Champs de masque	Choisissez le champ Sortie, puis choisissez Hash output.
Réinitialisez les paramètres précédents	Choisissez Réinitialiser.



e. Choisissez Suivant.

7. Pour l'étape 4 : révision et création :

   a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

   b. Choisissez Créer et exécuter.

      Un message apparaît, indiquant que le flux de travail correspondant a été créé et que le travail a commencé.

8. Sur la page des détails du flux de travail correspondant, sous l'onglet Mesures, consultez les informations suivantes sous Dernières mesures de travail :

   - Le Job ID.
   - État de la tâche de flux de travail correspondante : En file d'attente, en cours, terminée, échouée
   - Durée d'exécution de la tâche de flux de travail.
   - Le nombre d'enregistrements traités.
   - Le nombre d'enregistrements non traités.

- La correspondance unique IDs générée.
- Le nombre d'enregistrements en entrée.

Vous pouvez également consulter les statistiques des tâches correspondant aux tâches de flux de travail précédemment exécutées dans l'historique des tâches.

9. Une fois la tâche de flux de travail correspondante terminée (le statut est terminé), vous pouvez accéder à l'onglet Sortie de données, puis sélectionner votre site Amazon S3 pour afficher les résultats.

Création d'un flux de travail correspondant avec TransUnion

Si vous êtes abonné au TransUnion service, vous pouvez améliorer la compréhension des clients en reliant, en mettant en correspondance et en améliorant les dossiers relatifs aux clients stockés sur des canaux disparates à l'aide de clés électroniques personnelles TransUnion et domestiques et de plus de 200 attributs de données.

Le TransUnion service fournit des identifiants appelés « TransUnion individu » et « ménage IDs ». TransUnion permet d'attribuer un identifiant (également appelé encodage) à des identifiants connus tels que le nom, l'adresse, le numéro de téléphone et l'adresse e-mail.

Ce flux de travail nécessite un compartiment de transfert de données Amazon S3 dans lequel vous souhaitez que la sortie du flux de travail correspondante soit temporairement écrite. Avant de créer un flux de travail correspondant avec TransUnion, ajoutez les autorisations suivantes au bucket de transit des données.

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

Remplacez chacun *<user input placeholder>* avec vos propres informations.

staging-bucket	Compartiment Amazon S3 qui stocke temporairement vos données lors de l'exécution d'un flux de travail basé sur les services d'un fournisseur.

Pour créer un flux de travail correspondant avec TransUnion :

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS (si vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, sous Workflows, choisissez Matching.
3. Sur la page des flux de travail correspondants, dans le coin supérieur droit, choisissez Créer un flux de travail correspondant.

4. Pour l'étape 1 : Spécifier les détails du flux de travail correspondants, procédez comme suit :

   a. Entrez un nom de flux de travail correspondant et une description facultative.

   b. Pour la saisie de données, choisissez une AWS Glue base de données dans la liste déroulante, sélectionnez la AWS Glue table, puis sélectionnez le mappage de schéma correspondant.

      Vous pouvez ajouter jusqu'à 20 entrées de données.

   c. L'option Normaliser les données est sélectionnée par défaut, afin que les entrées de données soient normalisées avant la mise en correspondance. Si vous ne souhaitez pas normaliser les données, désélectionnez l'option Normaliser les données.

   d. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.

Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut est `entityresolution-matching-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.

Option	Action recommandée
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

e. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

f. Choisissez Suivant.

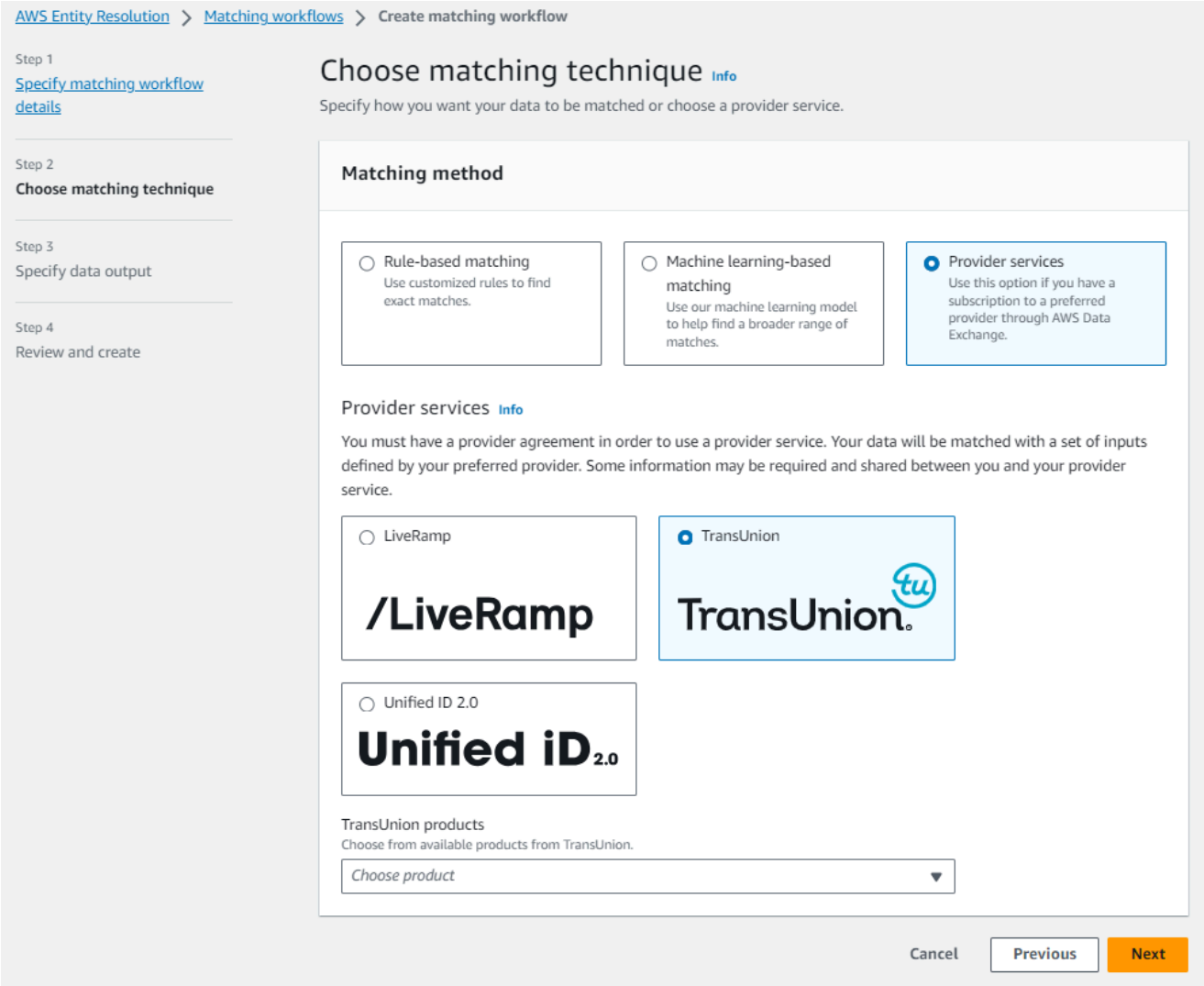
5. Pour l'étape 2 : Choisissez la technique de correspondance :

a. Pour Méthode de correspondance, choisissez Provider services.

b. Pour les services du fournisseur, sélectionnez TransUnion.

> **Note**
>
> Assurez-vous que le format et la normalisation de votre fichier d'entrée de données sont conformes aux directives du fournisseur de services.

c. Pour les TransUnion produits, choisissez-en un dans la liste déroulante.



d. Pour le stockage des données, choisissez l'emplacement Amazon S3 pour le stockage temporaire de vos données pendant leur traitement.

   Vous devez être autorisé à transférer les données sur le site Amazon S3. Pour de plus amples informations, veuillez consulter the section called “Création d'un rôle de travail dans le flux de travail”.

6. Choisissez Suivant.
7. Pour l'étape 3 : Spécifier les données de sortie :

   a. Pour la destination et le format de sortie des données, choisissez l'emplacement Amazon S3 pour la sortie des données et indiquez si le format des données sera des données normalisées ou des données d'origine.

b. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS cléARN.

c. Affichez le résultat TransUnion généré.

   Il s'agit des informations supplémentaires générées par TransUnion.

d. Pour la sortie de données, choisissez les champs que vous souhaitez inclure, masquer ou masquer, puis prenez les mesures recommandées en fonction de vos objectifs.

Votre objectif	Option recommandée
Inclure les champs	Conservez l'état de sortie sur Inclus.
Masquer les champs (exclure de la sortie)	Choisissez le champ de sortie, puis choisissez Masquer.
Champs de masque	Choisissez le champ Sortie, puis choisissez Hash output.
Réinitialisez les paramètres précédents	Choisissez Réinitialiser.

e. Pour la sortie générée par le système, consultez tous les champs inclus.

f. Choisissez Suivant.

8. Pour l'étape 4 : révision et création :

   a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

   b. Choisissez Créer et exécuter.

      Un message apparaît, indiquant que le flux de travail correspondant a été créé et que le travail a commencé.

9. Sur la page des détails du flux de travail correspondant, sous l'onglet Mesures, consultez les informations suivantes sous Dernières mesures de travail :

   - Le Job ID.
   - État de la tâche de flux de travail correspondante : En file d'attente, en cours, terminée, échouée
   - Durée d'exécution de la tâche de flux de travail.

- Le nombre d'enregistrements traités.
- Le nombre d'enregistrements non traités.
- La correspondance unique IDs générée.
- Le nombre d'enregistrements en entrée.

Vous pouvez également consulter les statistiques des tâches correspondant aux tâches de flux de travail précédemment exécutées dans l'historique des tâches.

10. Une fois la tâche de flux de travail correspondante terminée (le statut est terminé), vous pouvez accéder à l'onglet Sortie de données, puis sélectionner votre site Amazon S3 pour afficher les résultats.

Création d'un flux de travail correspondant avec UID 2.0

Si vous êtes abonné au service Unified ID 2.0, vous pouvez activer des campagnes publicitaires avec une identité déterministe et vous appuyer sur l'interopérabilité avec de nombreux UID2 participants actifs au sein de l'écosystème publicitaire. Pour plus d'informations, consultez la section Présentation d'Unified ID 2.0.

Le service Unified ID 2.0 fournit le format raw UID 2, qui est utilisé pour créer des campagnes publicitaires sur la plateforme The Trade Desk. UIDLa version 2.0 est générée à l'aide d'un framework open source.

Dans un flux de travail, vous pouvez utiliser l'un **`Email Address`** ou l'autre ou **`Phone number`** pour UID2 la génération brute, mais pas les deux. Si les deux sont présents dans le mappage du schéma, le flux de travail **`Phone number`** choisira le champ qui deviendra un champ direct. **`Email Address`** Pour prendre en charge les deux, créez un nouveau mappage de schéma où **`Phone number`** il est mappé mais **`Email Address`** pas mappé. Créez ensuite un deuxième flux de travail à l'aide de ce nouveau mappage de schéma.

> **Note**
>
> UID2sLes produits bruts sont créés en ajoutant des sels provenant de seaux à sel qui sont alternés environ une fois par an, ce qui permet de UID2 faire également tourner le brut avec celui-ci. Par conséquent, il est recommandé d'actualiser le RAW UID2s tous les jours. Pour plus d'informations, consultez https://unifiedid.com/docs/how-often-should-uidgetting-started/gs-faqs# 2 -incremental-updates. s-be-refreshed-for

Pour créer un flux de travail correspondant avec UID 2.0 :

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS (si vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, sous Workflows, choisissez Matching.
3. Sur la page des flux de travail correspondants, dans le coin supérieur droit, choisissez Créer un flux de travail correspondant.
4. Pour l'étape 1 : Spécifier les détails du flux de travail correspondants, procédez comme suit :

   a. Entrez un nom de flux de travail correspondant et une description facultative.

   b. Pour la saisie de données, choisissez une AWS Glue base de données dans la liste déroulante, sélectionnez la AWS Glue table, puis sélectionnez le mappage de schéma correspondant.

      Vous pouvez ajouter jusqu'à 20 entrées de données.

   c. Laissez l'option Normaliser les données sélectionnée afin que les entrées de données (**`Email Address`**ou**`Phone number`**) soient normalisées avant la mise en correspondance.

      Pour plus d'informations sur **`Email Address`** la normalisation, consultez la section Normalisation des adresses e-mail dans la documentation UID 2.0.

      Pour plus d'informations sur **`Phone number`** la normalisation, consultez la section Normalisation des numéros de téléphone dans la documentation UID 2.0.

   d. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.

Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut `estentityresolution-matching-workflow-<timestamp>` .

Option	Action recommandée
	• Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

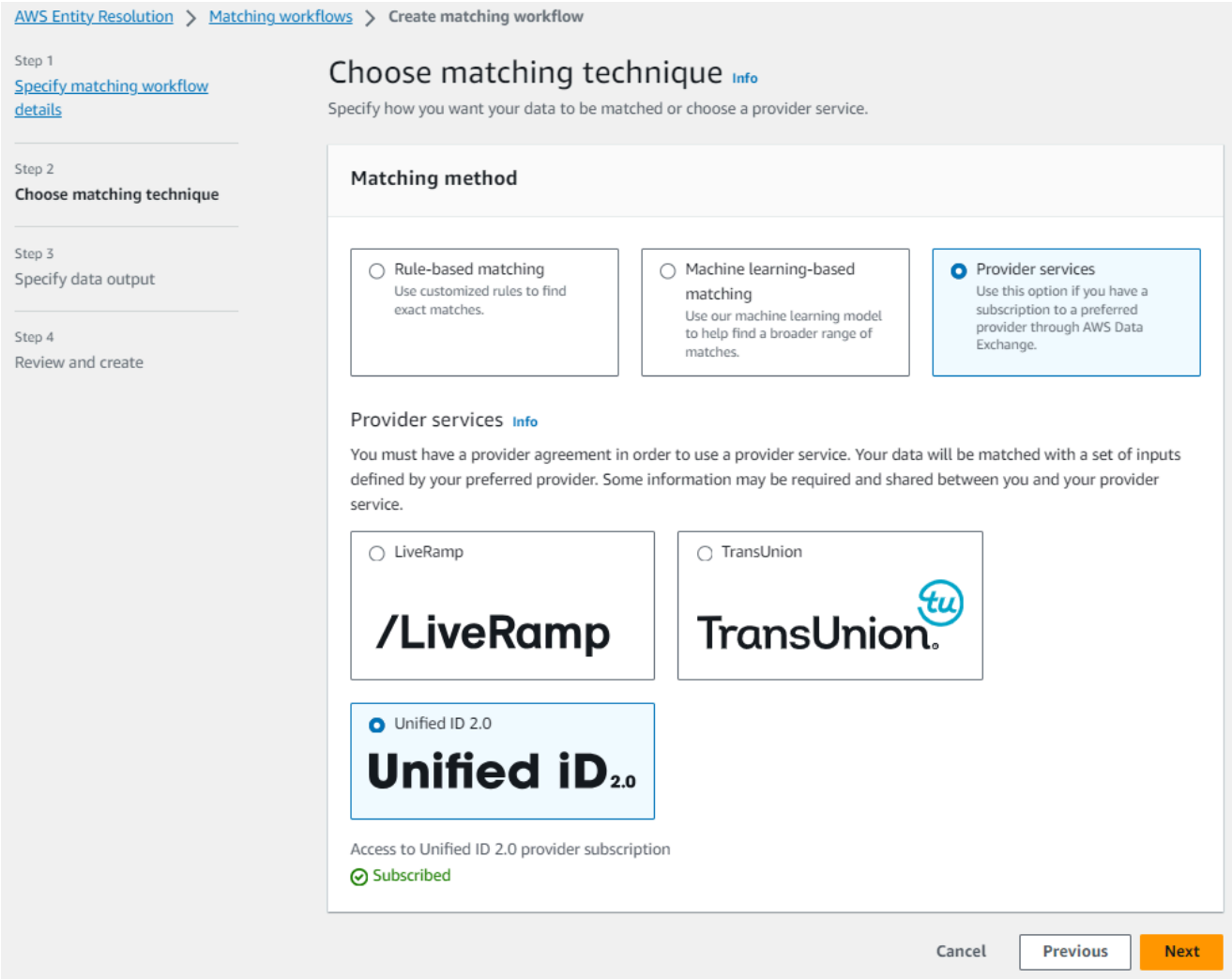
e. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

f. Choisissez Suivant.

5. Pour l'étape 2 : Choisissez la technique de correspondance :

a. Pour Méthode de correspondance, choisissez Provider services.

b. Pour les services du fournisseur, choisissez Unified ID 2.0.



c. Choisissez Suivant.

6. Pour l'étape 3 : Spécifier les données de sortie :

a. Pour la destination et le format de sortie des données, choisissez l'emplacement Amazon S3 pour la sortie des données et indiquez si le format des données sera des données normalisées ou des données d'origine.

b. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS cléARN.

c. Affichez la sortie générée par Unified ID 2.0.

   Il s'agit d'une liste de toutes les informations supplémentaires générées par UID 2.0

d. Pour la sortie de données, choisissez les champs que vous souhaitez inclure, masquer ou masquer, puis prenez les mesures recommandées en fonction de vos objectifs.

Votre objectif	Option recommandée
Inclure les champs	Conservez l'état de sortie sur Inclus.
Masquer les champs (exclure de la sortie)	Choisissez le champ de sortie, puis choisissez Masquer.
Champs de masque	Choisissez le champ Sortie, puis choisissez Hash output.
Réinitialisez les paramètres précédents	Choisissez Réinitialiser.

e. Pour la sortie générée par le système, consultez tous les champs inclus.

f. Choisissez Suivant.

7. Pour l'étape 4 : révision et création :

   a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

   b. Choisissez Créer et exécuter.

      Un message apparaît, indiquant que le flux de travail correspondant a été créé et que le travail a commencé.

8. Sur la page des détails du flux de travail correspondant, sous l'onglet Mesures, consultez les informations suivantes sous Dernières mesures de travail :

   - Le Job ID.
   - État de la tâche de flux de travail correspondante : En file d'attente, en cours, terminée, échouée
   - Durée d'exécution de la tâche de flux de travail.
   - Le nombre d'enregistrements traités.
   - Le nombre d'enregistrements non traités.
   - La correspondance unique IDs générée.
   - Le nombre d'enregistrements en entrée.

Vous pouvez également consulter les statistiques des tâches correspondant aux tâches de flux de travail précédemment exécutées dans l'historique des tâches.

9. Une fois la tâche de flux de travail correspondante terminée (le statut est terminé), vous pouvez accéder à l'onglet Sortie de données, puis sélectionner votre site Amazon S3 pour afficher les résultats.

Modification d'un flux de travail correspondant

La modification du flux de travail correspondant vous permet de maintenir vos processus de résolution des entités up-to-date et de répondre aux exigences changeantes de votre organisation au fil du temps. Vous souhaiterez peut-être ajuster les critères de correspondance, les techniques ou les sorties de données afin d'améliorer la précision et l'efficacité du processus de résolution des entités. Si vous identifiez des problèmes ou des erreurs dans les résultats du flux de travail actuel, le fait de le modifier peut vous aider à diagnostiquer et à résoudre ces problèmes.

Pour modifier un flux de travail correspondant :

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez Matching.
3. Choisissez le flux de travail correspondant.
4. Sur la page des détails du flux de travail correspondant, dans le coin supérieur droit, choisissez Modifier.
5. Sur la page Spécifier les détails du flux de travail correspondant, apportez les modifications nécessaires, puis choisissez Suivant.
6. Sur la page Choisir une technique de correspondance, apportez les modifications nécessaires, puis choisissez Suivant.
7. Sur la page Spécifier les données de sortie, apportez les modifications nécessaires, puis choisissez Next.
8. Sur la page Réviser et enregistrer, apportez les modifications nécessaires, puis choisissez Enregistrer.

Supprimer un flux de travail correspondant

Si un flux de travail correspondant n'est plus utilisé ou est devenu obsolète, sa suppression peut vous aider à garder votre espace de travail organisé et épuré. Si vous avez développé un nouveau flux de travail amélioré qui remplace un ancien, la suppression de l'ancien peut vous permettre de n'utiliser que le plus grand nombre de up-to-date processus.

Pour supprimer un flux de travail correspondant :

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez Matching.
3. Choisissez le flux de travail correspondant.
4. Sur la page des détails du flux de travail correspondant, dans le coin supérieur droit, choisissez Supprimer.
5. Confirmez la suppression, puis choisissez Supprimer.

Trouver un identifiant de correspondance pour un flux de travail de correspondance basé sur des règles

Après avoir exécuté un flux de travail de correspondance basé sur des règles, vous pouvez trouver l'ID de correspondance correspondant et la règle associée pour les enregistrements traités.

Pour trouver un identifiant de correspondance pour un flux de travail de correspondance basé sur des règles :

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez Matching.
3. Choisissez le flux de travail de correspondance basé sur des règles qui a été traité (le statut du Job est terminé).
4. Sur la page des détails du flux de travail correspondant, choisissez l'onglet Rechercher un identifiant de correspondance.
5. Effectuez l'une des actions suivantes :

Si...	Alors...
Un seul mappage de schéma est associé à ce flux de travail.	Affichez le mappage du schéma sélectionné par défaut.
Plusieurs mappages de schéma sont associés à ce flux de travail.	Choisissez le mappage du schéma dans la liste déroulante.

6. Développez les règles de correspondance.
7. Entrez une valeur pour chaque clé de correspondance.

   L'option Normaliser les données est sélectionnée par défaut, afin que les entrées de données soient normalisées avant la mise en correspondance. Si vous ne souhaitez pas normaliser les données, désélectionnez l'option Normaliser les données.

   > **Tip**
   >
   > Entrez autant de valeurs que possible pour aider à trouver le Match ID.

8. Choisissez Recherche.
9. Affichez l'ID de correspondance correspondant et la règle associée qui a été utilisée pour le rapprochement.

Suppression d'enregistrements d'un flux de travail de correspondance basé sur des règles ou basé sur le ML

Si vous devez respecter les réglementations relatives à la gestion des données, vous pouvez supprimer les enregistrements d'un flux de travail de correspondance basé sur des règles ou basé sur le ML.

Pour supprimer des enregistrements d'un flux de travail de correspondance basé sur des règles ou basé sur le ML

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez Matching.

3. Choisissez le flux de travail de correspondance basé sur des règles ou basé sur le ML.
4. Sur la page des détails du flux de travail correspondant, choisissez Supprimer l'unique IDs dans la liste déroulante Actions.
5. Entrez l'identifiant unique que vous souhaitez supprimer dans la IDs section Unique.

   Vous pouvez saisir jusqu'à 10 uniquesIDs.
6. Spécifiez la source d'entrée à partir de laquelle vous souhaitez supprimer l'uniqueIDs.

   S'il n'existe qu'une seule source d'entrée pour le flux de travail, la source d'entrée est répertoriée par défaut.

   Si vous ne spécifiez qu'une seule source d'entrée, IDs l'unique des autres sources d'entrée ne sera pas affectée.
7. Choisissez Supprimer l'unique IDs.

Résolution des problèmes liés aux workflows correspondants

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'exécution de flux de travail correspondants.

J'ai reçu un fichier d'erreur après avoir exécuté un flux de travail correspondant

Cause commune

Un flux de travail correspondant peut comporter plusieurs exécutions et les résultats (réussites ou erreurs) sont écrits dans un dossier portant le `jobId` nom.

Les résultats positifs d'un flux de travail correspondant sont écrits `success` dans un dossier contenant plusieurs fichiers, et chaque fichier contient un sous-ensemble des enregistrements réussis.

Les erreurs associées à un flux de travail correspondant sont enregistrées `error` dans un dossier contenant plusieurs champs, chacun contenant un sous-ensemble des enregistrements d'erreurs.

Le fichier d'erreur peut être créé pour les raisons suivantes :

- L'identifiant unique est le suivant :

- null
- manquant dans une ligne de données
- absent d'un enregistrement de la table de données
- répété dans une autre ligne de données du tableau de données
- non précisé
- pas unique au sein de la même source
- pas unique parmi plusieurs sources
- chevauchements entre les sources
- dépasse 38 caractères (flux de travail de correspondance basé sur des règles uniquement)

- L'un des champs du mappage du schéma inclut un nom réservé :
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - Identifiant du match
  - HashingProtocol
  - ConfidenceLevel
  - Source

> **Note**
>
> Si l'enregistrement dans le fichier d'erreur est créé pour les raisons énumérées précédemment, vous êtes facturé, car cela entraîne des frais de traitement pour le service. Si l'enregistrement dans le fichier d'erreur est dû à une erreur interne du serveur, vous n'êtes pas débité.

Résolution

Pour résoudre ce problème

1. Vérifiez si l'identifiant unique est valide.

Si l'identifiant unique n'est pas valide, mettez-le à jour dans votre table de données, enregistrez la nouvelle table de données, créez un nouveau mappage de schéma et réexécutez le flux de travail correspondant.

2. Vérifiez si l'un des champs du mappage du schéma inclut un nom réservé.

   Si l'un des champs inclut un nom réservé, créez un nouveau mappage de schéma avec un nouveau nom, puis réexécutez le flux de travail correspondant.

Mapper les données d'entrée à l'aide d'un flux de travail de mappage

Un flux de travail de mappage d'ID est une tâche de traitement de données qui mappe les données d'une source de données d'entrée vers une cible de données d'entrée en fonction de la méthode de mappage d'ID spécifiée. Il produit une table de mappage des identifiants.

Un flux de travail de mappage d'identifiants nécessite une source de données d'entrée et une cible de données d'entrée. La source et la cible de vos données d'entrée dépendent du type de mappage d'identifiants que vous souhaitez effectuer. Il existe deux méthodes pour effectuer le mappage des identifiants : les services basés sur des règles ou les services du fournisseur :

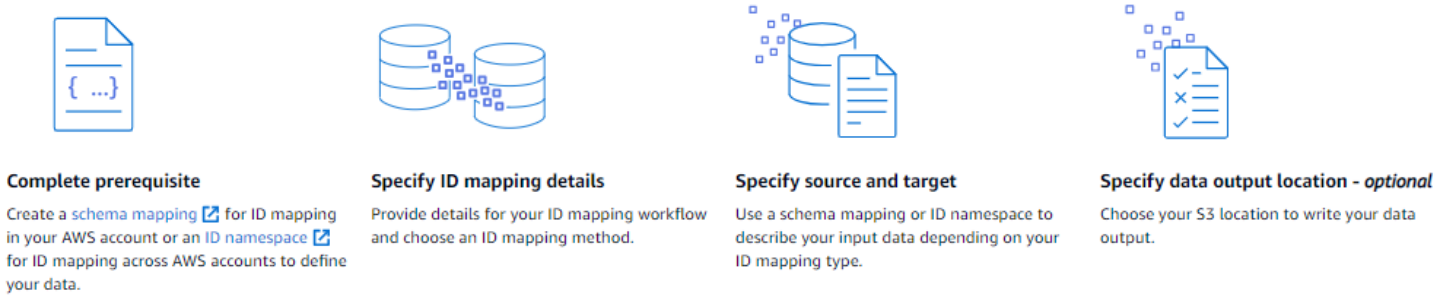
- Mappage des identifiants basé sur des règles : vous utilisez des règles de correspondance pour traduire les données de première partie d'une source vers une cible.
- Mappage des identifiants des services du LiveRamp fournisseur : vous utilisez le service du fournisseur pour traduire des données tierces d'une source vers une cible.

> **Note**
>
> Le flux de travail de mappage des identifiants des services fournisseurs dans Résolution des entités AWS est actuellement intégré à LiveRamp. Si vous êtes abonné au LiveRamp service, vous pouvez créer un flux de travail de mappage d'identifiants LiveRamp pour effectuer le transcodage. Avec le LiveRamp transcodage, vous pouvez traduire un ensemble de sources R ampIDs en n'importe quel RampID de destination cible. En utilisant le RamPid comme jeton pour représenter vos clients, vous pouvez éviter de partager les données des clients directement avec les plateformes publicitaires.
> Pour plus d'informations, consultez Perform Translation Through ADX sur le site Web de LiveRamp documentation.

Vous pouvez effectuer un mappage d'ID entre deux ensembles de données dans l'un des scénarios suivants :

- Au sein du vôtre Compte AWS
- À travers deux modèles différents Comptes AWS

Le schéma suivant explique comment configurer un flux de travail de mappage d'identifiants.



Rubriques

- Workflow de mappage d'identité pour une personne Compte AWS
- Flux de travail de mappage des identifiants sur deux Comptes AWS
- Exécuter un flux de travail de mappage d'identifiants
- Exécution d'un flux de travail de mappage d'identifiants avec une nouvelle destination de sortie
- Modification d'un flux de travail de mappage d'identifiants
- Supprimer un flux de travail de mappage d'identifiants
- Ajouter ou mettre à jour une politique de ressources pour un flux de travail de mappage d'identifiants

Workflow de mappage d'identité pour une personne Compte AWS

Un flux de travail de mappage d'identifiants vous Compte AWS permet d'effectuer vous-même le mappage d'identifiants entre deux ensembles de données. Compte AWS

Avant de créer vous-même un flux de travail de mappage d'identifiants Compte AWS, vous devez d'abord remplir les conditions préalables.

Après avoir créé et exécuté un flux de travail de mappage d'ID, vous pouvez afficher le résultat (la table de mappage d'ID) et l'utiliser à des fins d'analyse.

Les rubriques suivantes vous guident à travers une série d'étapes pour créer un flux de travail de mappage d'identifiants dans le même flux de travail Compte AWS.

Rubriques

- Prérequis

- Création d'un flux de travail de mappage d'identifiants (basé sur des règles)
- Création d'un flux de travail de mappage d'identifiants (services aux fournisseurs)

Prérequis

Avant de créer un flux de travail de mappage des identifiants pour un utilisateur Compte AWS utilisant la méthode de mappage des identifiants basée sur des règles ou la méthode de mappage des identifiants des fournisseurs de services, vous devez d'abord effectuer les opérations suivantes :

- Effectuez les tâches de la section Configuration de la résolution des AWS entités.
- Créez un mappage de schéma ou créez un flux de travail correspondant.
- (Mappage d'ID pour les services des fournisseurs uniquement) Avant de créer un flux de travail de mappage d'ID avec LiveRamp, vous devez choisir un bucket de stockage de données Amazon Simple Storage Service (Amazon S3) dans lequel vous souhaitez écrire temporairement le résultat du flux de mappage d'ID.

  Si vous utilisez le service du LiveRamp fournisseur pour traduire des données tierces, ajoutez la politique d'autorisation suivante, qui vous permet d'accéder au bucket de transit des données.

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

Dans la politique d'autorisation précédente, remplacez chaque *<user input placeholder>* avec vos propres informations.

staging-bucket	Le compartiment Amazon S3 qui stocke temporairement vos données lors de l'exécuti on d'un flux de travail basé sur les services d'un fournisseur.

Création d'un flux de travail de mappage d'identifiants (basé sur des règles)

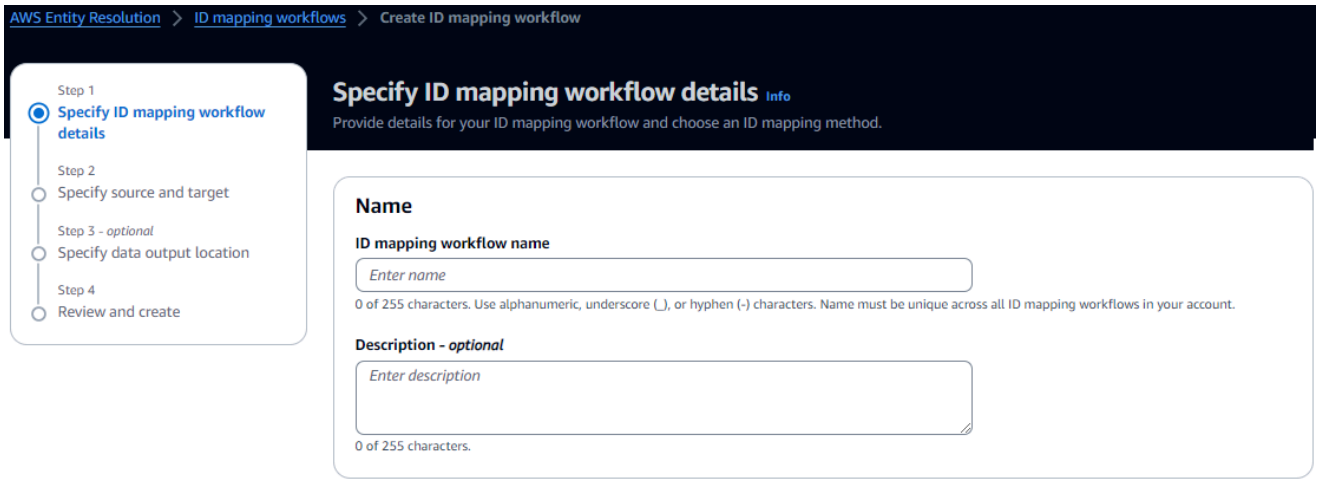
Cette rubrique décrit le processus de création d'un flux de travail de mappage d'identifiants pour un flux de travail Compte AWS qui utilise des règles de correspondance pour traduire des données de première partie d'une source vers une cible.

Pour créer un flux de travail de mappage des identifiants basé sur des règles pour un Compte AWS

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez ID mapping.

3. Sur la page des flux de travail de mappage des identifiants, dans le coin supérieur droit, choisissez Créer un flux de travail de mappage des identifiants.
4. Pour l'étape 1 : Spécifier les détails du flux de travail de mappage des identifiants, procédez comme suit.

   a. Entrez un nom de flux de travail de mappage d'identifiants et une description facultative.



   b. Pour la méthode de mappage des identifiants, choisissez Basée sur des règles.

   c. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

   d. Choisissez Suivant.

5. Pour l'étape 2 : Spécifier la source et la cible, procédez comme suit.

   a. Pour Source, choisissez le scénario qui s'applique à vous, puis prenez les mesures recommandées.

Scénario	Action recommandée
Utilisez votre propre base de données AWS Glue, votre table AWS Glue et votre propre mappage de schéma dans le flux de travail de mappage des identifiants.	1. Choisissez Schema mapping. 2. Sélectionnez une AWS Gluebase de données dans la liste déroulante, sélectionnez la AWS Glue table, puis sélectionnez le mappage de schéma correspondant.

Scénario	Action recommandée
	Vous pouvez ajouter jusqu'à 19 entrées de données.
Utilisez un flux de travail de correspon dance existant qui pointe vers les données d'enregistrement que vous souhaitez utiliser dans le flux de travail de mappage des identifiants.	1. Choisissez Matching Workflow. 2. Sélectionnez un flux de travail correspon dant existant dans la liste déroulante.

b. Pour Target, sélectionnez un flux de travail correspondant existant dans la liste déroulante.

c. Pour les paramètres de règle, procédez comme suit.

i. Spécifiez les contrôles de règle en choisissant l'une des options suivantes en fonction de votre type de source.

Source type (Type de source)	Action recommandée
Flux de travail correspondant	Spécifiez les contrôles de règle en choisissant si une source, une cible ou les deux peuvent fournir des règles dans un flux de travail de mappage d'identif iants. Les contrôles de règles doivent être compatibles entre la source et la cible pour être utilisés dans un flux de travail de mappage d'identifiants. Par exemple, si un espace de noms d'ID source limite les règles à la cible mais que l'espace de noms d'ID cible limite les règles à la source, cela entraîne une erreur.
Cartographie du schéma	Ignorez cette étape.

ii. Pour les paramètres de comparaison et de correspondance, le type de comparaison est automatiquement défini sur Plusieurs champs de saisie.

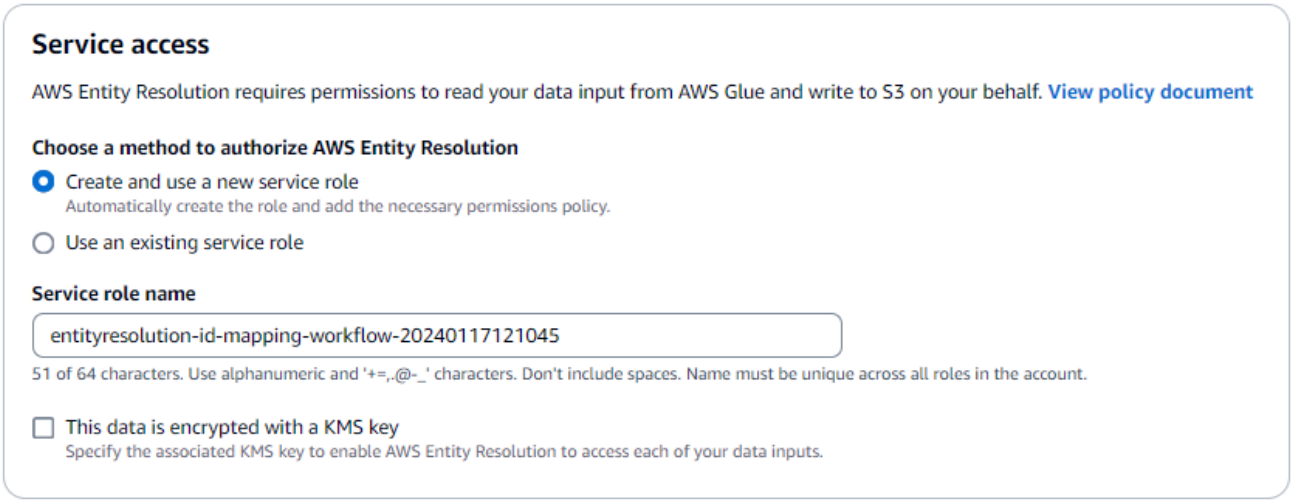
Cela est dû au fait que les deux participants avaient précédemment sélectionné cette option.

d. Spécifiez le type de correspondance des enregistrements en choisissant l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Limitez le type de correspondance d'enregistrements afin de ne stocker qu'un seul enregistrement correspondant dans la source pour chaque enregistrement correspondant dans la cible lorsque vous créez le flux de travail de mappage d'identifiants.	Une source pour une cible
Limitez le type de correspondance d'enregistrements afin de stocker tous les enregistrements correspondants dans la source pour chaque enregistrement correspondant dans la cible lorsque vous créez le flux de travail de mappage d'identifiants.	De nombreuses sources pour une seule cible

> **Note**
>
> Vous devez spécifier des limites compatibles pour les espaces de noms d'ID source et cible.

e. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.



Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut est `entityresolution-id-mapping-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.

Option	Action recommandée
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

6. Choisissez Suivant.
7. Pour l'étape 3 : Spécifier l'emplacement de sortie des données. Procédez comme suit si vous le souhaitez.
   a. Pour Destination de sortie des données, procédez comme suit :
      i. Choisissez l'emplacement Amazon S3 pour la sortie des données.
      ii. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS clé ARN ou choisissez Créer une AWS KMS clé.
   b. Choisissez Suivant.
8. Pour l'étape 4 : révision et création, procédez comme suit.
   a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

b. Sélectionnez Create (Créer).

   Un message apparaît, indiquant que le flux de travail de mappage des identifiants a été créé.

Après avoir créé le flux de travail de mappage des identifiants, vous êtes prêt à exécuter un flux de travail de mappage des identifiants.

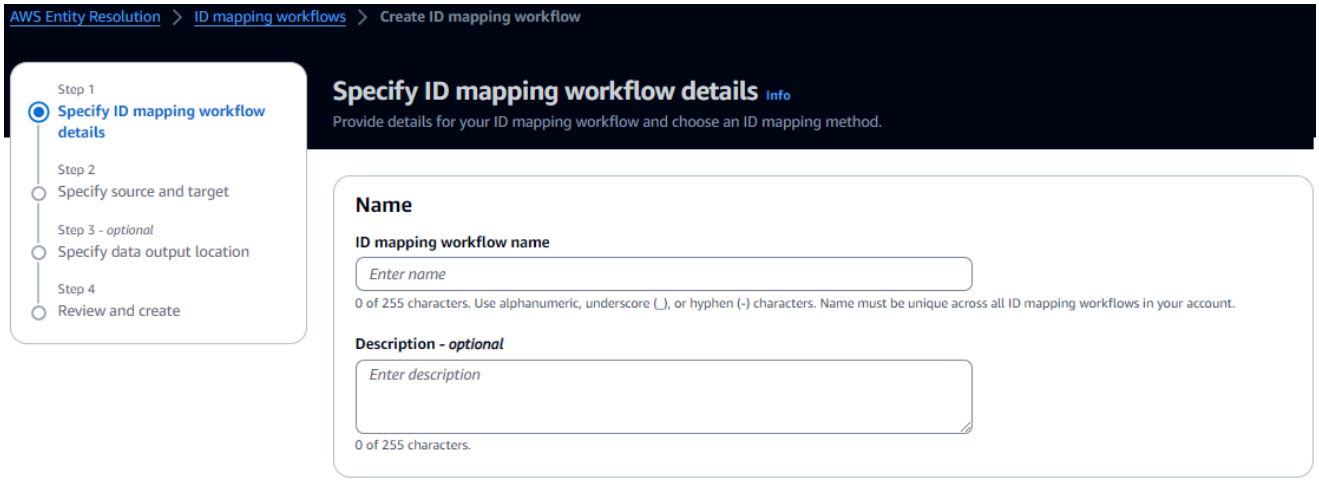
Création d'un flux de travail de mappage d'identifiants (services aux fournisseurs)

Cette rubrique décrit le processus de création d'un flux de travail de mappage d'identifiants pour un utilisateur Compte AWS utilisant un service fournisseur appelé LiveRamp. LiveRamp traduit un ensemble de R source ampIDs en un autre ensemble en utilisant R maintenu ou dérivéampIDs.

Pour créer un flux de travail de mappage des identifiants basé sur les services des fournisseurs pour un Compte AWS

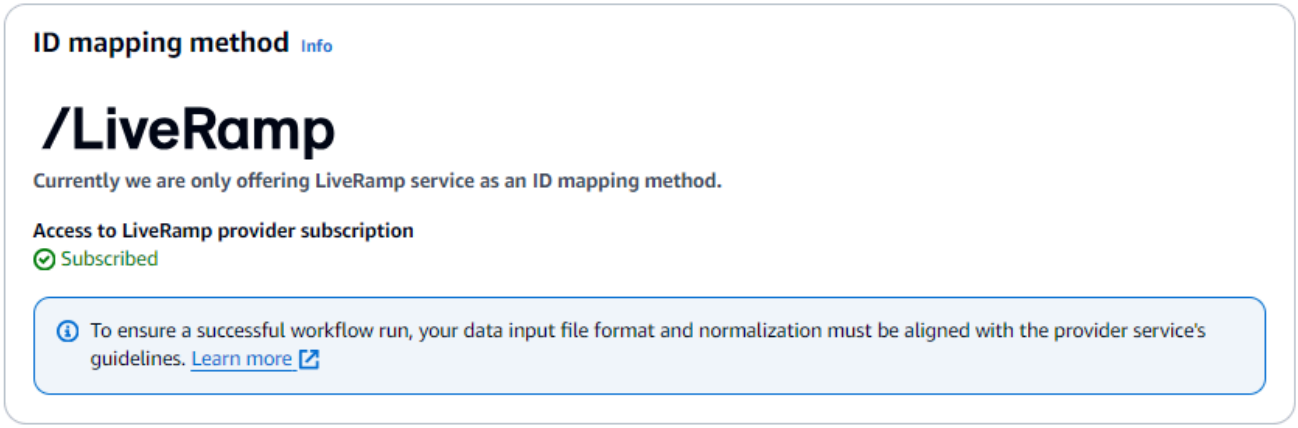
1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez ID mapping.
3. Sur la page des flux de travail de mappage des identifiants, dans le coin supérieur droit, choisissez Créer un flux de travail de mappage des identifiants.
4. Pour l'étape 1 : Spécifier les détails du flux de travail de mappage des identifiants, procédez comme suit.

   a. Entrez un nom de flux de travail de mappage d'identifiants et une description facultative.



b. Pour la méthode de mappage des identifiants, choisissez Provider services.

Résolution des entités AWS propose actuellement le service du LiveRamp fournisseur en tant que méthode de mappage d'identifiants. Si vous êtes abonné à LiveRamp, le statut apparaît comme Abonné. Pour plus d'informations sur la façon de s'abonner à LiveRamp, consultez[Étape 1 : Abonnez-vous à un service fournisseur sur AWS Data Exchange](#).



> **Note**
>
> Assurez-vous que le format de votre fichier de saisie de données est conforme aux directives du fournisseur de services. Pour plus d'informations sur les directives LiveRamp de formatage des fichiers d'entrée, voir Perform Translation Through ADX sur le site Web de LiveRamp documentation.

c. Pour LiveRamp la configuration, entrez les valeurs suivantes qui LiveRamp fournissent :

- Gestionnaire d'identifiants clients ARN
- Gestionnaire des secrets clients ARN

d. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

e. Choisissez Suivant.

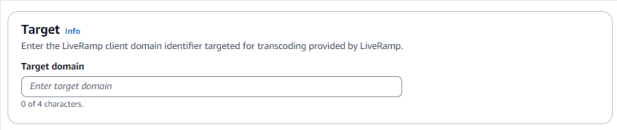
5. Pour l'étape 2 : Spécifier la source et la cible, procédez comme suit.

a. Pour Source, choisissez le scénario qui s'applique à vous, puis prenez les mesures recommandées.

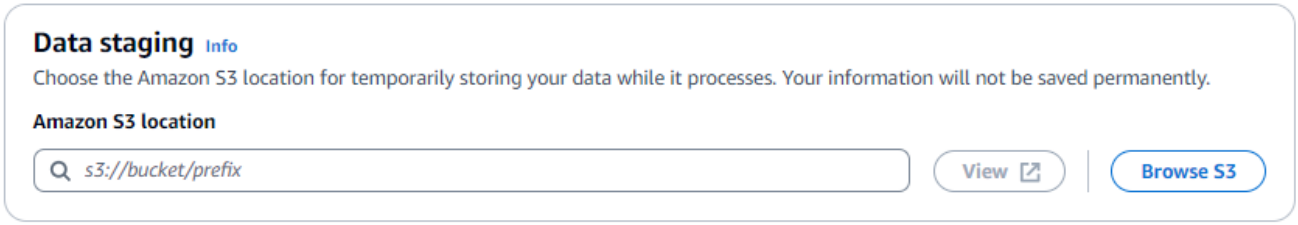
Scénario	Action recommandée
Utilisez votre propre base de données AWS Glue, votre table AWS Glue et votre propre mappage de schéma dans le flux de travail de mappage des identifiants.	1. Choisissez Schema mapping. 2. Sélectionnez une AWS Gluebase de données dans la liste déroulante, sélectionnez la AWS Glue table, puis sélectionnez le mappage de schéma correspondant. Vous pouvez ajouter jusqu'à 19 entrées de données.
Utilisez un flux de travail de correspon dance existant qui pointe vers les données d'enregistrement que vous souhaitez	1. Choisissez Matching Workflow.

Scénario	Action recommandée
utiliser dans le flux de travail de mappage des identifiants.	2. Sélectionnez un flux de travail correspon dant existant dans la liste déroulante.

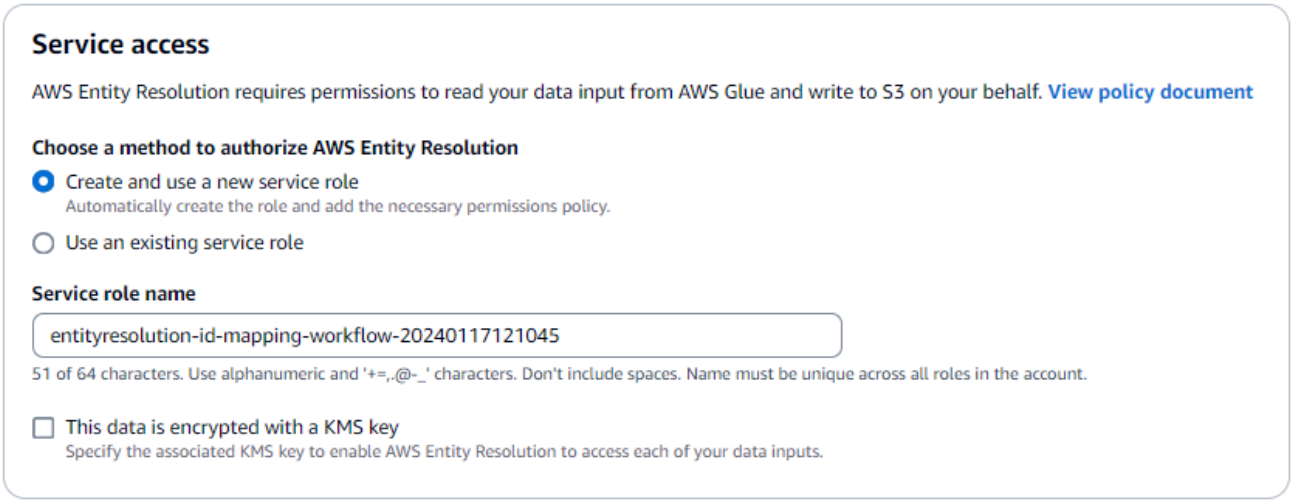
b. Pour Target, effectuez l'une des actions suivantes en fonction de la méthode de mappage d'identifiants que vous avez choisie.

Méthode de mappage des identifiants	Action recommandée
Basé sur des règles	Sélectionnez un flux de travail correspon dant existant dans la liste déroulante.
Services fournis par les fournisseurs	Entrez l'identifiant de domaine LiveRamp client ciblé pour le transcodage qui est LiveRamp fourni dans le domaine cible. 

c. Pour le Data staging, choisissez l'emplacement Amazon S3 où vous souhaitez écrire temporairement le résultat du flux de travail de mappage d'identifiants.



d. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.



Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut est `entityresolution-id-mapping-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.

Option	Action recommandée
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

6. Choisissez Suivant.
7. Pour l'étape 3 : Spécifier l'emplacement de sortie des données. Procédez comme suit si vous le souhaitez.

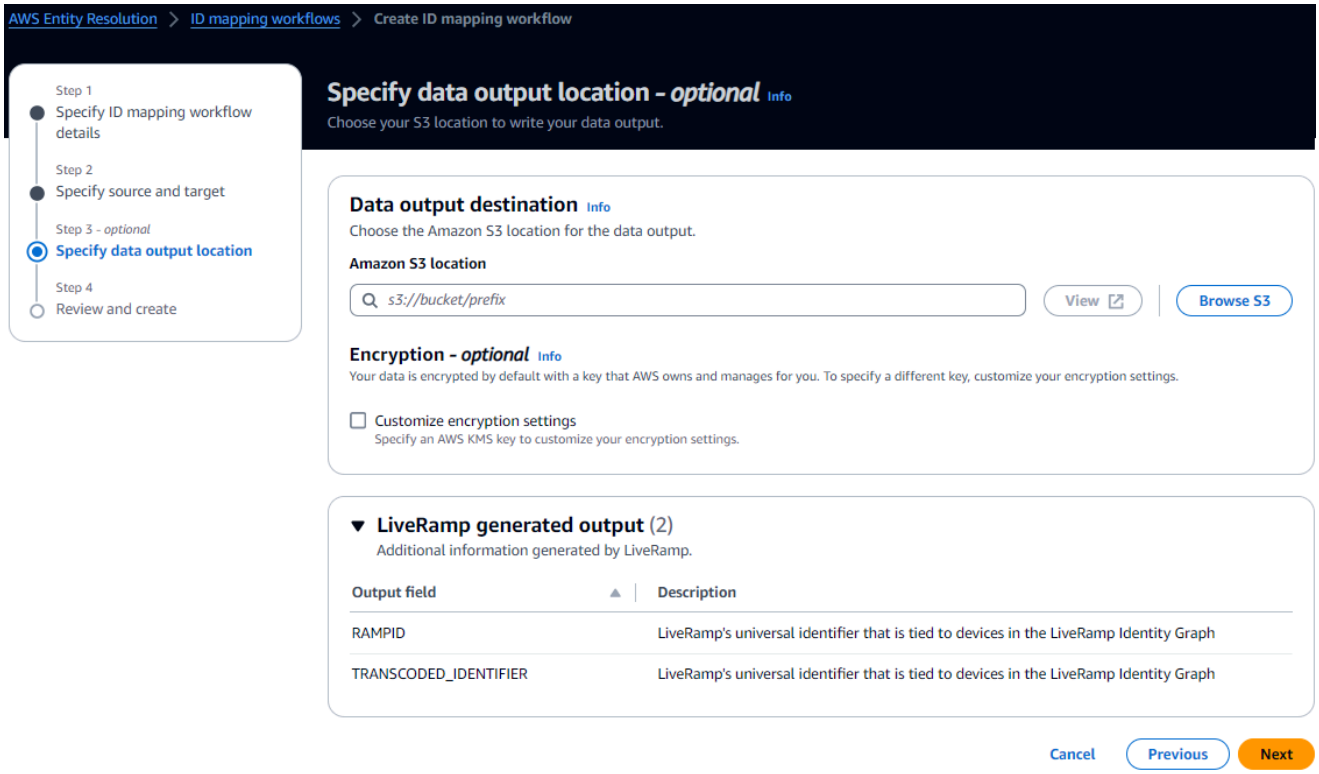
   a. Pour Destination de sortie des données, procédez comme suit :

      i. Choisissez l'emplacement Amazon S3 pour la sortie des données.

      ii. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS clé ARN ou choisissez Créer une AWS KMS clé.

   b. Affichez le résultat LiveRamp généré.

   c. Choisissez Suivant.



8. Pour l'étape 4 : révision et création, procédez comme suit.

   a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

   b. Sélectionnez Create (Créer).

      Un message apparaît, indiquant que le flux de travail de mappage des identifiants a été créé.

9. Après avoir créé le flux de travail de mappage des identifiants, vous êtes prêt à exécuter un flux de travail de mappage des identifiants.

Flux de travail de mappage des identifiants sur deux Comptes AWS

Un flux de travail de mappage d'ID sur deux vous Comptes AWS permet d'effectuer un mappage d'ID entre deux ensembles de données sur deux Comptes AWS. Cela se fait généralement entre le vôtre Compte AWS et un autre Compte AWS.

Par exemple, un éditeur peut créer un flux de travail de mappage d'identifiants en utilisant son propre espace de noms d'ID cible (dans le sien Compte AWS) et l'espace de noms d'identifiant source d'un annonceur (dans un autre). Compte AWS

Avant de créer un flux de travail de mappage d'identifiants sur deux Comptes AWS, vous devez d'abord remplir les conditions préalables.

Après avoir créé un flux de travail de mappage d'ID, vous pouvez afficher le résultat (la table de mappage d'ID) et l'utiliser pour l'analyse.

Les rubriques suivantes vous guident à travers une série d'étapes pour créer un flux de travail de mappage d'identifiants en deux parties Comptes AWS :

Rubriques

Prérequis

Avant de créer un flux de travail de mappage d'identifiants sur deux Comptes AWS, vous devez d'abord effectuer les opérations suivantes :

- Effectuez les tâches définies dans Configurez Résolution des entités AWS.
- Créez une source d'espace de noms ID.
- Créez une cible d'espace de noms ID.
- Acquérez l'espace de noms ID ARN si vous utilisez une source d'espace de noms ID provenant d'une autre source. Compte AWS
- (Services du fournisseur uniquement) La création d'un flux de travail de mappage d'identifiants entre deux Comptes AWS nécessite l'autorisation d'accéder LiveRamp au compartiment S3 et à la clé gérée par le client AWS Key Management Service (AWS KMS).

  Avant de créer un flux de travail de mappage Comptes AWS d'identifiants entre deux LiveRamp, ajoutez la politique d'autorisation suivante, qui permet LiveRamp d'accéder au compartiment S3 et à la clé gérée par le client.

```
{
```

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

Dans la politique d'autorisation précédente, remplacez chaque *<user input placeholder>* avec vos propres informations.

<KMSKeyARN>	Le ARN d'une clé gérée par le AWS KMS client.

Création d'un flux de travail de mappage d'identifiants (basé sur des règles)

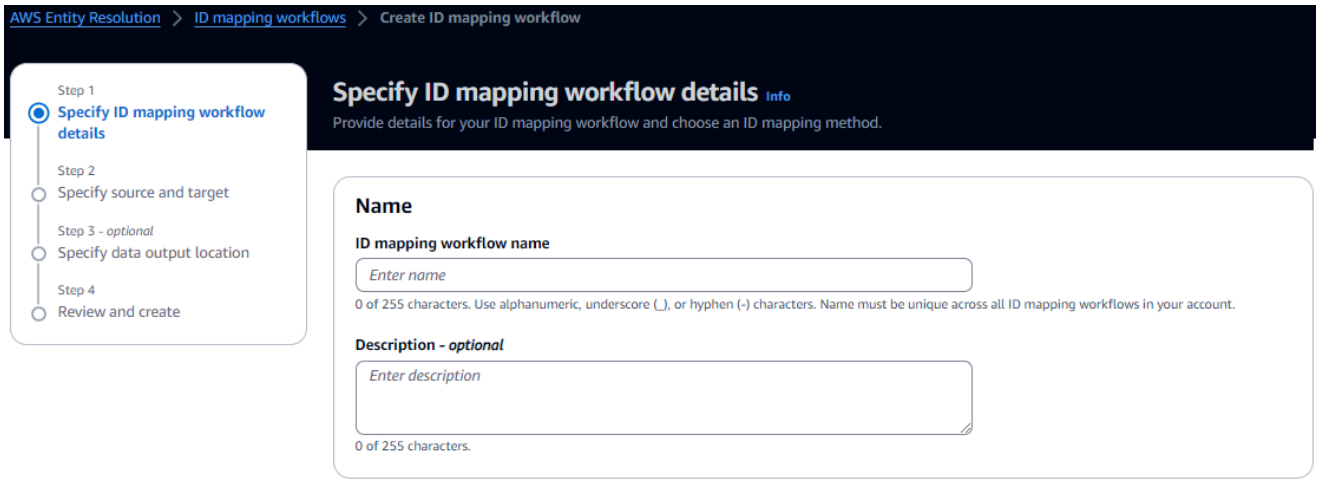
Une fois que vous avez rempli les conditions requises, vous pouvez créer un ou plusieurs flux de travail de mappage d'identifiants afin d'utiliser des règles de correspondance pour traduire les données de première partie d'une source vers une cible.

Pour créer un flux de travail de mappage des identifiants basé sur des règles entre deux Comptes AWS

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez ID mapping.
3. Sur la page des flux de travail de mappage des identifiants, dans le coin supérieur droit, choisissez Créer un flux de travail de mappage des identifiants.

4. Pour l'étape 1 : Spécifier les détails du flux de travail de mappage des identifiants, procédez comme suit.

   a. Entrez un nom de flux de travail de mappage d'identifiants et une description facultative.



   b. Pour la méthode de mappage des identifiants, choisissez Basée sur des règles.

   c. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

   d. Choisissez Suivant.

5. Pour l'étape 2 : Spécifier la source et la cible, procédez comme suit.

   a. Activez les options avancées.

   b. Pour Source, choisissez Flux de travail correspondant, puis sélectionnez le flux de travail correspondant existant dans la liste déroulante.

   c. Pour Target, choisissez Processus de correspondance, puis sélectionnez le flux de travail de correspondance existant dans la liste déroulante.

   d. Pour les paramètres de règle, spécifiez les contrôles de règle en choisissant si une source ou une cible peut fournir des règles dans un flux de travail de mappage d'identifiants.

      Les contrôles de règles doivent être compatibles entre la source et la cible pour être utilisés dans un flux de travail de mappage d'identifiants. Par exemple, si un espace de noms d'ID source limite les règles à la cible mais que l'espace de noms d'ID cible limite les règles à la source, cela entraîne une erreur.

   e. Pour les paramètres de comparaison et de correspondance, procédez comme suit.

      i. Spécifiez le type de comparaison en choisissant une option en fonction de votre objectif.

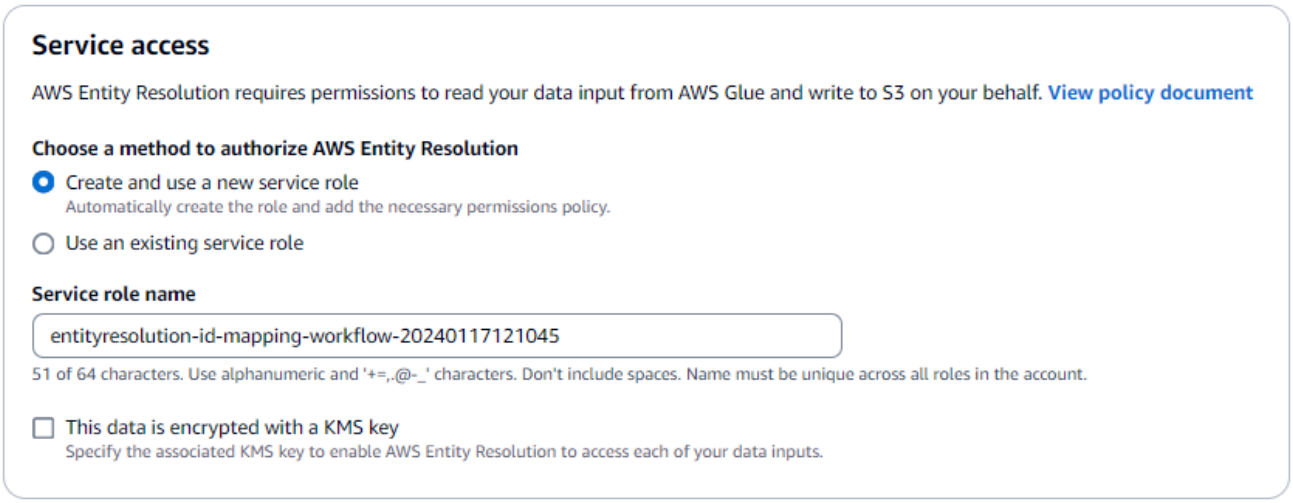
Votre objectif	Option recommandée
Trouvez n'importe quelle combinaison de correspondances entre les données stockées dans plusieurs champs de saisie, que les données se trouvent dans le même champ de saisie ou dans un autre champ de saisie.	Plusieurs champs de saisie
Limitez la comparaison au sein d'un seul champ de saisie, lorsque des données similaires stockées dans plusieurs champs de saisie ne doivent pas être mises en correspondance.	Champ de saisie unique

ii. Spécifiez le type de correspondance des enregistrements en choisissant une option en fonction de votre objectif.

Votre objectif	Option recommandée
Limitez le type de correspondance d'enregistrements afin de ne stocker qu'un seul enregistrement correspondant dans la source pour chaque enregistr ement correspondant dans la cible lorsque vous créez le flux de travail de mappage d'identifiants.	Une source pour une cible
Limitez le type de correspondance d'enregistrements afin de stocker tous les enregistrements correspondants dans la source pour chaque enregistr ement correspondant dans la cible lorsque vous créez le flux de travail de mappage d'identifiants.	De nombreuses sources pour une seule cible

> **Note**
>
> Vous devez spécifier des limites compatibles pour les espaces de noms d'ID source et cible.

f. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.



Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut `estentityresolution-id-mapping-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.

Option	Action recommandée
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

6. Choisissez Suivant.
7. Pour l'étape 3 : Spécifier l'emplacement de sortie des données. Procédez comme suit si vous le souhaitez.
   a. Pour Destination de sortie des données, procédez comme suit.
      i. Choisissez l'emplacement Amazon S3 pour la sortie des données.
      ii. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS clé ARN ou choisissez Créer une AWS KMS clé.
   b. Affichez le résultat LiveRamp généré.
   c. Choisissez Suivant.
8. Pour l'étape 4 : révision et création, procédez comme suit.

a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

b. Sélectionnez Create (Créer).

   Un message apparaît, indiquant que le flux de travail de mappage des identifiants a été créé.

Après avoir créé le flux de travail de mappage des identifiants, vous êtes prêt à exécuter un flux de travail de mappage des identifiants.

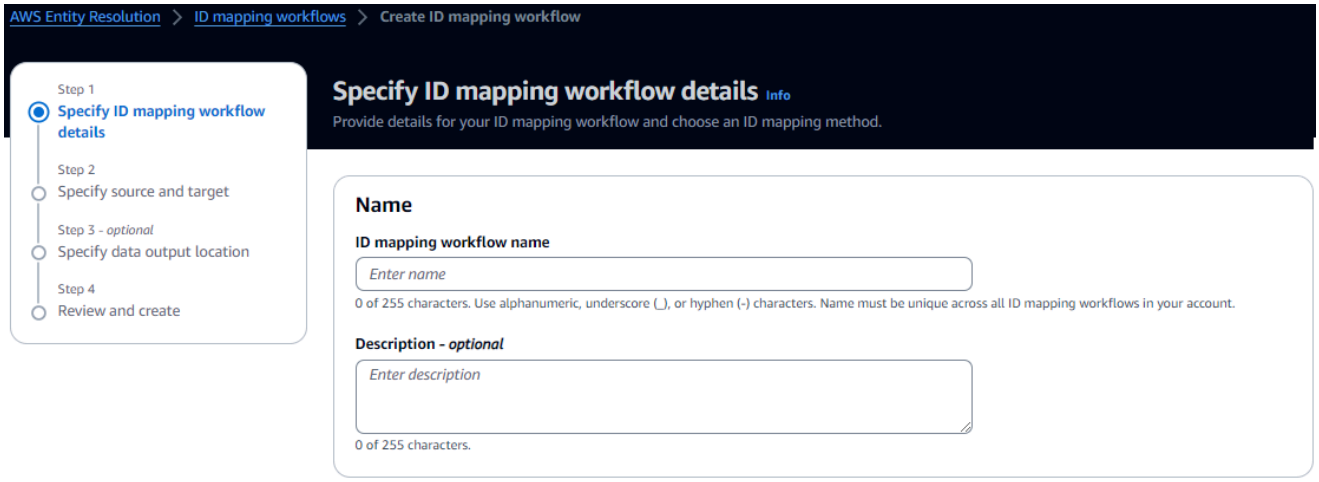
Création d'un flux de travail de mappage d'identifiants (services aux fournisseurs)

Une fois les conditions requises remplies, vous pouvez créer un ou plusieurs flux de travail de mappage d'identifiants à l'aide du service du LiveRamp fournisseur. LiveRamp traduit un ensemble de R source ampIDs en un autre ensemble en utilisant R maintenu ou dérivéampIDs.

Pour créer un flux de travail de mappage d'identifiants à l'aide du service du fournisseur

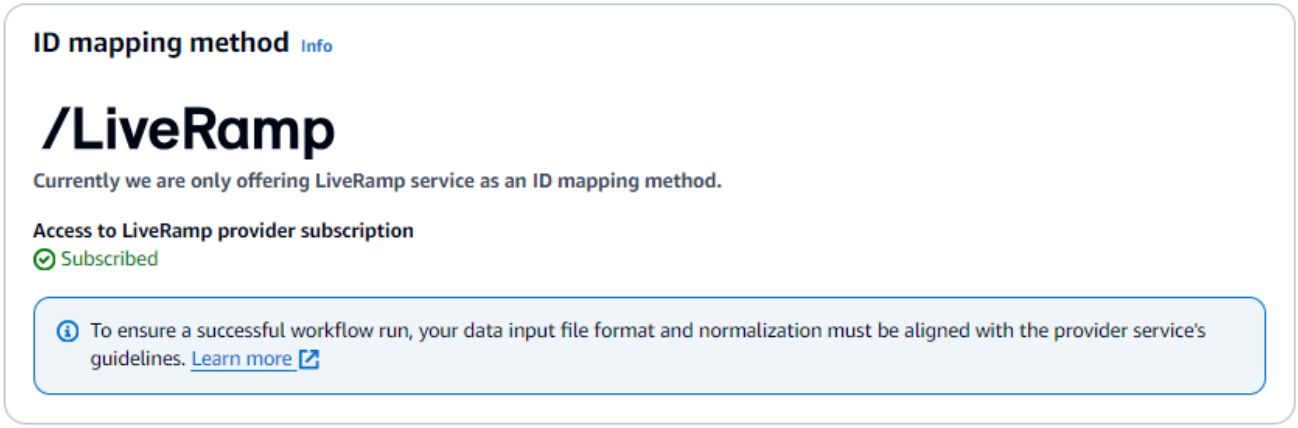
1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez ID mapping.
3. Sur la page des flux de travail de mappage des identifiants, dans le coin supérieur droit, choisissez Créer un flux de travail de mappage des identifiants.
4. Pour l'étape 1 : Spécifier les détails du flux de travail de mappage des identifiants, procédez comme suit.

   a. Entrez un nom de flux de travail de mappage d'identifiants et une description facultative.



b. Pour la méthode de mappage des identifiants, choisissez Provider services.

Résolution des entités AWS propose actuellement le service du LiveRamp fournisseur en tant que méthode de mappage d'identifiants. Si vous êtes abonné à LiveRamp, le statut apparaît comme Abonné. Pour plus d'informations sur la façon de s'abonner à LiveRamp, consultezÉtape 1 : Abonnez-vous à un service fournisseur sur AWS Data Exchange.



> **Note**
>
> Assurez-vous que le format de votre fichier de saisie de données est conforme aux directives du fournisseur de services. Pour plus d'informations sur les directives LiveRamp de formatage des fichiers d'entrée, voir Perform Translation Through ADX sur le site Web de LiveRamp documentation.

c. Pour LiveRamp la configuration, entrez les valeurs suivantes qui LiveRamp fournissent :

- Gestionnaire d'identifiants clients ARN
- Gestionnaire des secrets clients ARN

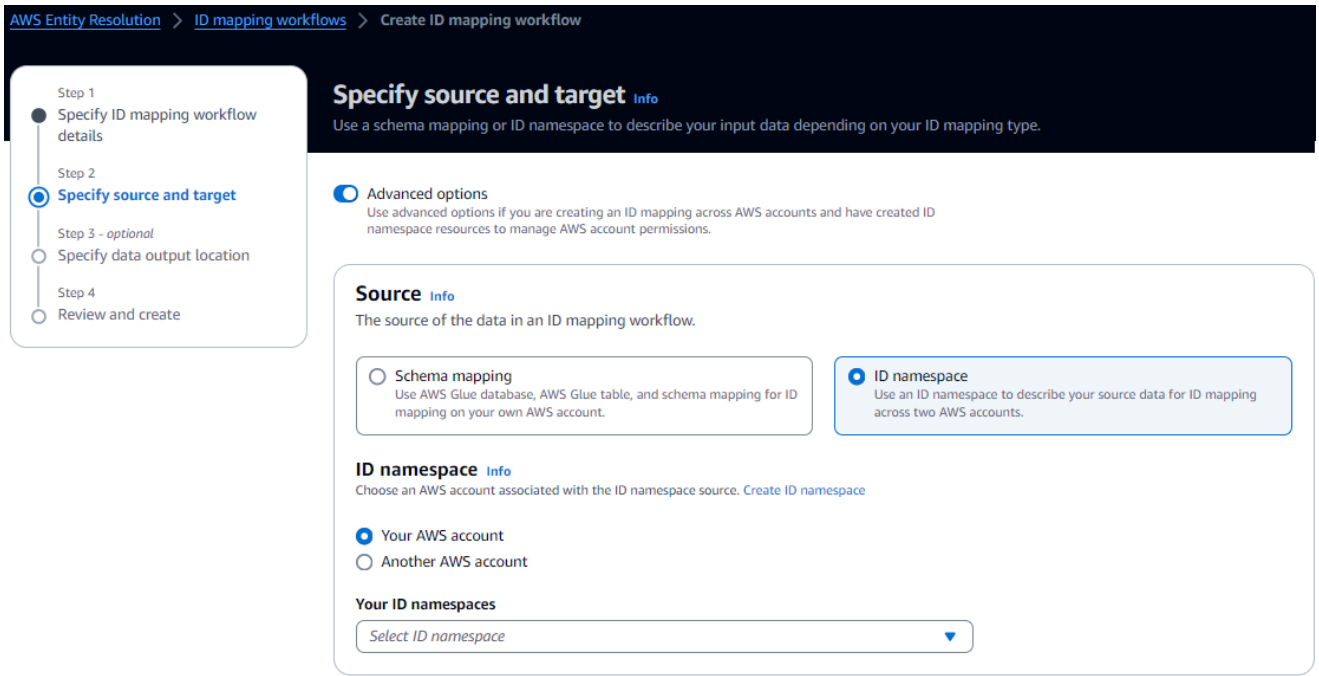
d. (Facultatif) Pour activer les balises pour la ressource, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

e. Choisissez Suivant.

5. Pour l'étape 2 : Spécifier la source et la cible, procédez comme suit.

a. Activez les options avancées.

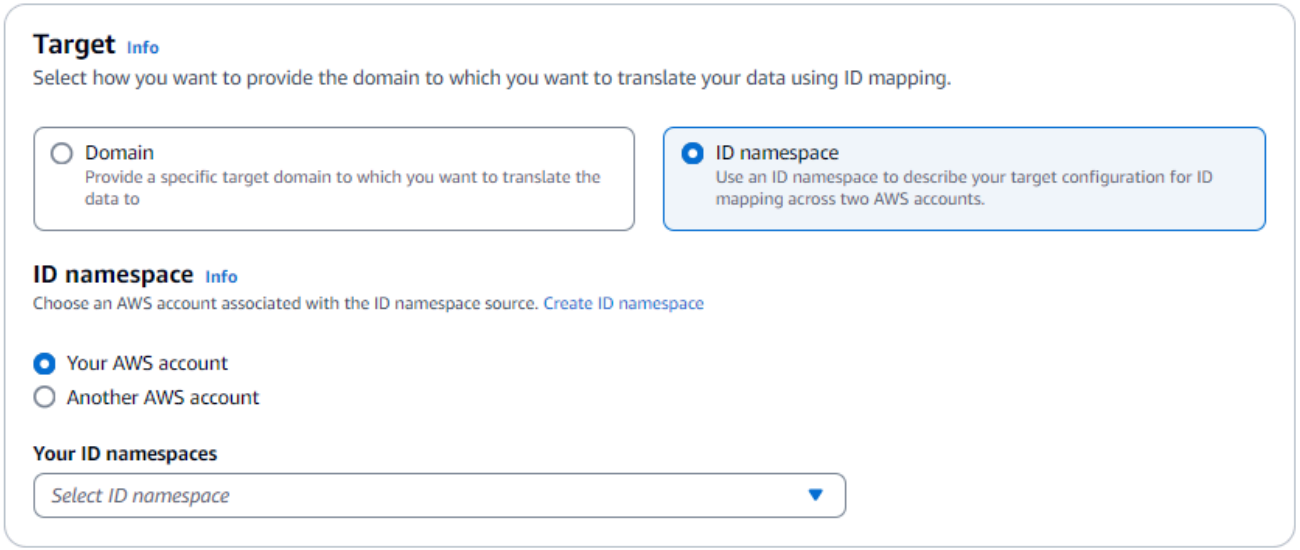
b. Pour Source, choisissez l'espace de noms ID.



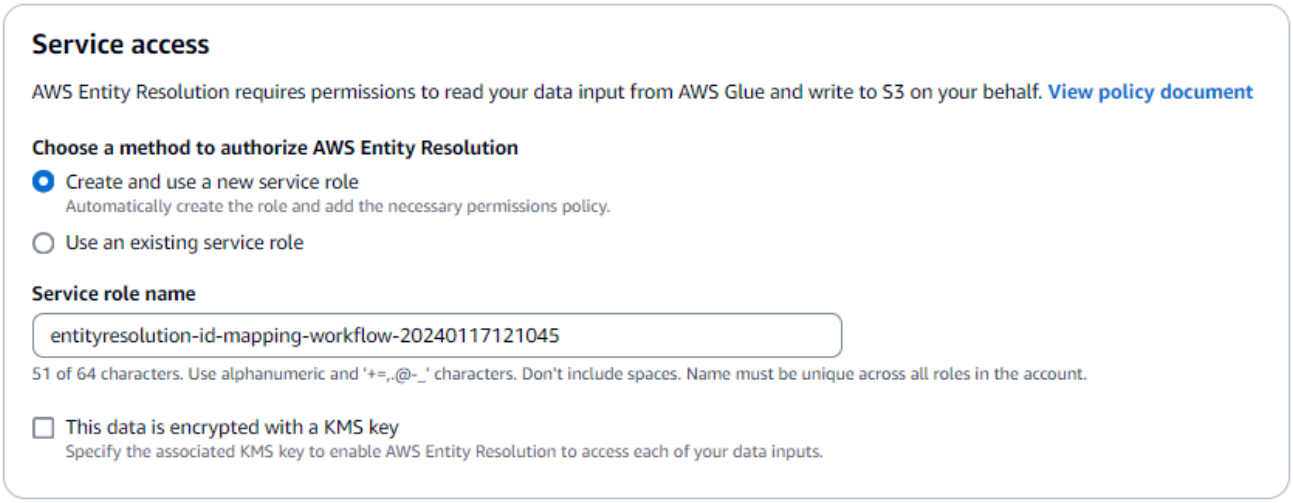
c. Pour l'espace de noms d'ID, identifiez l'emplacement de l'espace de noms d'ID, puis prenez les mesures recommandées.

Emplacement de l'espace de noms ID	Action recommandée
Le vôtre Compte AWS	1. Choisissez votre Compte AWS. 2. Sélectionnez l'espace de noms ID dans la liste déroulante Vos espaces de noms ID.
Celui de quelqu'un d'autre Compte AWS	1. Choisissez-en un autre Compte AWS. 2. Entrez l'espace de noms ARN ID.

d. Pour Target, choisissez l'espace de noms ID.



e. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.



Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut est `entityresolution-id-mapping-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.

Option	Action recommandée
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante. La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

6. Choisissez Suivant.
7. Pour l'étape 3 : Spécifier l'emplacement de sortie des données. Procédez comme suit si vous le souhaitez.

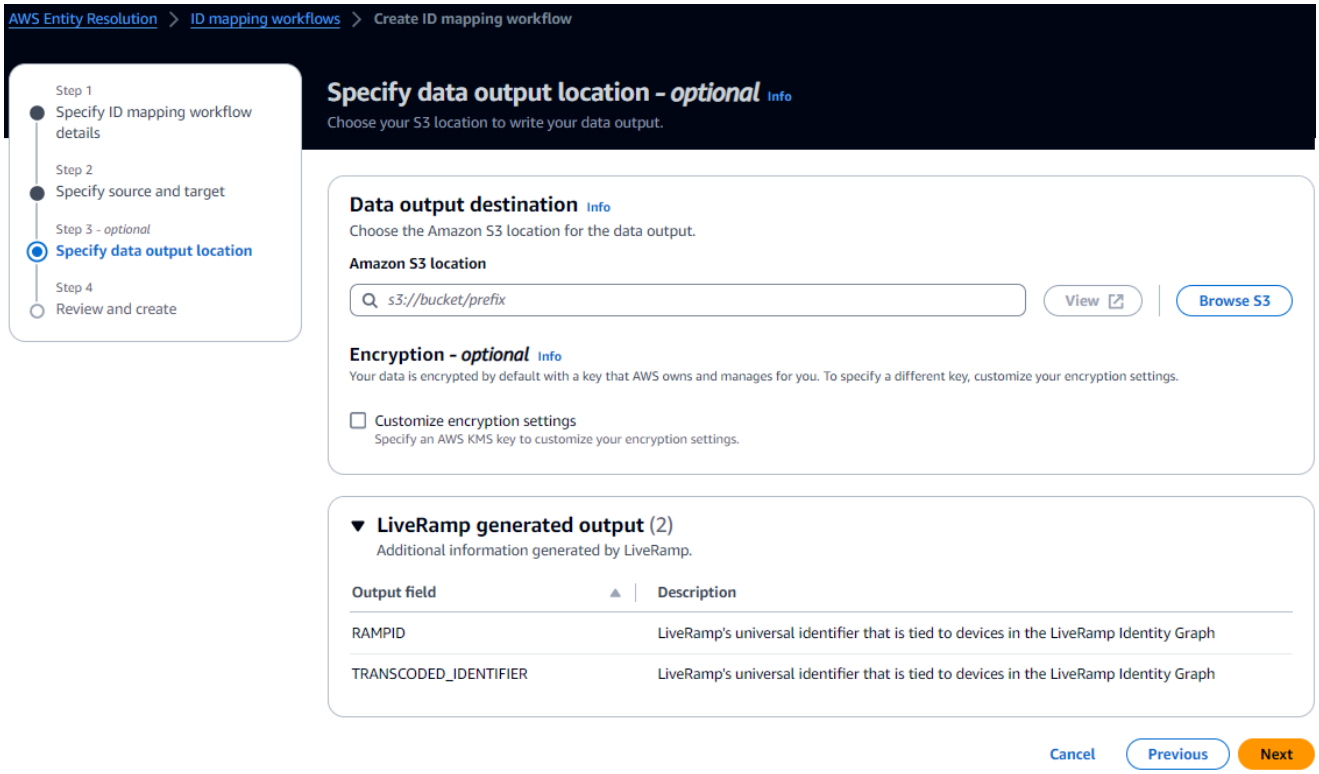
   a. Pour Destination de sortie des données, procédez comme suit.

      i. Choisissez l'emplacement Amazon S3 pour la sortie des données.

      ii. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS clé ARN ou choisissez Créer une AWS KMS clé.

   b. Affichez le résultat LiveRamp généré.

   c. Choisissez Suivant.



8. Pour l'étape 4 : révision et création, procédez comme suit.

   a. Passez en revue les sélections que vous avez effectuées lors des étapes précédentes et modifiez-les si nécessaire.

   b. Sélectionnez Create (Créer).

      Un message apparaît, indiquant que le flux de travail de mappage des identifiants a été créé.

Après avoir créé le flux de travail de mappage des identifiants, vous êtes prêt à exécuter un flux de travail de mappage des identifiants.

Exécuter un flux de travail de mappage d'identifiants

Après avoir créé un flux de travail de mappage d'ID pour l'un Compte AWS ou créé un flux de travail de mappage d'ID pour deux Comptes AWS, vous pouvez exécuter le flux de travail de mappage d'ID. Le flux de travail de mappage des identifiants produit un CSV fichier.

Pour exécuter un flux de travail de mappage d'identifiants

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez ID mapping.
3. Choisissez le flux de travail de mappage des identifiants.
4. Sur la page des détails du flux de travail de mappage des identifiants, dans le coin supérieur droit, sélectionnez Exécuter.
5. Sur la page des détails du flux de travail correspondant, sous l'onglet Mesures, consultez les informations suivantes sous Dernières mesures de travail :

   - Le Job ID
   - Durée d'exécution de la tâche de flux de travail
   - État de la tâche de flux de travail correspondante : En file d'attente, en cours, terminée, échouée
   - Le nombre d'enregistrements traités
   - Le nombre d'enregistrements non traités
   - Le nombre d'enregistrements d'entrée

   Sous Historique des tâches, vous pouvez également consulter les statistiques des tâches relatives aux tâches de flux de travail de mappage d'identifiants exécutées précédemment.
6. Une fois le travail de mappage des identifiants terminé (le statut est terminé), choisissez Data output, puis choisissez votre emplacement Amazon S3 pour afficher les résultats.

   Une fois que vous avez obtenu votre CSV fichier, vous pouvez le joindre `RAMPID` au`TRANSCODED_ID`.

Exécution d'un flux de travail de mappage d'identifiants avec une nouvelle destination de sortie

Après avoir créé un flux de travail de mappage d'ID pour l'un d'entre eux Compte AWS ou créé un flux de travail de mappage d'ID pour deux Comptes AWS, vous pouvez choisir un autre emplacement S3 pour écrire vos données de sortie.

Pour exécuter un flux de travail de mappage d'identifiants avec une nouvelle destination de sortie

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez ID mapping.
3. Choisissez le flux de travail de mappage des identifiants.
4. Sur la page des détails du flux de travail de mappage des identifiants, dans le coin supérieur droit, choisissez Exécuter avec une nouvelle destination de sortie dans la liste déroulante Exécuter le flux de travail.
5. Pour Destination de sortie des données, procédez comme suit.

   a. Choisissez l'emplacement Amazon S3 pour la sortie des données.

   b. Pour le chiffrement, si vous choisissez de personnaliser les paramètres de chiffrement, entrez la AWS KMS clé ARN ou choisissez Créer une AWS KMS clé.
6. Pour spécifier les autorisations d'accès au service, choisissez une option et prenez les mesures recommandées.

Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	• Résolution des entités AWS crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut est `entityresolution-id-mapping-workflow-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, choisissez l'option This data is encrypted by a KMS key. Entrez ensuite une AWS KMS clé qui sera utilisée pour déchiffrer vos données saisies.
Utiliser un rôle de service existant	1. Choisissez le nom d'un rôle de service existant dans la liste déroulante.

Option	Action recommandée
	La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles. Si vous n'êtes pas autorisé à répertorier les rôles, vous pouvez saisir le nom de ressource Amazon (ARN) du rôle que vous souhaitez utiliser. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. Par défaut, Résolution des entités AWS ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.

7. Cliquez sur Exécuter.
8. Sur la page des détails du flux de travail correspondant, sous l'onglet Mesures, consultez les informations suivantes sous Dernières mesures de travail :

   - Le Job ID
   - Durée d'exécution de la tâche de flux de travail
   - État de la tâche de flux de travail correspondante : En file d'attente, en cours, terminée, échouée
   - Le nombre d'enregistrements traités
   - Le nombre d'enregistrements non traités
   - Le nombre d'enregistrements d'entrée

   Sous Historique des tâches, vous pouvez également consulter les statistiques des tâches relatives aux tâches de flux de travail de mappage d'identifiants exécutées précédemment.

9. Une fois le travail de mappage des identifiants terminé (le statut est terminé), choisissez Data output, puis choisissez votre emplacement Amazon S3 pour afficher les résultats.

   Une fois que vous avez obtenu votre CSV fichier, vous pouvez le joindre `RAMPID` au`TRANSCODED_ID`.

Modification d'un flux de travail de mappage d'identifiants

La modification du flux de travail de mappage des identifiants vous permet de conserver vos capacités de résolution des entités up-to-date et de les adapter à l'évolution des besoins de votre entreprise au fil du temps. Vous souhaiterez peut-être ajuster les règles, les techniques et les paramètres de mappage. Vous pouvez optimiser le flux de travail pour fournir des résultats de correspondance d'identifiants plus précis et plus fiables. Vous souhaiterez peut-être également ajouter de nouvelles sources de données, étendre les types de IDs mappage ou intégrer des critères de correspondance supplémentaires dans le flux de travail. Si vous identifiez des problèmes ou des erreurs dans les résultats du mappage des identifiants, la modification à l'aide du flux de travail peut vous aider à diagnostiquer et à résoudre ces problèmes.

Pour modifier un flux de travail de mappage d'identifiants :

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez ID mapping.
3. Choisissez le flux de travail de mappage des identifiants.
4. Sur la page des détails du flux de travail de mappage des identifiants, dans le coin supérieur droit, choisissez Modifier.
5. Sur la page des détails du flux de travail de mappage des identifiants, apportez les modifications nécessaires, puis choisissez Suivant.
6. Sur la page Spécifier les données de sortie, apportez les modifications nécessaires, puis choisissez Next.
7. Sur la page Réviser et enregistrer, apportez les modifications nécessaires, puis choisissez Enregistrer.

Supprimer un flux de travail de mappage d'identifiants

Si vous n'utilisez plus de flux de travail de mappage d'identifiants, sa suppression peut contribuer à rationaliser la gestion de votre flux de travail. En outre, la suppression des flux de travail de mappage d'identité redondants ou moins efficaces ayant des objectifs similaires peut vous aider à consolider vos processus.

Pour supprimer un flux de travail de mappage d'identifiants :

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez ID mapping.
3. Choisissez le flux de travail de mappage des identifiants.
4. Sur la page des détails du flux de travail de mappage des identifiants, dans le coin supérieur droit, choisissez Supprimer.
5. Confirmez la suppression, puis choisissez Supprimer.

Ajouter ou mettre à jour une politique de ressources pour un flux de travail de mappage d'identifiants

Une politique de ressources permet au créateur de la ressource de mappage d'identification d'accéder à votre ressource de flux de travail de mappage d'identification.

Pour ajouter ou mettre à jour une politique de ressources

1. Connectez-vous à la Résolution des entités AWS console AWS Management Console et ouvrez-la avec votre Compte AWS, si vous ne l'avez pas encore fait.
2. Dans le volet de navigation de gauche, sous Workflows, choisissez ID mapping.
3. Choisissez le flux de travail de mappage des identifiants.
4. Sur la page des détails du flux de travail de mappage des identifiants, choisissez l'onglet Autorisations.
5. Dans la section Politique des ressources, choisissez Modifier.
6. Ajoutez ou mettez à jour la politique dans l'JSONéditeur.
7. Sélectionnez Enregistrer les modifications.

Intégrez avec Résolution des entités AWS en tant que fournisseur

Résolution des entités AWS les intégrations de fournisseurs tiers aident les clients à protéger la vie privée des consommateurs et à se conformer aux lois sur la souveraineté des données. Les fournisseurs tiers, tels que LiveRamp et TransUnion, traduisent les identifiants des consommateurs en publicitéIDs, tels que Ramp IDs et Fabrick. IDs Ces identifiants publicitaires sont couramment utilisés dans les outils de publicité et de marketing, afin d'empêcher l'exportation des données des consommateurs vers des entités non gouvernementales.AWS systèmes gérés. Cette section fournit des conseils aux fournisseurs pour intégrer Résolution des entités AWS pour coder ou transcoder les identifiants des consommateurs en publicité à utiliser dans un flux de travail de mise en correspondance basé sur IDs les services d'un fournisseur de services.

Pour plus d'informations sur les services des fournisseurs actuellement intégrés à Résolution des entités AWS, voir Création d'un flux de travail de correspondance basé sur les services des fournisseurs.

Rubriques

Prérequis

Avant de procéder à l'intégration en tant que fournisseur de services avec Résolution des entités AWS, remplissez les conditions suivantes.

Rubriques

Répertorier un fournisseur de services sur AWS Data Exchange

En tant que fournisseur tiers, vous devez répertorier votre produit dans le catalogue de produits AWSData Exchange (ADX). Une fois que votre produit est répertorié sur le AWS Data Exchange Catalogue de produits, les abonnés peuvent s'abonner à votre produit par le biais d'une offre publique ou privée.

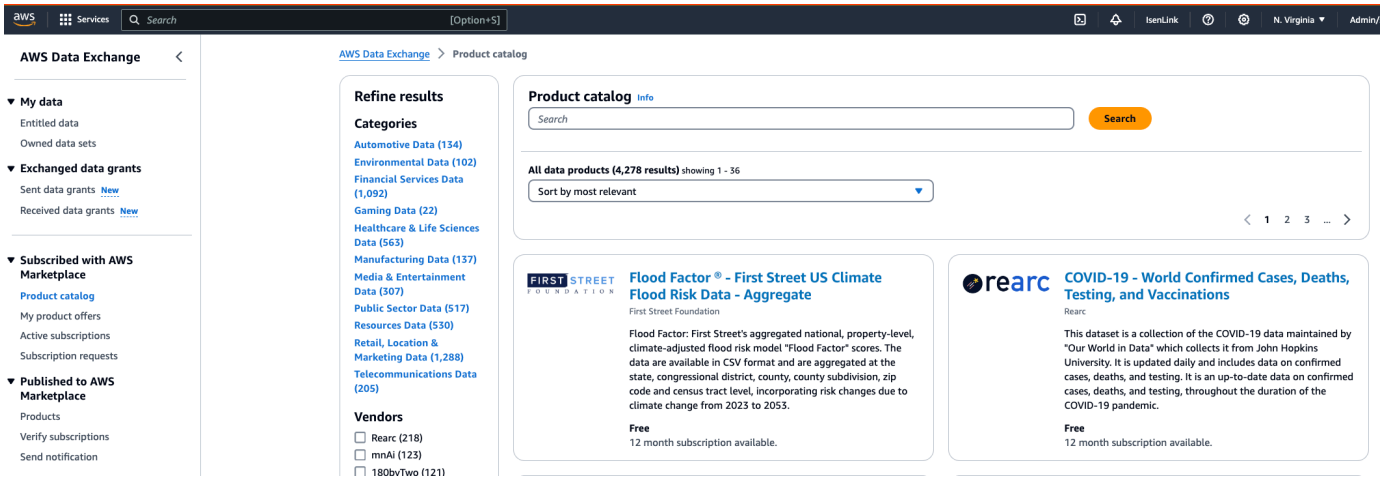
Pour répertorier un service fournisseur sur AWS Data Exchange

1. Si vous êtes un nouveau fournisseur de produits de données sur AWS Data Exchange, suivez les étapes décrites dans la section intitulée Commencer en tant que fournisseur dans le AWS Data Exchange Guide de l'utilisateur
2. Créez un ensemble de REST API données et publiez un nouveau produit contenant APIs sur AWS Data Exchange en suivant les étapes décrites dans la section intitulée Comment publier un produit figurant APIs dans le AWS Data Exchange Guide de l'utilisateur Vous pouvez terminer le processus en utilisant soit AWS Data Exchange console ou AWS Command Line Interface.

   Si vous avez défini la visibilité du produit comme publique, l'offre publique est accessible à tous les abonnés.

   Si vous avez défini la visibilité du produit comme privée, suivez les étapes de la section intitulée Créer des offres personnalisées dans le AWS Data Exchange Guide de l'utilisateur, en fonction de votre cas d'utilisation.

   L'image suivante montre un exemple de produit disponible dans le AWS Data Exchange Catalogue de produits.



3. Une fois le produit disponible sur AWS Data Exchange Catalogue de produits, l'abonné peut s'abonner au produit des manières suivantes.

   - Abonnez-vous au produit public.
   - Utilisez une offre privée (offre personnalisée) émise par le service fournisseur.
   - Utilisez une offre Bring Your Own Subscription (BYOS).

   Pour plus d'informations, voir S'abonner et accéder à un produit contenu APIs dans le AWS Data Exchange Guide de l'utilisateur

Identifiez vos attributs

Les attributs des données d'entrée sont les définitions de type des entités à résoudre dans un flux de travail. Voici quelques exemples d'attributs : `FirstNameLastName`,`Email`, ou`Custom String`.

Lorsque vous identifiez vos attributs, vous devez prendre note de toutes les exigences ou directives.

Example Exemple

Voici un exemple de validations permettant d'identifier les attributs des fournisseurs.

- L'`LastName`attribut `FirstName` or est obligatoire.
- Si l'`Email`attribut est présent, il doit être haché.

En tant que fournisseur, vous devez identifier les attributs de votre produit de service fournisseur, puis communiquer ces attributs au Résolution des entités AWS L'équipe de développement commercial de <aws-entity-resolution-bd@amazon .com> pour une validation supplémentaire avant de continuer.

Demandez le Résolution des entités AWS APISpécification ouverte

Résolution des entités AWS possède une API spécification Open que vous pouvez utiliser en tant que fournisseur comme poignée de main contenant les APIs personnes impliquées dans l'intégration. Pour de plus amples informations, veuillez consulter Utilisation de Résolution des entités AWS APISpécification ouverte.

Pour demander la API définition ouverte, contactez le Résolution des entités AWS L'équipe de développement commercial de <aws-entity-resolution-bd@amazon .com>.

Utilisation de Résolution des entités AWS APISpécification ouverte

La API spécification Open définit tous les protocoles associés à Résolution des entités AWS. Cette spécification est nécessaire pour implémenter l'intégration.

La API définition Open contient les API opérations suivantes :

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

Pour demander la API spécification Open, contactez le Résolution des entités AWS L'équipe de développement commercial de `<aws-entity-resolution-bd@amazon .com>`.

La API spécification Open prend en charge deux types d'intégrations pour le codage et le transcodage des identifiants des consommateurs, le traitement par lots et le traitement synchrone. Après avoir obtenu la API spécification Open, implémentez le type d'intégration de traitement adapté à votre cas d'utilisation.

Rubriques

Intégration du traitement par lots

L'intégration du traitement par lots suit un modèle de conception asynchrone. Après le lancement d'un flux de travail sur AWS Data Exchange, il soumet une tâche via un point de terminaison d'intégration des fournisseurs, puis le flux de travail attend la fin de cette tâche en interrogeant périodiquement l'état de la tâche. Cette solution est préférable pour les travaux qui peuvent prendre plus de temps et dont le débit du fournisseur est inférieur. Le fournisseur saisira l'emplacement du jeu de données sous forme de lien Amazon S3, qu'il pourra traiter de son côté et écrire les résultats dans un emplacement S3 de sortie prédéterminé.

L'intégration du traitement par lots est activée à l'aide de trois API définitions. Résolution des entités AWS appellera le point de terminaison du fournisseur qui est disponible via AWS Data Exchange dans l'ordre suivant :

1. `POST CreateJob`: Cette API opération soumet les informations relatives à la tâche au fournisseur pour qu'il les traite. Ces informations concernent le type de tâche, le codage ou le transcodage, les emplacements S3, le schéma fourni par le client et toutes les propriétés de tâche supplémentaires requises.

   Cela API renvoie un`JobId`, et le statut du Job sera l'un des suivants : `PENDINGREADY`,`IN_PROGRESS`,`COMPLETE`, ou`FAILED`.

   Exemple de demande d'encodage

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

   Exemple de réponse

```
{
```

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

2. `POST StartJob`: Cela API permet au fournisseur de savoir qu'il doit démarrer le travail en fonction des informations `JobId` fournies. Cela permet au fournisseur d'effectuer toutes les validations nécessaires du début à la `CreateJob` fin`StartJob`.

   Cela API renvoie a`JobId`, le `Status` pour le Jobstatus`Message`, le et`statusCode`.

   Exemple de demande d'encodage

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

   Exemple de réponse

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

3. `GET GetJob`: Cela API informe Résolution des entités AWS si le travail est terminé ou s'il existe un autre statut.

   Cela API renvoie a`JobId`, le `Status` pour le Jobstatus`Message`, le et`statusCode`.

   Exemple de demande d'encodage

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

   Exemple de réponse

   ```
   {
   ```

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

La définition complète de APIs ceux-ci est fournie dans le Résolution des entités AWS APISpécification ouverte.

Intégration du traitement synchrone

La solution de traitement synchrone est plus souhaitable pour les fournisseurs qui ont un temps de réponse en temps quasi réel avec un temps de réponse en temps réel avec un débit de plus en plus élevé. TPS Cette Résolution des entités AWS le flux de travail partitionne le jeu de données et effectue plusieurs API requêtes en parallèle. Le Résolution des entités AWS Le flux de travail gère ensuite l'écriture des résultats à l'emplacement de sortie souhaité.

Ce processus est activé à l'aide de l'une des API définitions. Résolution des entités AWS appelle le point de terminaison du fournisseur qui est disponible via AWS Data Exchange:

`POST AssignIdentities`: Cela API envoie des données au fournisseur à l'aide d'un `source_id` identifiant `recordFields` associé à cet enregistrement.

Cela API renvoie le`assignedRecords`.

Exemple de demande d'encodage

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

```
  ]
}
```

Exemple de réponse

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

La définition complète de APIs ceux-ci est fournie dans le Résolution des entités AWS APISpécification ouverte.

En fonction de l'approche choisie par le fournisseur, Résolution des entités AWS créera une configuration pour cela, le fournisseur qui sera utilisé pour initier le codage ou le transcodage. De plus, ces configurations sont disponibles pour les clients à l'aide du APIs Résolution des entités AWS.

Cette configuration est accessible à l'aide d'un Amazon Resource Name (ARN), dérivé de l'endroit où le fournisseur de services propose sur AWS Data Exchange est hébergé, ainsi que le type de service du fournisseur. Résolution des entités AWS désigne cela ARN sous le nom de`providerServiceARN`.

Tester l'intégration d'un fournisseur

Tandis que Résolution des entités AWS héberge des services de mise en correspondance de données, l'intégration d'un fournisseur est un composant tiers crucial pour le flux de travail de end-to-end correspondance. Il existe plusieurs tests qui Résolution des entités AWS a défini pour

les fournisseurs une protection en cas d'échec de cette intégration. Cette approche permet aux prestataires de surveiller l'état de santé de leurs services en fonction de ces cas de end-to-end test.

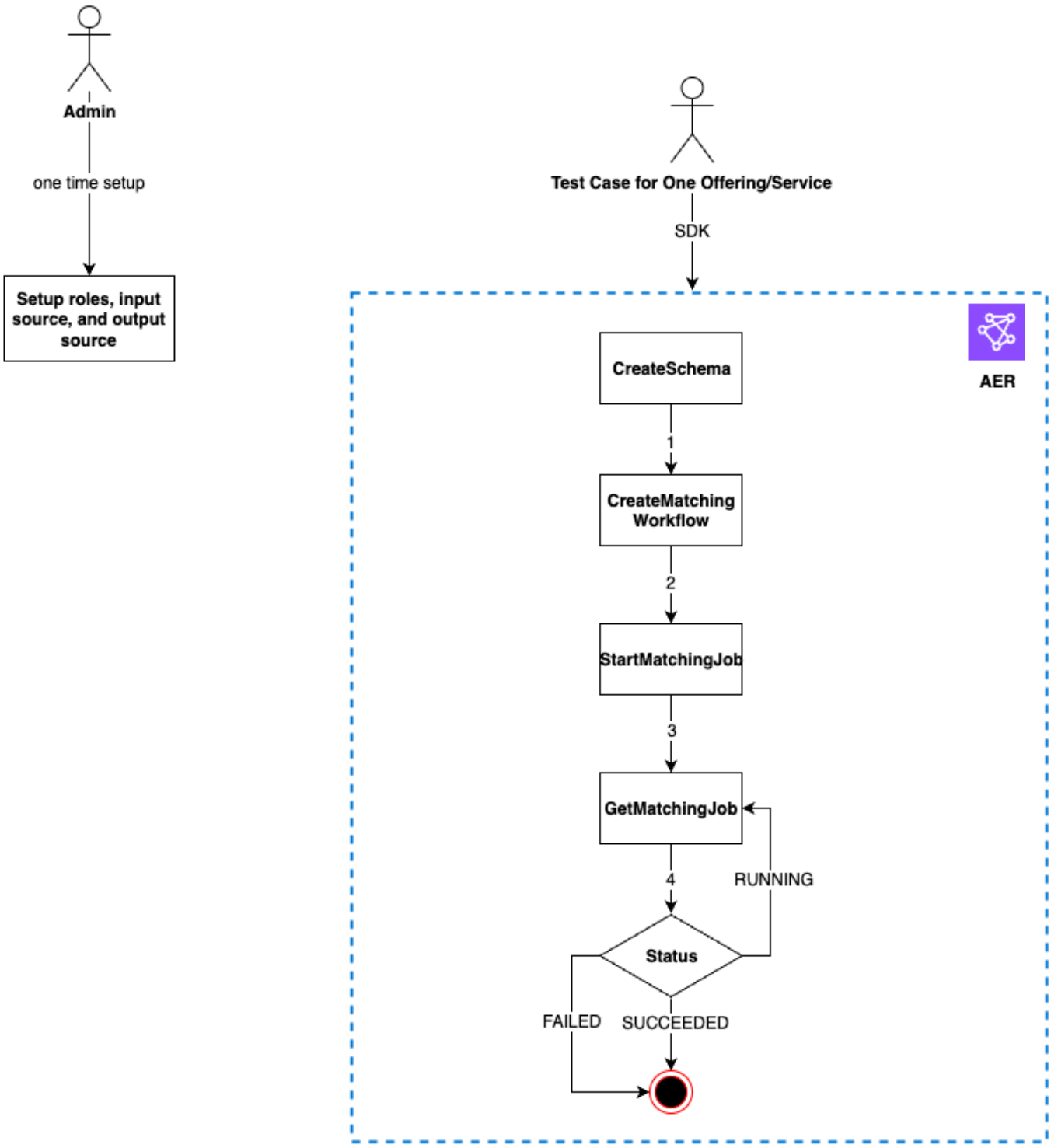
Les fournisseurs peuvent utiliser leurs comptes de test et leurs propres données pour exécuter ces scénarios de end-to-end test à l'aide du Résolution des entités AWS Kit de développement logiciel (SDK). En cas de problème de la part des fournisseurs, Résolution des entités AWS utilise le chemin d'escalade préféré pour aggraver le problème. En outre, les fournisseurs doivent mettre en œuvre leur propre surveillance des résultats des tests. Les fournisseurs doivent partager leurs Compte AWS IDsqui sont utilisés pour exécuter ces tests avec Résolution des entités AWS.

Une exécution réussie signifie qu'un fournisseur peut configurer ses données, utiliser son propre service via Résolution des entités AWS, et le statut de la tâche renvoie Terminé sans erreur. Cela peut être accompli par programmation en utilisant le APIs Résolution des entités AWS.

Par exemple, les fournisseurs peuvent configurer leur compartiment S3, leur source d'entrée, leurs rôles, leur schéma et leurs flux de travail en fonction de leurs services. Une fois ces configurations terminées, les fournisseurs peuvent exécuter ces flux de travail une fois par jour avec 200 enregistrements pour tester leur service. Dans cette approche, les fournisseurs utilisent les services de leur choix SDK et end-to-end testent leurs services proposés via AWS Data Exchange en utilisant leurs comptes de test. Les fournisseurs sont tenus d'effectuer ces tests pour chacune de leurs offres ou services.

> **Note**
>
> Les fournisseurs doivent fournir Résolution des entités AWS le Compte AWS ID (`accountId`)qu'ils utilisent pour exécuter ces flux de travail à des fins de test). En outre, les fournisseurs doivent surveiller ces tests et s'assurer qu'ils sont réussis, ce qui signifie qu'ils doivent activer la notification en cas d'échec et résoudre le problème en conséquence.

Le schéma suivant montre un cas de test end-to-end de flux de travail typique.



Pour tester l'intégration d'un fournisseur

1. (Configuration unique) Configurer les ressources pour Résolution des entités AWS en suivant les procédures décrites dansConfigurez Résolution des entités AWS.

Une fois les procédures de configuration uniques terminées, vos rôles, vos données et votre source de données devraient être prêts. Vous êtes maintenant prêt à tester l'intégration du fournisseur à l'aide de Résolution des entités AWS console ouAPIs.

2. Testez l'intégration du fournisseur à l'aide de Résolution des entités AWS APIsou console.

API

Pour tester l'intégration d'un fournisseur à l'aide du Résolution des entités AWS APIs

1. Créez un mappage de schéma à l'aide du CreateSchemaMapping API. Pour obtenir la liste complète des langages de programmation pris en charge, consultez la section Voir aussi du CreateSchemaMapping API.

   Le mappage du schéma est le processus par lequel vous indiquez Résolution des entités AWS comment interpréter vos données à des fins de mise en correspondance. Vous définissez le schéma de la table de données d'entrée que vous souhaitez que AWS Entity Resolution lise dans un flux de travail correspondant.

   Lors de la création d'un mappage de schéma, un identifiant unique doit être désigné et attribué à chaque ligne de données d'entrée lue par AWS Entity Resolution. Par exemple, `Primary_key`, `Row_ID`, `Record_ID`.

   Example Création d'un mappage de schéma pour une source de données contenant **`id`** et **`email`**

   Voici un exemple de mappage de schéma pour une source de données contenant `id` et `email` :

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

Example Création d'un mappage de schéma pour une source de données contenant **`id`** et **`email`** utilisant Java SDK

Voici un exemple de mappage de schéma pour une source de données contenant `id` et `email` utilisant le langage Java SDK :

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

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

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

)
```

2. Créez un flux de travail correspondant à l'aide du CreateMatchingWorkflow API. Pour obtenir la liste complète des langages de programmation pris en charge, consultez la section Voir aussi du CreateMatchingWorkflow API.

   Example Création d'un flux de travail correspondant à l'aide de Java SDK

   Voici un exemple de flux de travail correspondant utilisant Java SDK :

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

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

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

 .resolutionTechniques(ResolutionTechniques.builder()

   .resolutionType(PROVIDER)
```

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

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

)
```

Une fois le flux de travail correspondant configuré, vous pouvez exécuter un flux de travail.

3. Exécutez un flux de travail correspondant à l'aide du StartMatchingJob API. Pour exécuter un flux de travail correspondant, vous devez avoir créé un flux de travail correspondant à l'aide du `CreateMatchingWorkflow` point de terminaison.

   Pour obtenir la liste complète des langages de programmation pris en charge, consultez la section Voir aussi du StartMatchingJob API.

   Example Exécution d'un flux de travail correspondant à l'aide de Java SDK

   Voici un exemple de flux de travail correspondant en cours d'exécution à l'aide de Java SDK :

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

4. Surveillez l'état d'un flux de travail à l'aide du GetMatchingJob API.

   Cela API renvoie le statut, les métriques et les erreurs (le cas échéant) associés à une tâche.

Example Surveillance d'un flux de travail correspondant à l'aide de Java SDK

Voici un exemple de surveillance d'une tâche de flux de travail correspondante à l'aide de Java SDK :

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

Le end-to-end test est terminé si le flux de travail s'est terminé avec succès.

Console

Pour tester l'intégration d'un fournisseur à l'aide du Résolution des entités AWS console

1. Créez un mappage de schéma en suivant les étapes décrites dansCréation d'un mappage de schéma.

   Le mappage du schéma est le processus par lequel vous indiquez Résolution des entités AWS comment interpréter vos données à des fins de mise en correspondance. Vous définissez le schéma de la table de données d'entrée que vous souhaitez Résolution des entités AWS pour lire un flux de travail correspondant.

   Lors de la création d'un mappage de schéma, un identifiant unique doit être désigné et attribué à chaque ligne de données d'entrée qui Résolution des entités AWS lit. Par exemple, `Primary_key`, `Row_ID`, `Record_ID`.

   Example Mappage de schéma pour une source de données contenant **`id`** et **`email`**

   Voici un exemple de mappage de schéma pour une source de données contenant `id` et `email` :

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

```
  {
    "fieldName": "email",
    "type": "EMAIL_ADDRESS"
  }
]
```

2. Créez et exécutez un flux de travail correspondant en suivant les étapes décrites dansCréation d'un flux de travail de correspondance basé sur les services des fournisseurs.

   La création d'un flux de travail correspondant est le processus que vous configurez pour spécifier les données d'entrée à associer et la manière dont la correspondance doit être effectuée. Dans le flux de travail basé sur le fournisseur, si un compte dispose d'un abonnement auprès d'un service fournisseur via AWS Data Exchange, vous pouvez associer vos identifiants connus à ceux de votre fournisseur préféré. En fonction du fournisseur et du service que vous utilisez pour effectuer un test de bout en bout, vous pouvez configurer votre flux de travail correspondant en conséquence.

   Le Résolution des entités AWS la console combine les actions de création et d'exécution dans un seul bouton. Après avoir sélectionné Créer et exécuter, un message apparaît, indiquant que le flux de travail correspondant a été créé et que le travail a commencé.

3. Surveillez l'état du flux de travail sur la page des flux de travail correspondants.

   Le end-to-end test est terminé si le flux de travail s'est terminé avec succès (le statut du Job est terminé).

   Dans l'onglet Mesures de la page détaillée du flux de travail correspondant, vous pouvez consulter les informations suivantes sous Statistiques relatives à la dernière tâche :

   - Le Job ID.
   - État de la tâche de flux de travail correspondante : En file d'attente, en cours, terminée, échouée
   - Durée d'exécution de la tâche de flux de travail.
   - Le nombre d'enregistrements traités.
   - Le nombre d'enregistrements non traités.
   - La correspondance unique IDs générée.
   - Le nombre d'enregistrements en entrée.

Vous pouvez également consulter les statistiques des tâches correspondant aux tâches de flux de travail précédemment exécutées dans l'historique des tâches.

Sécurité dans Résolution des entités AWS

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud – AWS est responsable de la protection de l'infrastructure qui exécute des Services AWS dans le AWS Cloud. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS programmes de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Résolution des entités AWS, consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud – Votre responsabilité est fonction du Service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Résolution des entités AWS. Les rubriques suivantes expliquent comment configurer Résolution des entités AWS pour répondre à vos objectifs de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autres Services AWS capables de vous aider à surveiller et à sécuriser vos ressources Résolution des entités AWS.

Rubriques

Protection des données dans Résolution des entités AWS

Le AWS modèle de responsabilité partagée modèle s'applique à la protection des données dans Résolution des entités AWS. Comme décrit dans ce modèle, AWS est chargé de protéger

l'infrastructure mondiale qui gère tous les AWS Cloud. Il vous incombe de garder le contrôle sur votre contenu hébergé sur cette infrastructure. Vous êtes également responsable de la configuration de la sécurité et des tâches de gestion pour Services AWS que tu utilises. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le AWS Modèle de responsabilité partagée et article de GDPR blog sur AWS Blog sur la sécurité.

Pour des raisons de protection des données, nous vous recommandons de protéger Compte AWS informations d'identification et configuration des utilisateurs individuels avec AWS IAM Identity Center or AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et enregistrement de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation CloudTrail des sentiers pour capturer AWS activités, voir Travailler avec les CloudTrail sentiers dans le AWS CloudTrail Guide de l'utilisateur.
- Utiliser AWS des solutions de chiffrement, ainsi que tous les contrôles de sécurité par défaut Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un FIPS point de terminaison. Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Résolution des entités AWS ou autre Services AWS à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

Chiffrement des données au repos pour Résolution des entités AWS

Résolution des entités AWS fournit un chiffrement par défaut pour protéger les données sensibles des clients au repos en utilisant AWS clés de chiffrement détenues.

AWSclés possédées — Résolution des entités AWS utilise ces clés par défaut pour chiffrer automatiquement les données personnelles identifiables. Vous ne pouvez ni afficher, ni gérer, ni utiliser AWS clés détenues, ou auditez leur utilisation. Cependant, vous n'êtes pas obligé de prendre des mesures pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez la section sur les clés AWS détenues dans le AWS Key Management Service Guide du développeur.

Le chiffrement des données au repos par défaut permet de réduire les frais opérationnels et la complexité liés à la protection des données sensibles. Dans le même temps, vous pouvez l'utiliser pour créer des applications sécurisées qui répondent aux exigences réglementaires et de conformité strictes en matière de chiffrement.

Vous pouvez également fournir une KMS clé de chiffrement gérée par le client lorsque vous créez la ressource de flux de travail correspondante.

Clés gérées par le client — Résolution des entités AWS prend en charge l'utilisation d'une KMS clé symétrique gérée par le client que vous créez, détenez et gérez pour permettre le chiffrement de vos données sensibles. Étant donné que vous avez le contrôle total de cette couche de chiffrement, vous pouvez effectuer les tâches suivantes :

- Établissement et gestion des stratégies de clé
- Établir et maintenir IAM des politiques et des subventions
- Activation et désactivation des stratégies de clé
- Rotation des matériaux de chiffrement de clé
- Ajout de balises
- Création d'alias de clé
- Planification des clés pour la suppression

Pour plus d'informations, consultez la section clé gérée par le client dans le AWS Key Management Service Guide du développeur.

Pour plus d'informations sur AWS KMS, voir Qu'est-ce que le service de gestion des AWS clés ?

Gestion des clés

Comment ? Résolution des entités AWS utilise les subventions dans AWS KMS

Résolution des entités AWS nécessite une autorisation pour utiliser votre clé gérée par le client. Lorsque vous créez un flux de travail correspondant chiffré à l'aide d'une clé gérée par le client, Résolution des entités AWS crée une subvention en votre nom en envoyant une CreateGrantdemande à AWS KMS. Subventions en AWS KMS sont utilisés pour donner Résolution des entités AWS accès à une KMS clé dans un compte client. Résolution des entités AWS nécessite l'autorisation d'utiliser votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez vos GenerateDataKeydemandes à AWS KMS pour générer des clés de données chiffrées par votre clé gérée par le client.
- Envoyer les demandes de déchiffrement à AWS KMS pour déchiffrer les clés de données chiffrées afin qu'elles puissent être utilisées pour chiffrer vos données.

Vous pouvez révoquer l'accès à l'octroi ou supprimer l'accès du service à la clé gérée par le client à tout moment. Si c'est le cas, Résolution des entités AWS ne pourra accéder à aucune des données chiffrées par la clé gérée par le client, ce qui affecte les opérations qui dépendent de ces données. Par exemple, si vous supprimez l'accès au service à votre clé par le biais de l'autorisation et que vous tentez de démarrer une tâche pour un flux de travail correspondant chiffré à l'aide d'une clé client, l'opération renverra une `AccessDeniedException` erreur.

Création d'une clé gérée par le client

Vous pouvez créer une clé symétrique gérée par le client à l'aide du AWS Management Console, ou le AWS KMS APIs.

Pour créer une clé symétrique gérée par le client

Résolution des entités AWS prend en charge le chiffrement à l'aide de KMSclés de chiffrement symétriques. Suivez les étapes de création d'une clé symétrique gérée par le client dans AWS Key Management Service Guide du développeur.

Déclaration de politique clé

Les politiques de clés contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Lorsque vous créez votre clé

gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations, consultez la section Gestion de l'accès aux clés gérées par le client dans le AWS Key Management Service Guide du développeur.

Pour utiliser votre clé gérée par le client avec votre Résolution des entités AWS ressources, les API opérations suivantes doivent être autorisées dans la politique clé :

- `kms:DescribeKey`— Fournit des informations telles que la cléARN, la date de création (et la date de suppression, le cas échéant), l'état de la clé, ainsi que les dates d'origine et d'expiration (le cas échéant) du matériel clé. Il inclut des champs, tels que`KeySpec`, qui vous aident à distinguer les différents types de KMS clés. Il affiche également l'utilisation de la clé (chiffrement, signature ou génération et vérificationMACs) et les algorithmes pris en charge par la KMS clé. Résolution des entités AWS confirme que le `KeySpec` est `SYMMETRIC_DEFAULT` et l'`KeyUsage`est`ENCRYPT_DECRYPT`.
- `kms:CreateGrant` : ajoute une attribution à une clé gérée par le client. Accorde un accès de contrôle à une KMS clé spécifiée, ce qui permet d'accéder aux opérations d'octroi Résolution des entités AWS nécessite. Pour plus d'informations sur l'utilisation des subventions, consultez le AWS Key Management Service Guide du développeur.

Cela permet Résolution des entités AWS pour effectuer les opérations suivantes :

- Appelez `GenerateDataKey` pour générer une clé de données chiffrée et la stocker, car la clé de données n'est pas immédiatement utilisée pour chiffrer.
- Appelez `Decrypt` pour utiliser la clé de données chiffrée stockée afin d'accéder aux données chiffrées.
- Configurez un directeur partant à la retraite pour permettre au service de`RetireGrant`.

Vous trouverez ci-dessous des exemples de déclarations de politique que vous pouvez ajouter Résolution des entités AWS:

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

Autorisations pour les utilisateurs

Lorsque vous configurez une KMS clé comme clé par défaut pour le chiffrement, la politique de KMS clé par défaut permet à tout utilisateur ayant accès aux KMS actions requises d'utiliser cette KMS clé pour chiffrer ou déchiffrer des ressources. Vous devez autoriser les utilisateurs à effectuer les actions suivantes afin d'utiliser le chiffrement par KMS clé géré par le client :

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

Lors d'une `CreateMatchingWorkflow`demande, Résolution des entités AWS enverra une demande DescribeKeyet une CreateGrantdemande à AWS KMS en votre nom. Cela obligera l'IAMentité qui fait la `CreateMatchingWorkflow` demande avec une KMS clé gérée par le client à disposer des `kms:DescribeKey` autorisations relatives à la politique des KMS clés.

Lors d'une `StartIdMappingJob`demande `CreateIdMappingWorkflow`et, Résolution des entités AWS enverra une demande DescribeKeyet une CreateGrantdemande à AWS KMS en votre nom. Cela obligera l'IAMentité qui fait la `StartIdMappingJob` demande `CreateIdMappingWorkflow` et à l'aide d'une KMS clé gérée par le client à disposer `kms:DescribeKey` des autorisations relatives à la politique KMS clé. Les fournisseurs pourront accéder à la clé gérée par le client pour déchiffrer les données du Résolution des entités AWS Compartiment Amazon S3.

Vous trouverez ci-dessous des exemples de déclarations de politique que vous pouvez ajouter pour que les fournisseurs puissent déchiffrer les données contenues dans Résolution des entités AWS Compartiment Amazon S3 :

```
{
```

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

Remplacez chacun *<user input placeholder>* avec vos propres informations.

<KMSKeyARN>	AWS KMS Amazon Resource Name.

De même, l'IAMentité invoquant le `StartMatchingJobAPI`must have `kms:Decrypt` et `kms:GenerateDataKey` les autorisations sur la KMS clé gérée par le client fournie dans le flux de travail correspondant.

Pour plus d'informations sur la définition des autorisations dans une politique, consultez le AWS Key Management Service Guide du développeur.

Pour plus d'informations sur la résolution des problèmes d'accès par clé, consultez le AWS Key Management Service Guide du développeur.

Spécification d'une clé gérée par le client pour Résolution des entités AWS

Vous pouvez spécifier une clé gérée par le client en tant que seconde couche de chiffrement pour les ressources suivantes :

Flux de travail correspondant : lorsque vous créez une ressource de flux de travail correspondante, vous pouvez spécifier la clé de données en saisissant un KMSArn, qui Résolution des entités AWS utilise pour chiffrer les données personnelles identifiables stockées par la ressource.

KMSArn— Entrez une cléARN, qui est un identifiant de clé pour AWS KMS clé gérée par le client.

Vous pouvez spécifier une clé gérée par le client comme deuxième couche de chiffrement pour les ressources suivantes si vous créez ou exécutez un flux de travail de mappage d'identifiants sur deux Comptes AWS:

Workflow de mappage d'ID ou Start ID Mapping Workflow — Lorsque vous créez une ressource de flux de travail de mappage d'ID ou que vous démarrez un travail de workflow de mappage d'ID, vous pouvez spécifier la clé de données en saisissant un KMSArn, qui Résolution des entités AWS utilise pour chiffrer les données personnelles identifiables stockées par la ressource.

KMSArn— Entrez une cléARN, qui est un identifiant de clé pour AWS KMS clé gérée par le client.

Surveillance de vos clés de chiffrement pour Résolution des entités AWS Service

Lorsque vous utilisez un AWS KMS clé gérée par le client avec votre Résolution des entités AWS Des ressources de service que vous pouvez utiliser AWS CloudTrailou Amazon CloudWatch Logs pour suivre les demandes qui Résolution des entités AWS envoie à AWS KMS.

Les exemples suivants sont AWS CloudTrail événements pour`CreateGrant`, `GenerateDataKeyDecrypt`, et `DescribeKey` à surveiller AWS KMS opérations appelées par Résolution des entités AWS pour accéder aux données chiffrées à l'aide de la clé gérée par le client :

Rubriques

- CreateGrant
- DescribeKey
- GenerateDataKey
- Decrypt

CreateGrant

Lorsque vous utilisez un AWS KMS clé gérée par le client pour chiffrer la ressource de flux de travail correspondante, Résolution des entités AWS envoie une `CreateGrant` demande en votre nom pour accéder à la KMS clé de votre Compte AWS. La subvention qui Résolution des entités AWS les créations sont spécifiques à la ressource associée au AWS KMS clé gérée par le client. En outre, Résolution des entités AWS utilise l'`RetireGrant`opération pour supprimer une subvention lorsque vous supprimez une ressource.

L'exemple d'événement suivant enregistre l'opération `CreateGrant` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "entityresolution.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "retiringPrincipal": "entityresolution.region.amazonaws.com",
        "operations": [
            "GenerateDataKey",
            "Decrypt",
        ],
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "granteePrincipal": "entityresolution.region.amazonaws.com"
    },
    "responseElements": {
```

```
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

DescribeKey

Résolution des entités AWS utilise l'`DescribeKey`opération pour vérifier si AWS KMS La clé gérée par le client associée à votre ressource correspondante existe dans le compte et dans la région.

L'exemple d'événement suivant enregistre l'`DescribeKey`opération.

```
{
    "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

Lorsque vous activez un AWS KMS clé gérée par le client pour votre ressource de flux de travail correspondante, Résolution des entités AWS envoie une `GenerateDataKey` demande via Amazon Simple Storage Service (Amazon S3) à AWS KMS qui spécifie le AWS KMS clé gérée par le client pour la ressource.

L'exemple d'événement suivant enregistre l'`GenerateDataKey`opération.

```
{
    "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

Lorsque vous activez un AWS KMS clé gérée par le client pour votre ressource de flux de travail correspondante, Résolution des entités AWS envoie une `Decrypt` demande via Amazon Simple

Storage Service (Amazon S3) à AWS KMS qui spécifie le AWS KMS clé gérée par le client pour la ressource.

L'exemple d'événement suivant enregistre l'`Decrypt`opération.


```
{
    "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"
}
```

Considérations

Résolution des entités AWS ne prend pas en charge la mise à jour d'un flux de travail correspondant avec une nouvelle KMS clé gérée par le client. Dans ce cas, vous pouvez créer un nouveau flux de travail à l'aide de la KMS clé gérée par le client.

En savoir plus

Les ressources suivantes fournissent plus d'informations sur le chiffrement des données au repos.

Pour plus d'informations sur les concepts de base du service de gestion des AWS clés, consultez le AWS Key Management Service Guide du développeur.

Pour plus d'informations sur les meilleures pratiques de sécurité pour le service de gestion des AWS clés, consultez le AWS Key Management Service Guide du développeur.

Accès Résolution des entités AWS en utilisant un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez utiliser … AWS PrivateLink pour créer une connexion privée entre votre VPC et Résolution des entités AWS. Vous pouvez accéder Résolution des entités AWS comme s'il se trouvait dans votre maisonVPC, sans utiliser de passerelle Internet, d'NATappareil, de VPN connexion ou AWS Direct Connect connexion. Les instances de votre site VPC n'ont pas besoin d'adresses IP publiques pour y accéder Résolution des entités AWS.

Vous établissez cette connexion privée en créant un point de terminaison d'interface, alimenté par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison de l'interface. Il s'agit d'interfaces réseau gérées par les demandeurs qui servent de point d'entrée pour le trafic destiné à Résolution des entités AWS.

Pour plus d'informations, consultez Access Services AWS à travers AWS PrivateLink dans le .AWS PrivateLink Guide.

Considérations relatives à Résolution des entités AWS

Avant de configurer un point de terminaison d'interface pour Résolution des entités AWS, passez en revue les considérations figurant dans le AWS PrivateLink Guide.

Résolution des entités AWS permet d'appeler toutes ses API actions via le point de terminaison de l'interface.

VPCLes politiques relatives aux terminaux sont prises en charge pour Résolution des entités AWS. Par défaut, accès complet à Résolution des entités AWS est autorisé via le point de terminaison de l'interface. Vous pouvez également associer un groupe de sécurité aux interfaces réseau des terminaux pour contrôler le trafic vers Résolution des entités AWS via le point de terminaison de l'interface.

Créez un point de terminaison d'interface pour Résolution des entités AWS

Vous pouvez créer un point de terminaison d'interface pour Résolution des entités AWS à l'aide de la VPC console Amazon ou du AWS Command Line Interface (AWS CLI). Pour plus d'informations, voir Création d'un point de terminaison d'interface dans le AWS PrivateLink Guide.

Créez un point de terminaison d'interface pour Résolution des entités AWS en utilisant le nom de service suivant :

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

Si vous activez le mode privé DNS pour le point de terminaison de l'interface, vous pouvez envoyer des API demandes à Résolution des entités AWS en utilisant son DNS nom régional par défaut. Par exemple, `entityresolution.us-east-1.amazonaws.com`.

Création d'une politique de point de terminaison pour votre point de terminaison d'interface

Une politique de point de terminaison est une IAM ressource que vous pouvez associer à un point de terminaison d'interface. La politique de point de terminaison par défaut autorise un accès complet à Résolution des entités AWS via le point de terminaison de l'interface. Pour contrôler l'accès autorisé à Résolution des entités AWS depuis votreVPC, attachez une politique de point de terminaison personnalisée au point de terminaison de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Les principes qui peuvent effectuer des actions (Comptes AWS, IAM utilisateurs et IAM rôles).
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

Pour plus d'informations, voir Contrôler l'accès aux services à l'aide des politiques relatives aux terminaux dans le AWS PrivateLink Guide.

Exemple : politique de VPC point de terminaison pour Résolution des entités AWS actions

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous attachez cette politique au point de terminaison de votre interface, elle accorde l'accès aux Résolution des entités AWS des actions pour tous les principaux sur toutes les ressources.

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

Gestion des identités et des accès pour Résolution des entités AWS

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les Résolution des entités AWS ressources. IAMest un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

> **Note**
>
> Résolution des entités AWS prend en charge les politiques relatives aux comptes croisés. Pour plus d'informations, consultez la section Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez Résolution des entités AWS.

Utilisateur du service : si vous utilisez le Résolution des entités AWS service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles Résolution des entités AWS fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Résolution des entités AWS, consultez Résolution des problèmes Résolution des entités AWS d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des Résolution des entités AWS ressources de votre entreprise, vous avez probablement un accès complet à Résolution des entités AWS. C'est à vous de déterminer les Résolution des entités AWS fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base deIAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec Résolution des entités AWS, voirComment Résolution des entités AWS fonctionne avec IAM.

IAMadministrateur — Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Résolution des entités AWS. Pour consulter des exemples de politiques Résolution des entités AWS basées sur l'identité que vous pouvez utiliser dansIAM, consultez. Exemples de politiques basées sur l'identité pour Résolution des entités AWS

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la version 4 de AWS Signature pour les API demandes dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, voir Authentification multifactorielle dans le guide de l'AWS IAM Identity Center utilisateur et Authentification AWS multifactorielle IAM dans le guide de l'IAMutilisateur.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine

peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour

de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez la section Cas d'utilisation pour IAM les utilisateurs dans le Guide de IAM l'utilisateur.

IAMrôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Pour assumer temporairement un IAM rôle dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un IAM rôle (console). Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Méthodes pour assumer un rôle dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir Créer un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy).

Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un Service AWS dans le guide de IAM l'utilisateur.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui AWS CLI soumettent des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utiliser un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Gestion des accès à l’aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C’est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d’aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d’une politique qui autorise l’action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l’identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, voir Définir des IAM autorisations personnalisées avec des politiques gérées par le client dans le Guide de l'IAMutilisateur.

Les politiques basées sur l’identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les

politiques AWS gérées et les politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre les politiques gérées et les politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur

l’identité d’une entité et de ses limites d’autorisation. Les politiques basées sur les ressources qui spécifient l’utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d’autorisations. Un refus explicite dans l’une de ces politiques annule l’autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.

- Politiques de contrôle des services (SCPs) : SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l’identité de l’utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d’une politique basée sur les ressources. Un refus explicite dans l’une de ces politiques annule l’autorisation. Pour plus d'informations, consultez la section Politiques de session dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s’appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment Résolution des entités AWS fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Résolution des entités AWS, découvrez quelles IAM fonctionnalités sont disponibles Résolution des entités AWS.

IAMfonctionnalités que vous pouvez utiliser avec Résolution des entités AWS

IAMfonctionnalité	Résolution des entités AWS soutien
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC(balises dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Transférer les sessions d'accès (FAS)	Oui
Rôles de service	Oui
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont Résolution des entités AWS les autres AWS services fonctionnent avec la plupart des IAM fonctionnalités, consultez la section AWS Services compatibles IAM dans le Guide de IAM l'utilisateur.

Politiques basées sur l'identité pour Résolution des entités AWS

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, voir Définir des IAM autorisations personnalisées avec des politiques gérées par le client dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Exemples de politiques basées sur l'identité pour Résolution des entités AWS

Pour consulter des exemples de politiques Résolution des entités AWS basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Résolution des entités AWS

Politiques basées sur les ressources au sein de Résolution des entités AWS

Prend en charge les politiques basées sur les ressources : Oui

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte de confiance doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Actions politiques pour Résolution des entités AWS

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des Résolution des entités AWS actions, reportez-vous à la section Actions définies par Résolution des entités AWS dans la référence d'autorisation de service.

Les actions de politique en Résolution des entités AWS cours utilisent le préfixe suivant avant l'action :

```
entityresolution
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour consulter des exemples de politiques Résolution des entités AWS basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Résolution des entités AWS

Ressources politiques pour Résolution des entités AWS

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de Résolution des entités AWS ressources et leurs caractéristiquesARNs, consultez la section Ressources définies par Résolution des entités AWS dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier pour chaque ressource, consultez la ARN section Actions définies par Résolution des entités AWS.

Pour consulter des exemples de politiques Résolution des entités AWS basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Résolution des entités AWS

Clés de conditions de politique pour Résolution des entités AWS

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez

plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Pour consulter la liste des clés de Résolution des entités AWS condition, voir Clés de condition pour Résolution des entités AWS la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, voir Actions définies par Résolution des entités AWS.

Pour consulter des exemples de politiques Résolution des entités AWS basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Résolution des entités AWS

ACLsdans Résolution des entités AWS

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

ABACavec Résolution des entités AWS

Supports ABAC (balises dans les politiques) : Partiel

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informationsABAC, voir Définir des autorisations avec ABAC autorisation dans le Guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Utilisation d'informations d'identification temporaires avec Résolution des entités AWS

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation IAM dans le Guide de IAM l'utilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, voir Passer d'un utilisateur à un IAM rôle (console) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI ou AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour Résolution des entités AWS

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Rôles de service pour Résolution des entités AWS

Prend en charge les rôles de service : oui

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un Service AWS dans le guide de IAM l'utilisateur.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber Résolution des entités AWS les fonctionnalités. Modifiez les rôles de service uniquement lorsque Résolution des entités AWS vous recevez des instructions à cet effet.

Rôles liés à un service pour Résolution des entités AWS

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés à un service, consultez la section AWS Services compatibles avec. IAM Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Résolution des entités AWS

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources Résolution des entités AWS . Ils ne peuvent pas non plus effectuer de tâches en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, voir Créer des IAM politiques (console) dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par Résolution des entités AWS, y compris le format de ARNs pour chacun des types de ressources, voir Actions, ressources et clés de condition Résolution des entités AWS dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Résolution des entités AWS
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer Résolution des entités AWS des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez

les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.

- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Valider les politiques avec IAM Access Analyzer dans le guide de l'IAMutilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section APIAccès sécurisé avec MFA dans le guide de IAM l'utilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console Résolution des entités AWS

Pour accéder à la Résolution des entités AWS console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails Résolution des entités AWS des ressources de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui passent des appels uniquement vers le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'APIopération qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la Résolution des entités AWS console, associez également la politique Résolution des entités AWS *ConsoleAccess* ou la politique *ReadOnly* AWS gérée aux entités. Pour plus d'informations, consultez la section Ajouter des autorisations à un utilisateur dans le Guide de IAM l'utilisateur.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. AWS API

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

```
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiques gérées pour Résolution des entités AWS

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSEntityResolutionConsoleFullAccess

Vous pouvez associer la politique `AWSEntityResolutionConsoleFullAccess` à vos identités IAM.

Cette politique accorde un accès complet aux Résolution des entités AWS points de terminaison et aux ressources.

Cette politique autorise également certains accès en lecture à des éléments connexes Services AWS tels que S3 AWS Glue, le balisage, AWS KMS afin que la console puisse afficher les choix et utiliser ceux sélectionnés pour effectuer des actions de résolution d'entités. Certaines ressources sont réduites pour contenir le nom `entityresolution` du service.

Comme elle Résolution des entités AWS repose sur un rôle transmis pour effectuer des actions sur les AWS ressources associées, cette politique accorde également les autorisations nécessaires pour sélectionner et transmettre le rôle souhaité.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `EntityResolutionAccess`— Permet aux principaux un accès complet aux Résolution des entités AWS points de terminaison et aux ressources.
- `GlueSourcesConsoleDisplay`— Accorde l'accès aux AWS Glue tables de liste en tant qu'options de source de données et le schéma de table d'importation d'une source de données pour l'expérience utilisateur.
- `S3BucketsConsoleDisplay`— Accorde l'accès à la liste de tous les compartiments S3 en tant qu'options de source de données.
- `S3SourcesConsoleDisplay`— Accorde l'accès permettant d'afficher les compartiments S3 en tant qu'options de source de données.
- `TaggingConsoleDisplay`— Permet de lire les clés et les valeurs de balisage.
- `KMSConsoleDisplay`— Permet de décrire les clés et de répertorier les alias AWS Key Management Service pour déchiffrer et chiffrer les sources de données.
- `ListRolesToPickForPassing`— Accorde l'accès à la liste de tous les rôles afin que l'utilisateur puisse choisir le rôle à transmettre.
- `PassRoleToEntityResolutionService`— Accorde l'accès permettant de transmettre un rôle restreint au Résolution des entités AWS service.

- `ManageEventBridgeRules`— Accorde l'accès pour créer, mettre à jour et supprimer la EventBridge règle Amazon pour recevoir les notifications S3.
- `ADXReadAccess`— Accorde l'accès AWS Data Exchange à pour vérifier si le client a un droit ou un abonnement.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EntityResolutionAccess",
            "Effect": "Allow",
            "Action": [
                "entityresolution:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GlueSourcesConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "glue:GetSchema",
                "glue:SearchTables",
                "glue:GetSchemaByDefinition",
                "glue:GetSchemaVersion",
                "glue:GetSchemaVersionsDiff",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetTableVersion",
                "glue:GetTableVersions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3BucketsConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
```

```
        {
            "Sid": "S3SourcesConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:ListBucketVersions",
                "s3:GetBucketVersioning"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TaggingConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSConsoleDisplay",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListRolesToPickRoleForPassing",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PassRoleToEntityResolutionService",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*entityresolution*",
```

```
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "entityresolution.amazonaws.com"
                    ]
                }
            }
        },
        {
           "Sid": "ManageEventBridgeRules",
           "Effect": "Allow",
           "Action": [
              "events:PutRule",
              "events:DeleteRule",
              "events:PutTargets",
           ],
           "Resource": [
                "arn:aws:events:*:*:rule/entity-resolution-automatic*"
           ]
        },
        {
            "Sid": "ADXReadAccess",
            "Effect": "Allow",
            "Action": [
                "dataexchange:GetDataSet"
            ],
            "Resource": "*"
        },
    ]
}
```

AWS politique gérée : AWSEntityResolutionConsoleReadOnlyAccess

Vous pouvez attacher `AWSEntityResolutionConsoleReadOnlyAccess` à vos entités IAM.

Cette politique accorde un accès en lecture seule aux Résolution des entités AWS points de terminaison et aux ressources.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `EntityResolutionRead`— Permet aux principaux d'accéder en lecture seule aux points de Résolution des entités AWS terminaison et aux ressources.

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

Résolution des entités AWS mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées Résolution des entités AWS depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du Résolution des entités AWS document.

Modification	Description	Date
`AWSEntityResolutionConsoleFullAccess` – Mise à jour de la politique existante	Ajouté `ADXReadAccess` et `ManageEventBridgeRules` pour activer l'option des services du fournisseur dans le flux de travail correspondant.	16 octobre 2023
Résolution des entités AWS a commencé à suivre les modifications	Résolution des entités AWS a commencé à suivre les modifications apportées AWS à ses politiques gérées.	18 août 2023

Résolution des problèmes Résolution des entités AWS d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Résolution des entités AWS etIAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans Résolution des entités AWS

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit lorsque l'`mateojackson`IAMutilisateur essaie d'utiliser la console pour afficher les détails d'une *`my-example-widget`* ressource fictive mais ne dispose pas des `entityresolution:`*`GetWidget`* autorisations fictives.

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

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-widget`* à l'aide de l'action `entityresolution:`*`GetWidget`*.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à Résolution des entités AWS.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Résolution des entités AWS. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes Résolution des entités AWS ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises Résolution des entités AWS en charge, consultezComment Résolution des entités AWS fonctionne avec IAM.
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.

- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

Validation de conformité pour Résolution des entités AWS

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la HIPAA sécurité et la conformité sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

> **Note**
>
> Tous ne Services AWS sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et reprennent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST),

le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).

- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résolution des entités AWS meilleures pratiques en matière de conformité

Cette section fournit les meilleures pratiques et les recommandations relatives à la conformité lorsque vous utilisez Résolution des entités AWS.

Normes de sécurité des données du secteur des cartes de paiement (PCIDSS)

Résolution des entités AWS prend en charge le traitement, le stockage et la transmission des données de carte de crédit par un commerçant ou un fournisseur de services, et sa conformité à la norme de sécurité des données de l'industrie des cartes de paiement (PCI) a été validée (DSS). Pour plus d'informations PCIDSS, notamment sur la manière de demander une copie du Package de AWS PCI conformité, consultez le PCIDSSniveau 1.

Contrôles du système et de l'organisation (SOC)

Résolution des entités AWS est conforme aux mesures de contrôle du système et de l'organisation (SOC), y compris les mesures SOC 1, SOC 2 et SOC 3. SOCles rapports sont des rapports d'examen indépendants réalisés par des tiers qui montrent comment AWS atteindre les principaux

contrôles et objectifs de conformité. Ces audits garantissent que les protections et procédures adéquates sont établies pour protéger contre les risques susceptibles d'avoir une incidence sur la sécurité, la confidentialité et la disponibilité des données des clients et des entreprises. Les résultats de ces audits tiers sont disponibles sur le site Web de AWS SOC conformité, où vous pouvez consulter les rapports publiés pour obtenir plus d'informations sur les contrôles qui soutiennent les AWS opérations et la conformité.

Résilience dans Résolution des entités AWS

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, Résolution des entités AWS propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Surveillance Résolution des entités AWS

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité Résolution des entités AWS et des performances de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller Résolution des entités AWS, signaler tout problème et prendre des mesures automatiques le cas échéant :

- AWS CloudTrailcapture les appels d'API et les événements associés effectués par vous ou en votre nom Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Rubriques

- Journalisation des appels Résolution des entités AWS d'API à l'aide AWS CloudTrail

Journalisation des appels Résolution des entités AWS d'API à l'aide AWS CloudTrail

Résolution des entités AWS est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Résolution des entités AWS. CloudTrail capture tous les appels d'API Résolution des entités AWS sous forme d'événements. Les appels capturés incluent des appels provenant de la Résolution des entités AWS console et des appels de code vers les opérations de l' Résolution des entités AWS API. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour Résolution des entités AWS. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite Résolution des entités AWS, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Résolution des entités AWS informations dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Résolution des entités AWS, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre région Compte AWS, y compris des événements pour Résolution des entités AWS, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les Résolution des entités AWS actions sont enregistrées CloudTrail et documentées dans la référence de l'Résolution des entités AWS API.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Comprendre les entrées du fichier Résolution des entités AWS journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Créez des ressources de résolution d'AWSentités avec AWS CloudFormation

AWSEntity Resolution est intégré à AWS CloudFormation un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à créer et à gérer vos ressources et votre infrastructure. Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez (telles que AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace et AWS::EntityResolution::PolicyStatement), et qui AWS CloudFormation fournit et configure ces ressources pour vous.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources de résolution d'AWSentités de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis distribuez les mêmes ressources encore et encore dans plusieurs Comptes AWS régions.

AWSRésolution d'entité et AWS CloudFormation modèles

Pour fournir et configurer des ressources pour AWS Entity Resolution et les services associés, vous devez comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés dans JSON ouYAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous ne connaissez pas JSON ouYAML, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec les AWS CloudFormation modèles. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormation Guide de l'utilisateur.

AWSEntity Resolution prend en charge la création AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace et AWS::EntityResolution::PolicyStatement l'entrée AWS CloudFormation. Pour plus d'informations, notamment des exemples JSON et des YAML modèles pour AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution:IdMappingWorkflow, AWS::EntityResolution::IdNamespace et AWS::EntityResolution::PolicyStatement, consultez la référence au type de ressource AWS Entity Resolution dans le guide de AWS CloudFormation l'utilisateur.

Les modèles suivants sont disponibles :

- Flux de travail correspondant

  Créez un `MatchingWorkflow` objet qui stocke la configuration de la tâche de traitement des données à exécuter.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::EntityResolution::MatchingWorkflow dans le guide de l'utilisateur AWS CloudFormation

  CreateMatchingWorkflowdans la Résolution des entités AWS APIréférence
- Cartographie du schéma

  Créez un mappage de schéma, qui définit le schéma de la table des enregistrements clients en entrée.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::EntityResolution::SchemaMapping dans le guide de l'utilisateur AWS CloudFormation

  CreateSchemaMappingdans la Résolution des entités AWS APIréférence
- Workflow de mappage des identifiants

  Créez un `IdMappingWorkflow` objet qui stocke la configuration de la tâche de traitement des données à exécuter.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::EntityResolution::IdMappingWorkflow dans le guide de l'utilisateur AWS CloudFormation

  CreateIdMappingWorkflowdans la Résolution des entités AWS APIréférence
- Espace de noms ID

  Créez un `IdNamespace` objet qui stocke les métadonnées expliquant le jeu de données et son utilisation.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::EntityResolution::IdNamespace dans le guide de l'utilisateur AWS CloudFormation

  CreateIdNamespacedans la Résolution des entités AWS APIréférence
- PolicyStatement

Créez un objet `PolicyStatement`.

Pour plus d’informations, consultez les rubriques suivantes :

AWS::EntityResolution::PolicyStatement dans le guide de l'utilisateur AWS CloudFormation

AddPolicyStatementdans la Résolution des entités AWS APIréférence

En savoir plus sur AWS CloudFormation

Pour en savoir plus AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur
- AWS CloudFormation APIRéférence
- AWS CloudFormation Guide de l'utilisateur de l'interface de ligne de commande

Quotas pour Résolution des entités AWS

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, mais d'autres quotas ne peuvent pas être augmentés.

Pour consulter les quotas pour Résolution des entités AWS, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez AWSles services, puis sélectionnez Résolution des entités AWS.

Pour demander une augmentation de quota, consultez Demander une augmentation de quota dans le Guide de l'utilisateur de Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le formulaire d'augmentation des limites.

Vous Compte AWS disposez des quotas suivants relatifs à Résolution des entités AWS.

Nom	Par défaut	Ajustable	Description
Tâches de mappage d'identifiants simultan	1	Non	Le nombre maximum de tâches de mappage d'identifiants qui peuvent être traitées simultanément dans le courant Région AWS.
Tâches correspondantes simultanées	1	Non	Le nombre maximum de tâches correspondantes qui peuvent être traitées simultanément dans le courant Région AWS.
Tâches simultanées de mise en correspondance des fournisseurs	1	Non	Le nombre maximum de tâches correspondant aux services du fournisseur qui peuvent être traitées simultanément dans le courant Région AWS.
Données en entrée	20	Non	Il s'agit de la liste des tables d'entrée que vous souhaitez utiliser dans un flux de travail correspondant. Chaque entrée correspond à une colonne de

Nom	Par défaut	Ajustable	Description
			votre table de données AWS Glue d'entrée, qui contient le nom de la colonne et des informations supplémentaires à Résolution des entités AWS utiliser à des fins de correspondance. Les entrées doivent contenir un identifiant unique et au moins un champ de saisie supplémentaire.
Sortie de données	750	Non	Il s'agit d'une liste d'`OutputAttribute` objets dont chacun possède les champs Name et Hashed. Chacun de ces objets représente une colonne à inclure dans la table AWS Glue de sortie et indique si vous souhaitez que les valeurs de la colonne soient hachées.
Schéma de données	25	Non	Nombre maximal de champs de saisie du schéma de données.
Workflows de mappage des identifiants	10	Oui	Le nombre maximum de flux de travail de mappage d'identifiants que vous pouvez créer Compte AWS dans ce cadre est actuellement Région AWS.
Espaces de noms d'ID	10	Oui	Le nombre maximum d'espaces de noms d'identification que vous pouvez créer Compte AWS dans cet espace est actuellement Région AWS.
Match IDs	500	Non	Le nombre maximum d'enregis trements pouvant être consolidés sous un seul MatchID par charge de travail.

Nom	Par défaut	Ajustable	Description
Règle de correspondance	15	Non	Pour le rapprochement basé sur des règles, il s'agit du numéro de règle appliqué qui a généré un ensemble d'enregistrements appariés. Cela fait partie des métadonnées de flux de travail correspondantes qui seront incluses dans la sortie.
Flux de travail correspondants	10	Oui	Le nombre maximum de flux de travail correspondants.
Nombre de règles par flux de travail	15	Non	Le nombre maximum de règles par flux de travail correspondant.
Taux de `GetMatchId` API demandes	50	Oui	Le nombre maximum de `GetCustomerID` API demandes par seconde.
Mappages de schémas	50	Oui	Le nombre maximum de mappages de schéma que vous pouvez créer dans ce compte dans la AWS région actuelle.

Nom	Par défaut	Ajustable	Description
Clés de correspondance uniques par ensemble de règles	15	Non	Le nombre maximum de clés de correspondance uniques par ensemble de règles. Une touche de correspondance indique Résolution des entités AWS quels champs de saisie doivent être considérés comme des données similaires et lesquels doivent être considérés comme des données différentes. Cela permet de configurer Résolution des entités AWS automatiquement des règles de correspondance basées sur des règles et de comparer des données similaires stockées dans différents champs de saisie.

Limitations d'API

Ressource	Limite de débit	Description
Taux de `CreateMatchingWorkflow` demandes	5 TPS	Nombre maximum d'`CreateMatchingWorkflow` APIappels par seconde.
Taux de `DeleteMatchingWorkflow` demandes	5 TPS	Nombre maximum d'`DeleteMatchingWorkflow` APIappels par seconde.
Taux de `GetMatchingWorkflow` demandes	5 TPS	Nombre maximum d'`GetMatchingWorkflow` APIappels par seconde.
Taux de `ListMatchingWorkflows` demandes	5 TPS	Nombre maximum d'`ListMatchingWorkflows` APIappels par seconde.

Ressource	Limite de débit	Description
Taux de `UpdateMatchingWorkflow` demandes	5 TPS	Nombre maximum d'`UpdateMatchingWorkflow` APIappels par seconde.
Taux de `CreateSchemaMapping` demandes	5 TPS	Nombre maximum d'`CreateSchemaMapping` APIappels par seconde.
Taux de `DeleteSchemaMapping` demandes	5 TPS	Nombre maximum d'`DeleteSchemaMapping` APIappels par seconde.
Taux de `GetSchemaMapping` demandes	5 TPS	Nombre maximum d'`GetSchemaMapping` APIappels par seconde.
Taux de `ListSchemaMappings` demandes	5 TPS	Nombre maximum d'`ListSchemaMappings` APIappels par seconde.
Taux de `UpdateSchemaMapping` demandes	5 TPS	Nombre maximum d'`UpdateSchemaMapping` APIappels par seconde.
Taux de `GetPartnerComponent` demandes	5 TPS	Nombre maximum d'`GetPartnerComponent` APIappels par seconde.
Taux de `ListPartnerComponents` demandes	5 TPS	Nombre maximum d'`ListPartnerComponents` APIappels par seconde.
Taux de `TagResource` demandes	5 TPS	Nombre maximum d'`TagResource` APIappels par seconde.

Ressource	Limite de débit	Description
Taux de `UntagResource` demandes	5 TPS	Nombre maximum d'`UntagResource` APIappels par seconde.
Taux de `ListTagsForResource` demandes	5 TPS	Nombre maximum d'`ListTagsForResource` APIappels par seconde.
Taux de `CreateIdMappingWorkflow` demandes	5 TPS	Nombre maximum d'`CreateIdMappingWorkflow` APIappels par seconde.
Taux de `DeleteIdMappingWorkflow` demandes	5 TPS	Nombre maximum d'`DeleteIdMappingWorkflow` APIappels par seconde.
Taux de `GetIdMappingWorkflow` demandes	5 TPS	Nombre maximum d'`GetIdMappingWorkflow` APIappels par seconde.
Taux de `ListIdMappingWorkflow` demandes	5 TPS	Nombre maximum d'`ListIdMappingWorkflow` APIappels par seconde.
Taux de `UpdateIdMappingWorkflow` demandes	5 TPS	Nombre maximum d'`UpdateIdMappingWorkflow` APIappels par seconde.
Taux de `ListProviderServices` demandes	5 TPS	Nombre maximum d'`ListProviderServices` APIappels par seconde.

Ressource	Limite de débit	Description
Taux de GetProvid erService demandes	5 TPS	Nombre maximum d'GetProviderService APIappels par seconde.
Taux de CreateIdN amespace demandes	5 TPS	Nombre maximum d'CreateIdN amespace APIappels par seconde.
Taux de DeleteIdN amespace demandes	5 TPS	Nombre maximum d'DeleteIdN amespace APIappels par seconde.
Taux de GetIdNamespace demandes	5 TPS	Nombre maximum d'GetIdName space APIappels par seconde.
Taux de ListIdNam espaces demandes	5 TPS	Nombre maximum d'ListIdNam espaces APIappels par seconde.
Taux de UpdateIdN amespace demandes	5 TPS	Nombre maximum d'UpdateIdN amespace APIappels par seconde.
Taux de AddPolicy Statement demandes	5 TPS	Nombre maximum d'AddPolicyStatement APIappels par seconde.
Taux de DeletePol icyStatement demandes	5 TPS	Nombre maximum d'DeletePolicyStatem ent APIappels par seconde.

Ressource	Limite de débit	Description
Taux de `GetPolicy` demandes	5 TPS	Nombre maximum d'`GetPolicy` APIappels par seconde.
Taux de `PutPolicy` demandes	5 TPS	Nombre maximum d'`PutPolicy` APIappels par seconde.
Taux de `GetMatchingJob` demandes	10 TPS	Nombre maximum d'`GetMatchingJob` APIappels par seconde.
Taux de `ListMatchingJobs` demandes	5 TPS	Nombre maximum d'`ListMatchingJobs` APIappels par seconde.
Taux de `StartMatchingJob` demandes	5 TPS	Nombre maximum d'`StartMatchingJob` APIappels par seconde.
Taux de `GetMatchId` demandes	50 TPS	Nombre maximum d'`GetMatchId` APIappels par seconde.
Taux de `GetIdMappingJob` demandes	10 TPS	Nombre maximum d'`GetIdMappingJob` APIappels par seconde.
Taux de `ListIdMappingJobs` demandes	5 TPS	Nombre maximum d'`ListIdMappingJobs` APIappels par seconde.

Ressource	Limite de débit	Description
Taux de `StartIdMappingJob` demandes	5 TPS	Nombre maximum d'`StartIdMappingJob` APIappels par seconde.
Taux de `BatchDeleteUniqueId` demandes	5 TPS	Nombre maximum d'`BatchDeleteUniqueId` APIappels par seconde.

Historique du document pour le guide de Résolution des entités AWS l'utilisateur

Le tableau suivant décrit les versions de documentation pour Résolution des entités AWS.

Pour être informé des mises à jour de cette documentation, vous pouvez vous abonner au RSS flux. Pour vous abonner aux RSS mises à jour, un RSS plug-in doit être activé pour le navigateur que vous utilisez.

Modification	Description	Date
Intégration des fournisseurs	Mise à jour de documentation uniquement. Les clients peuvent apprendre comment s'intégrer en tant que fournisseur de services à Résolution des entités AWS.	8 août 2024
Workflow de mappage des identifiants — mise à jour	Les clients peuvent désormais utiliser des règles de correspondance pour traduire des données de première partie dans un flux de travail de mappage d'identifiants.	23 juillet 2024
Flux de travail correspondant — mise à jour	Les clients peuvent désormais supprimer les enregistrements d'un flux de travail de correspondance basé sur des règles ou basé sur le ML afin de se conformer aux réglementations en matière de gestion des données.	8 avril 2024
Workflow de mappage des identifiants — mise à jour	Les clients peuvent désormais utiliser un flux de travail de	2 avril 2024

	mappage d'identifiants sur plusieurs Comptes AWS.	
AWS CloudFormation Ressources - Ressources nouvelles et mises à jour	AWSEntity Resolution a ajouté les ressources suivantes : `AWS::EntityResolution::IdNamespace` `AWS::EntityResolution::PolicyStatement` et a mis à jour la ressource suivante :`AWS::EntityResolution::IdMappingWorkflow` .	2 avril 2024
Trouver l'identifiant du match	Les clients peuvent désormais trouver le Match ID correspondant et la règle associée pour un flux de travail traité basé sur des règles.	25 mars 2024
Flux de travail correspondant — mise à jour	Résolution des entités AWS prend désormais en charge l'RAMPIDattribution PII basée sur les services du LiveRamp fournisseur dans le flux de travail de correspondance.	12 février 2024
AWS PrivateLink	Résolution des entités AWS prend désormais en charge une sécurité supplémentaire des données, AWS PrivateLink ce qui permet aux clients d'accéder de manière privée aux services hébergés sur AWS.	20 octobre 2023

AWS CloudFormation Ressources — Ressources nouvelles et mises à jour	Résolution des entités AWS a ajouté la ressource suivante : `AWS::EntityResolution:IdMappingWorkflow` et a mis à jour les ressources suivantes : `AWS::EntityResolution::MatchingWorkflow` et`AWS::EntityResolution::Schemamapping` .	19 octobre 2023
Mise à jour de la politique existante	Les nouvelles autorisations suivantes ont été ajoutées à la politique `AWSEntityResolutionConsoleFullAccess` gérée : `ADXReadAccess` et`ManageEventBridgeRules` .	16 octobre 2023
Cartographie du schéma — mise à jour	Les clients ont désormais la possibilité de modifier et de mettre à jour un schéma de données existant.	16 octobre 2023
Flux de travail correspondant — mise à jour	Les clients peuvent désormais sélectionner un service de fournisseur de données préféré pour les aider à faire correspondre et à lier leurs données.	16 octobre 2023

Workflow de mappage des identifiants	Les clients peuvent utiliser ce nouveau flux de travail pour spécifier les détails du mappage des identifiants, choisir la méthode de mappage des identifiants de leur choix et spécifier les champs d'entrée et de sortie des données.	16 octobre 2023
AWS CloudFormation intégration	Résolution des entités AWS s'intègre désormais à AWS CloudFormation.	24 août 2023
AWS mise à jour des politiques gérée - Nouvelles politiques	Résolution des entités AWS a ajouté deux nouvelles politiques gérées.	18 août 2023
Première version	Publication initiale du guide de Résolution des entités AWS l'utilisateur	26 juillet 2023

Résolution des entités AWS Glossaire

Nom de la ressource Amazon (ARN)

Identifiant unique pour les AWS ressources. ARNssont obligatoires lorsque vous devez spécifier une ressource sans ambiguïté dans l'ensemble, par exemple dans les Résolution des entités AWS politiques Résolution des entités AWS, les balises Amazon Relational Database Service (AmazonRDS) et les appels. API

Traitement automatique

Une option de cadence de traitement pour une tâche de flux de travail correspondante qui permet de l'exécuter automatiquement lorsque votre saisie de données change.

Cette option n'est disponible que pour le rapprochement basé sur des règles.

Par défaut, la cadence de traitement d'une tâche de flux de travail correspondante est définie sur Manuel, ce qui permet de l'exécuter à la demande. Vous pouvez configurer le traitement automatique pour exécuter automatiquement la tâche de flux de travail correspondante lorsque votre saisie de données change. Cela permet de conserver le résultat correspondant à votre flux de travail up-to-date.

AWS KMS key ARN

Il s'agit de votre nom de ressource AWS KMS Amazon (ARN) pour le chiffrement au repos. Si elle n'est pas fournie, le système utilisera une KMS clé Résolution des entités AWS gérée.

Texte clair

Données qui ne sont pas protégées par cryptographie.

Niveau de confiance (ConfidenceLevel)

Pour la correspondance ML, il s'agit du niveau de confiance appliqué Résolution des entités AWS lorsque ML identifie un ensemble d'enregistrements correspondants. Cela fait partie des métadonnées de flux de travail correspondantes qui seront incluses dans la sortie.

Déchiffrement

Processus qui consiste à remettre les données chiffrées dans leur forme d'origine. Le déchiffrement ne peut être effectué que si vous avez accès à la clé secrète.

Chiffrement

Processus consistant à coder des données sous une forme qui semble aléatoire à l'aide d'une valeur secrète appelée clé. Il est impossible de déterminer le texte brut d'origine sans accéder à la clé.

Nom du groupe

Le nom du groupe fait référence à l'ensemble des champs de saisie et peut vous aider à regrouper les données analysées à des fins de correspondance.

Par exemple, s'il existe trois champs de saisie : **`first_namemiddle_name`**, et**`last_name`**, vous pouvez les regrouper en saisissant le nom du groupe comme **`full_name`** pour la correspondance et la sortie.

Hachage

Le hachage consiste à appliquer un algorithme cryptographique qui produit une chaîne de caractères unique et irréversible de taille fixe, appelée hachage. Résolution des entités AWS utilise le protocole de hachage 256 bits (SHA256) de l'algorithme de hachage sécurisé et produira une chaîne de caractères de 32 octets. Dans Résolution des entités AWS, vous pouvez choisir de hacher ou non les valeurs des données dans votre sortie.

Protocole de hachage () HashingProtocol

Résolution des entités AWS utilise le protocole de hachage 256 bits (SHA256) de l'algorithme de hachage sécurisé et produira une chaîne de caractères de 32 octets. Cela fait partie des métadonnées de flux de travail correspondantes qui seront incluses dans la sortie.

Méthode de mappage des identifiants

Comment souhaitez-vous que le mappage des identifiants soit effectué.

Il existe deux méthodes de mappage des identifiants :

- Basée sur des règles : méthode par laquelle vous utilisez des règles de correspondance pour traduire des données de première partie d'une source vers une cible dans un flux de travail de mappage d'identifiants.
- Services du fournisseur : méthode par laquelle vous utilisez un service fournisseur pour traduire des données codées par des tiers d'une source vers une cible dans un flux de travail de mappage d'identifiants.

  Résolution des entités AWS est actuellement prise en charge en LiveRamp tant que méthode de mappage d'identifiants basée sur les services des fournisseurs. Vous devez être abonné à LiveRamp through AWS Data Exchange pour utiliser cette méthode. Pour de plus amples informations, veuillez consulter Étape 1 : Abonnez-vous à un service fournisseur sur AWS Data Exchange.

Workflow de mappage des identifiants

Une tâche de traitement de données qui mappe les données d'une source de données d'entrée vers une cible de données d'entrée en fonction de la méthode de mappage d'ID spécifiée. Il produit une table de mappage des identifiants. Ce flux de travail vous oblige à spécifier la méthode de mappage des identifiants et les données d'entrée que vous souhaitez traduire d'une source vers une cible.

Vous pouvez configurer un flux de travail de mappage d'identifiants pour qu'il s'exécute seul Compte AWS ou en deux Comptes AWS.

Espace de noms ID

Une ressource Résolution des entités AWS qui contient des métadonnées expliquant les ensembles de données sur plusieurs Comptes AWS et expliquant comment utiliser ces ensembles de données dans un flux de travail de mappage d'identifiants.

Il existe deux types d'espaces de noms d'ID : `SOURCE` et`TARGET`. `SOURCE`contient les configurations des données sources qui seront traitées dans un flux de travail de mappage d'identifiants. `TARGET`Contient une configuration des données cibles vers laquelle toutes les sources seront résolues. Pour définir les données d'entrée que vous souhaitez résoudre entre deux Comptes AWS, créez une source d'espace de noms ID et une cible d'espace de noms ID pour traduire vos données d'un ensemble (`SOURCE`) à un autre (). `TARGET`

Une fois que vous et un autre membre avez créé des espaces de noms d'identification et exécuté un flux de travail de mappage d'identifiants, vous pouvez rejoindre une collaboration AWS Clean Rooms pour exécuter une jointure multitable sur la table de mappage d'identifiants et analyser les données.

Pour plus d'informations, consultez le AWS Clean Rooms Guide de l'utilisateur .

Champ de saisie

Un champ de saisie correspond au nom d'une colonne de votre table de données AWS Glue d'entrée.

Source d'entrée ARN (InputSourceARN)

Le nom de ressource Amazon (ARN) qui a été généré pour une entrée de AWS Glue table. Cela fait partie des métadonnées de flux de travail correspondantes qui seront incluses dans la sortie.

Type d'entrée

Type de données d'entrée. Vous le sélectionnez dans une liste préconfigurée de valeurs telles que le nom, l'adresse, le numéro de téléphone ou l'adresse e-mail. Le type d'entrée indique Résolution des entités AWS le type de données que vous présentez, ce qui permet de les classer et de les normaliser correctement.

Correspondance basée sur le machine learning

La mise en correspondance basée sur l'apprentissage automatique (ML matching) permet de trouver des correspondances entre vos données qui peuvent être incomplètes ou ne pas avoir exactement la même apparence. La correspondance ML est un processus prédéfini qui tentera de faire correspondre les enregistrements de toutes les données que vous entrez. La correspondance ML renvoie un ID de correspondance et un niveau de confiance pour chaque ensemble de données correspondant.

Traitement manuel

Option de cadence de traitement pour une tâche de flux de travail correspondante qui permet de l'exécuter à la demande.

Cette option est définie par défaut et est disponible à la fois pour la correspondance basée sur des règles et pour la correspondance basée sur l'apprentissage automatique.

Many-to-Many appariement

Many-to-many matching compare plusieurs instances de données similaires. Les valeurs des champs de saisie auxquels la même clé de correspondance a été attribuée seront comparées les unes aux autres, qu'elles se trouvent dans le même champ de saisie ou dans des champs de saisie différents.

Par exemple, vous pouvez avoir plusieurs champs de saisie de numéros de téléphone, tels `home_phone` que `mobile_phone` et qui ont la même touche de correspondance « Téléphone ». Utilisez le many-to-many rapprochement pour comparer les données du champ de `mobile_phone` saisie aux données du champ de `mobile_phone` saisie et aux données du champ de `home_phone` saisie.

Les règles de correspondance évaluent les données de plusieurs champs de saisie avec la même clé de correspondance à l'aide d'une opération (ou), et le one-to-many rapprochement compare les valeurs entre plusieurs champs de saisie. Cela signifie que si une combinaison `mobile_phone` ou une `home_phone` correspondance entre deux enregistrements, la touche de correspondance « Téléphone » renverra une correspondance. Pour la touche de correspondance « Téléphone » pour trouver une correspondance, `Record One mobile_phone = Record Two mobile_phone` OU `Record One mobile_phone = Record Two home_phone` OU `Record One home_phone = Record Two home_phone` OU`Record One home_phone = Record Two mobile_phone`.

Identifiant du match (MatchID)

Pour la correspondance basée sur des règles et la correspondance ML, il s'agit de l'ID généré Résolution des entités AWS et appliqué à chaque ensemble d'enregistrements appariés. Cela fait partie des métadonnées de flux de travail correspondantes qui seront incluses dans la sortie.

Clé de correspondance (MatchKey)

La touche Match indique les Résolution des entités AWS champs de saisie à considérer comme des données similaires et ceux à considérer comme des données différentes. Cela permet de configurer Résolution des entités AWS automatiquement des règles de correspondance basées sur des règles et de comparer des données similaires stockées dans différents champs de saisie.

S'il existe plusieurs types d'informations de numéro de téléphone, comme un `mobile_phone` champ de `home_phone` saisie et un champ de saisie dans vos données, vous pouvez leur attribuer la touche correspondante « Téléphone ». La correspondance basée sur des règles peut ensuite être configurée pour comparer les données à l'aide des instructions « ou » dans tous les champs de saisie avec la touche de correspondance « Téléphone » (voir les définitions de One-to-One correspondance et Many-to-Many de correspondance dans la section Matching Workflow).

Si vous souhaitez que la correspondance basée sur des règles prenne en compte les différents types d'informations de numéro de téléphone de manière complètement séparée, vous pouvez créer des clés de correspondance plus spécifiques, telles que « Mobile_Phone » et « Home_Phone ». Ensuite, lors de la configuration d'un flux de travail de correspondance, vous pouvez spécifier comment chaque touche de correspondance téléphonique sera utilisée dans le cadre de la correspondance basée sur des règles.

Si non MatchKey est spécifié pour un champ de saisie particulier, il ne peut pas être utilisé pour la mise en correspondance mais peut être effectué tout au long du processus de correspondance et peut être sorti si vous le souhaitez.

Nom de la clé de correspondance

Le nom attribué à une clé de correspondance.

Règle de correspondance (MatchRule)

Pour le rapprochement basé sur des règles, il s'agit du numéro de règle appliqué qui a généré un ensemble d'enregistrements correspondants. Cela fait partie des métadonnées de flux de travail correspondantes qui seront incluses dans la sortie.

Correspondance

Processus qui consiste à combiner et à comparer des données provenant de différents champs d'entrée, tables ou bases de données et à déterminer lesquelles de ces données sont similaires (ou « correspondent ») en fonction de certains critères de correspondance (par exemple, par le biais de règles ou de modèles de correspondance).

Flux de travail correspondant

Le processus que vous avez configuré pour spécifier les données d'entrée à associer et la manière dont la correspondance doit être effectuée.

Description du flux de travail correspondant

Description facultative du flux de travail correspondant que vous pouvez choisir de saisir. Les descriptions vous aident à différencier les flux de travail correspondants si vous en créez plusieurs.

Nom du flux de travail correspondant

Nom du flux de travail correspondant que vous spécifiez.

> **Note**
>
> Les noms de flux de travail correspondants doivent être uniques. Ils ne peuvent pas porter le même nom, sinon une erreur sera renvoyée.

Metadonnées de flux de travail correspondantes

Informations générées et sorties par Résolution des entités AWS lors d'une tâche de flux de travail correspondante. Ces informations sont requises en sortie.

Normalisation (ApplyNormalization)

Choisissez si vous souhaitez normaliser les données d'entrée telles que définies dans le schéma. La normalisation normalise les données en supprimant les espaces et les caractères spéciaux supplémentaires et en normalisant le format en minuscules.

Par exemple, si un champ de saisie est de `PHONE_NUMBER` type et que les valeurs de la table d'entrée sont mises en forme`(123) 456-7890`, les valeurs Résolution des entités AWS seront normalisées en`1234567890`.

Les sections suivantes décrivent nos règles de normalisation standard. Pour la correspondance basée sur le ML en particulier, voir. Normalisation (ApplyNormalization) — Basé uniquement sur le ML

Rubriques

Nom

- TRIM= Supprime les espaces blancs avant et arrière
- LOWERCASE= En minuscules tous les caractères alphabétiques
- CONVERT_ ACCENT = Convertir une lettre accentuée en lettre ordinaire
- REMOVE_ _ ALL NON _ ALPHA = Supprime tous les caractères non alphabétiques [A-za-Z]

E-mails

- TRIM= Supprime les espaces blancs avant et arrière
- LOWERCASE= En minuscules tous les caractères alphabétiques
- CONVERT_ ACCENT = Convertir une lettre accentuée en lettre ordinaire
- EMAIL_ _ ADDRESS UTIL _ NORM = Supprime tous les points (.) du nom d'utilisateur, supprime tout ce qui se trouve après un signe plus (+) dans le nom d'utilisateur et normalise les variations de domaine courantes
- REMOVE_ _ ALL _ NON EMAIL _ CHARS = Supprime tous les non-alpha-numeric caractères [A-za-Z0-9] et [.@-]

Téléphone

- TRIM= Supprime les espaces blancs avant et arrière
- REMOVE_ _ ALL NON _ NUMERIC = Supprime tous les caractères non numériques [0-9]
- REMOVE_ _ ALL LEADING _ ZEROES = Supprime tous les zéros en tête

- ENSURE_ PREFIX _ WITH _MAP, "phonePrefixMap" = Examine chaque numéro de téléphone et essaie de le comparer aux modèles du phonePrefixMap. Si une correspondance est trouvée, la règle ajoutera ou modifiera le préfixe du numéro de téléphone pour s'assurer qu'il est conforme au format standardisé spécifié sur la carte.

Address

- TRIM= Supprime les espaces blancs avant et arrière
- LOWERCASE= En minuscules tous les caractères alphabétiques
- CONVERT_ ACCENT = Convertir une lettre accentuée en lettre ordinaire
- REMOVE_ _ ALL NON _ ALPHA = Supprime tous les caractères non alphabétiques [A-za-Z]
- RENAME_ WORDS en utilisant ADDRESS _ RENAME _ WORD _ MAP = remplacer les mots de la chaîne d'adresse par des mots provenant de ADDRESS_ RENAME _ WORD _ MAP
- RENAME_ DELIMITERS en utilisant ADDRESS _ RENAME _ DELIMITER _ MAP = remplacer les délimiteurs dans la chaîne d'adresse par une chaîne de ADDRESS_ _ RENAME _ DELIMITER MAP
- RENAME_ DIRECTIONS en utilisant ADDRESS _ RENAME _ DIRECTION _ MAP = remplacer les délimiteurs dans la chaîne d'adresse par une chaîne de ADDRESS_ _ RENAME _ DIRECTION MAP
- RENAME_ NUMBERS en utilisant ADDRESS _ RENAME _ NUMBER _ MAP = remplacez les nombres dans la chaîne d'adresse par une chaîne de ADDRESS_ RENAME _ NUMBER _ MAP
- RENAME_ SPECIAL _ CHARS en utilisant ADDRESS _ RENAME _ SPECIAL _ CHAR _ MAP = remplacez les caractères spéciaux de la chaîne d'adresse par une chaîne de ADDRESS_ RENAME _ SPECIAL _ CHAR _ MAP

ADDRESS_RENAME_WORD_MAP

Ce sont les mots qui seront renommés lors de la normalisation de la chaîne d'adresse.

```
"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

Ce sont les délimiteurs qui seront renommés lors de la normalisation de la chaîne d'adresse.

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

ADDRESS_RENAME_DIRECTION_MAP

Il s'agit des identificateurs de direction qui seront renommés lors de la normalisation de la chaîne d'adresse.

```
"east": "e",
```

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

ADDRESS_RENAME_NUMBER_MAP

Il s'agit des chaînes numériques qui seront renommées lors de la normalisation de la chaîne d'adresse.

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

ADDRESS_RENAME_SPECIAL_CHAR_MAP

Il s'agit de la chaîne de caractères spéciaux qui sera renommée lors de la normalisation de la chaîne d'adresse.

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

Haché

- TRIM= Supprime les espaces blancs avant et arrière

Identifiant de la source

- TRIM= Supprime les espaces blancs avant et arrière

Normalisation (ApplyNormalization) — Basé uniquement sur le ML

Choisissez si vous souhaitez normaliser les données d'entrée telles que définies dans le schéma. La normalisation normalise les données en supprimant les espaces et les caractères spéciaux supplémentaires et en normalisant le format en minuscules.

Par exemple, si un champ de saisie est de `NAME` type et que les valeurs de la table d'entrée sont mises en forme`Johns Smith`, les valeurs Résolution des entités AWS seront normalisées en`john smith`.

Les sections suivantes décrivent les règles de normalisation pour les flux de travail de correspondance basés sur le machine learning.

Rubriques

- Nom
- E-mails
- Téléphone

Nom

- TRIM= Supprime les espaces blancs avant et arrière
- LOWERCASE= Tous les caractères alphabétiques en minuscules

E-mails

- LOWERCASE= Tous les caractères alphabétiques en minuscules
- Remplace uniquement (at) (sensible aux majuscules et minuscules) par le symbole @
- Supprime tous les espaces blancs, n'importe où dans la valeur
- Supprime tout ce qui se trouve en dehors du premier "< >" s'il existe

Téléphone

- TRIM= Supprime les espaces blancs avant et arrière
- REMOVE_ _ ALL NON _ NUMERIC = Supprime tous les caractères non numériques [0-9]

- REMOVE_ _ ALL LEADING _ ZEROES = Supprime tous les zéros en tête
- ENSURE_ PREFIX _ WITH _MAP, "phonePrefixMap" = Examine chaque numéro de téléphone et essaie de le comparer aux modèles du phonePrefixMap. Si une correspondance est trouvée, la règle ajoutera ou modifiera le préfixe du numéro de téléphone pour s'assurer qu'il est conforme au format standardisé spécifié sur la carte.

One-to-One appariement

One-to-one le matching compare des instances uniques de données similaires. Les champs de saisie ayant la même clé de correspondance et les mêmes valeurs dans le même champ de saisie seront comparés les uns aux autres.

Par exemple, vous pouvez avoir plusieurs champs de saisie de numéros de téléphone, tels `home_phone` que `mobile_phone` et qui ont la même touche de correspondance « Téléphone ». Utilisez le one-to-one rapprochement pour comparer les données du champ de `mobile_phone` saisie avec les données du champ de `mobile_phone` saisie et pour comparer les données du champ de `home_phone` saisie avec les données du champ de `home_phone` saisie. Les données du champ de `mobile_phone` saisie ne seront pas comparées aux données du champ de `home_phone` saisie.

Les règles de correspondance évaluent les données de plusieurs champs de saisie avec la même clé de correspondance à l'aide d'une opération (ou), et le one-to-many rapprochement compare les valeurs d'un seul champ de saisie. Cela signifie que si `mobile_phone` ou `home_phone` correspond entre deux enregistrements, la touche de correspondance « Téléphone » renverra une correspondance. Pour la touche de correspondance « Téléphone » pour trouver une correspondance, `Record One mobile_phone = Record Two mobile_phone` OU`Record One home_phone = Record Two home_phone`.

Les règles de correspondance évaluent les données dans les champs de saisie dotés de différentes clés de correspondance avec une opération (et). Si vous souhaitez que la correspondance basée sur des règles prenne en compte les différents types d'informations de numéro de téléphone de manière complètement séparée, vous pouvez créer des clés de correspondance plus spécifiques, telles que « mobile_phone » et « home_phone ». Si vous souhaitez utiliser les deux touches de correspondance dans une règle pour trouver des correspondances, `Record One mobile_phone = Record Two mobile_phone` AND`Record One home_phone = Record Two home_phone`.

Sortie

Une liste d'OutputAttributeobjets, dont chacun comporte les champs Name et Hashed. Chacun de ces objets représente une colonne à inclure dans la table AWS Glue de sortie et indique si vous souhaitez que les valeurs de la colonne soient hachées.

Sorties 3 voies

Destination S3 vers laquelle Résolution des entités AWS sera écrite la table de sortie.

OutputSourceConfig

Une liste d' OutputSource objets, dont chacun possède les champs Outputs3Path et Output. ApplyNormalization

Correspondance basée sur les services des fournisseurs

Le jumelage basé sur les services des fournisseurs est un processus conçu pour associer, relier et améliorer vos dossiers avec les fournisseurs de services de données préférés et les ensembles de données sous licence. Vous devez avoir souscrit un abonnement AWS Data Exchange auprès du service du fournisseur pour utiliser cette technique de mise en correspondance.

Résolution des entités AWS s'intègre actuellement aux fournisseurs de services de données suivants :

- LiveRamp
- TransUnion
- UID2,0

Correspondance basée sur des règles

La correspondance basée sur des règles est un processus conçu pour trouver des correspondances exactes. La correspondance basée sur des règles est un ensemble hiérarchique de règles de correspondance en cascade, suggérées par Résolution des entités AWS, sur la base des données que vous saisissez et entièrement configurables par vos soins. Toutes les clés de correspondance

fournies dans les critères des règles doivent correspondre exactement pour que les données comparées soient déclarées concordantes et pour que les métadonnées associées soient sorties. La correspondance basée sur des règles renvoie un identifiant de correspondance et un numéro de règle pour chaque ensemble de données correspondant.

Nous recommandons de définir des règles permettant d'identifier une entité de manière unique. Classez vos règles pour trouver d'abord des correspondances plus précises.

Supposons, par exemple, que vous ayez deux règles, la règle 1 et la règle 2.

Ces règles comportent les clés de correspondance suivantes :

- La règle 1 inclut le nom complet et l'adresse
- La règle 2 inclut le nom complet, l'adresse et le téléphone

Comme la Règle 1 s'exécute en premier, aucune correspondance ne sera trouvée par la Règle 2 car elles auraient toutes été trouvées selon la Règle 1.

Pour trouver des correspondances différenciées par téléphone, réorganisez les règles comme suit :

- La règle 2 inclut le nom complet, l'adresse et le téléphone
- La règle 1 inclut le nom complet et l'adresse

Schema

Terme utilisé pour désigner une structure ou une mise en page définissant la manière dont un ensemble de données est organisé et connecté.

Description du schéma

Description facultative du schéma que vous pouvez choisir de saisir. Les descriptions vous aident à différencier les mappages de schéma si vous en créez plusieurs.

Nom du schéma

Nom du schéma.

> **Note**
>
> Les noms de schéma doivent être uniques. Ils ne peuvent pas porter le même nom, sinon une erreur sera renvoyée.

Cartographie du schéma

Le mappage du schéma Résolution des entités AWS est le processus par lequel vous indiquez Résolution des entités AWS comment interpréter vos données à des fins de correspondance. Vous définissez le schéma de la table de données d'entrée que vous Résolution des entités AWS souhaitez lire dans un flux de travail correspondant.

Cartographie du schéma ARN

Le nom de ressource Amazon (ARN) généré pour le mappage du schéma.

Identifiant unique

Identifiant unique que vous désignez et qui doit être attribué à chaque ligne de données d'entrée Résolution des entités AWS lue.

Example

Par exemple : **`Primary_key`**, **`Row_ID`** ou **`Record_ID`**.

La colonne Unique ID est obligatoire.

L'identifiant unique doit être un identifiant unique au sein d'une même table.

Dans différentes tables, l'identifiant unique peut comporter des valeurs dupliquées.

Lorsque le flux de travail correspondant est exécuté, l'enregistrement est rejeté si l'ID unique :

- n'est pas spécifié
- n'est pas unique au sein d'une même table
- chevauchements en termes de nom d'attribut entre les sources.
- dépasse 38 caractères (flux de travail de correspondance basés sur des règles uniquement)

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.