Guide de l’utilisateur

AWS Clean Rooms

AWS Clean Rooms: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS Clean Rooms ?

AWS Clean Rooms vous permet, à vous et à vos partenaires, d'analyser et de collaborer sur vos ensembles de données collectifs afin d'obtenir de nouvelles informations sans révéler les données sous-jacentes les uns aux autres. Vous pouvez utiliser AWS Clean Rooms un espace de travail collaboratif sécurisé pour créer vos propres salles blanches en quelques minutes et commencer à analyser vos ensembles de données collectifs en quelques étapes seulement. Vous pouvez choisir les partenaires avec lesquels vous souhaitez collaborer, sélectionner leurs ensembles de données et configurer des restrictions pour les participants.

Avec AWS Clean Rooms, vous pouvez collaborer avec des milliers d'entreprises qui l'utilisent déjà AWS. La collaboration ne nécessite pas de déplacer des données AWS ou de les charger sur une autre plateforme. Lorsque vous exécutez des requêtes, lisez AWS Clean Rooms les données depuis leur emplacement d'origine et appliquez des règles d'analyse intégrées pour vous aider à garder le contrôle sur leurs données.

AWS Clean Rooms fournit des contrôles d'accès aux données intégrés et des contrôles d'assistance à l'audit que vous pouvez configurer. Ces contrôles incluent :

- Règles d'analyse pour restreindre les SQL requêtes et fournir des contraintes de sortie
- Informatique cryptographique Clean Rooms pour garder les données cryptées, même pendant le traitement des requêtes, afin de se conformer aux politiques strictes de traitement des données
- Journaux de requêtes pour examiner les requêtes et faciliter les audits
- Confidentialité différentielle pour protéger contre les tentatives d'identification des utilisateurs. AWS Clean Rooms La confidentialité différentielle est une fonctionnalité entièrement gérée qui protège la confidentialité de vos utilisateurs grâce à des techniques mathématiques et à des commandes intuitives que vous pouvez appliquer en quelques clics.
- AWS Clean Rooms ML pour permettre à deux parties d'identifier des utilisateurs similaires dans leurs données sans avoir à partager leurs données entre elles. La première partie crée et configure un modèle similaire à partir de ses données d'entraînement. Les données de départ sont ensuite transmises à la collaboration afin de créer un segment similaire aux données d'entraînement.

La vidéo suivante explique plus en détail AWS Clean Rooms.

AWS Clean Rooms

Utilisez-vous pour la première fois AWS Clean Rooms ?

Si vous utilisez pour la première fois AWS Clean Rooms, nous vous recommandons de commencer par lire les sections suivantes :

- Comment AWS Clean Rooms fonctionne
- Accès AWS Clean Rooms
- Con AWS Clean Rooms figuration
- AWS Clean Rooms Glossaire

Comment AWS Clean Rooms fonctionne

Dans AWS Clean Rooms, vous créez une collaboration et ajoutez celle que Comptes AWS vous souhaitez inviter, ou vous rejoignez une collaboration à laquelle vous êtes invité en créant un abonnement. Vous liez ensuite les ressources de données nécessaires à votre cas d'utilisation : tables configurées pour les données d'événements, modèles configurés pour la modélisation ML ou espaces de noms d'identification pour la résolution d'entités. Vous avez la possibilité de créer ou d'approuver des modèles d'analyse afin de convenir à l'avance des requêtes exactes que vous souhaitez autoriser dans le cadre d'une collaboration. Enfin, vous analysez les données conjointes en exécutant des SQL requêtes sur les tables configurées, en effectuant la résolution des entités dans les tables de mappage d'identité ou en utilisant la modélisation ML pour générer des segments d'audience similaires.

Le schéma suivant explique comment AWS Clean Rooms cela fonctionne.

Services connexes

Les éléments suivants AWS services sont liés à AWS Clean Rooms :

- Amazon S3

  Les membres de la collaboration peuvent stocker les données qu'ils AWS Clean Rooms introduisent dans Amazon S3.

  Pour plus d'informations, consultez les rubriques suivantes :

  Préparation des tables de données pour les requêtes dans AWS Clean Rooms

Qu'est-ce qu'Amazon S3 ? dans le guide de l'utilisateur d'Amazon Simple Storage Service

- AWS Glue

  Les membres de la collaboration peuvent créer AWS Glue des tables à partir de leurs données dans Amazon S3 pour les utiliser dans AWS Clean Rooms.

  Pour plus d'informations, consultez les rubriques suivantes :

  Préparation des tables de données pour les requêtes dans AWS Clean Rooms

  Qu'est-ce que AWS Glue ?dans le Guide du développeur AWS Glue

- AWS CloudFormation

  Créez les ressources suivantes dans AWS CloudFormation : collaborations, tables configurées, associations de tables configurées et adhésions

  Pour de plus amples informations, veuillez consulter Création de AWS Clean Rooms ressources avec AWS CloudFormation.

- AWS CloudTrail

  AWS Clean Rooms Utilisez-le avec CloudTrail les journaux pour améliorer votre analyse de AWS service l'activité.

  Pour de plus amples informations, veuillez consulter Journalisation des appels d'API AWS Clean Rooms avec AWS CloudTrail.

- Résolution des entités AWS

  Utilisez AWS Clean Rooms avec Résolution des entités AWS pour effectuer la résolution d'entités.

  Pour de plus amples informations, veuillez consulter Travailler avec Résolution des entités AWS in AWS Clean Rooms.

Accès AWS Clean Rooms

Vous pouvez y accéder AWS Clean Rooms via les options suivantes :

- Directement via la AWS Clean Rooms console à l'adresse https://console.aws.amazon.com/cleanrooms/.

- Programmatiquement par le biais du. AWS Clean Rooms API Pour plus d'informations, consultez la AWS Clean Rooms APIréférence.

Tarification pour AWS Clean Rooms

Pour de plus amples informations sur la tarification, veuillez consulter AWS Clean Rooms Pricing (français non garanti).

Facturation pour AWS Clean Rooms

AWS Clean Rooms donne au créateur de la collaboration la possibilité de configurer quel membre paie les coûts de calcul des requêtes dans le cadre de la collaboration.

Dans la plupart des cas, le membre autorisé à effectuer une requête et le membre payant les frais de calcul des requêtes sont les mêmes. Toutefois, si le membre autorisé à effectuer des requêtes et le membre payant les frais de calcul des requêtes sont différents, alors, lorsque le membre habilité à effectuer des requêtes exécute des requêtes sur sa propre ressource d'adhésion, la ressource d'adhésion du membre payant les coûts de calcul des requêtes est facturée.

Le membre qui paie les frais de calcul des requêtes ne voit aucun événement lié aux requêtes exécutées dans son historique des CloudTrail événements, car le payeur n'est ni celui qui exécute les requêtes ni le propriétaire de la ressource sur laquelle les requêtes sont exécutées. Cependant, le payeur voit les factures générées sur sa ressource d'adhésion pour toutes les requêtes exécutées par le membre qui peut exécuter des requêtes dans le cadre de la collaboration.

Pour plus d'informations sur la façon de créer une collaboration et de configurer le membre payant les coûts de calcul des requêtes, consultezCréation d'une collaboration.

Règles d'analyse dans AWS Clean Rooms

Dans le cadre de l'activation d'une table à des AWS Clean Rooms fins d'analyse de collaboration, le membre de la collaboration doit configurer une règle d'analyse.

Une règle d'analyse est un contrôle renforçant la confidentialité que chaque propriétaire de données met en place sur une table configurée. Une règle d'analyse détermine la manière dont la table configurée peut être analysée.

La règle d'analyse est un contrôle au niveau du compte sur la table configurée (une ressource au niveau du compte) et est appliquée dans toute collaboration où la table configurée est associée. Si aucune règle d'analyse n'est configurée, la table configurée peut être associée à des collaborations, mais elle ne peut pas être interrogée. Les requêtes peuvent uniquement faire référence à des tables configurées avec le même type de règle d'analyse.

Pour configurer une règle d'analyse, vous devez d'abord sélectionner un type d'analyse, puis spécifier la règle d'analyse. Pour les deux étapes, vous devez prendre en compte le cas d'utilisation que vous souhaitez activer et la manière dont vous souhaitez protéger vos données sous-jacentes.

AWS Clean Rooms applique les contrôles les plus restrictifs à toutes les tables configurées référencées dans une requête.

Les exemples suivants illustrent les contrôles restrictifs.

Example Contrôle restrictif : contrainte de sortie

- Le collaborateur A a une contrainte de sortie sur la colonne d'identificateur de 100.
- Le collaborateur B a une contrainte de sortie sur la colonne d'identificateur de 150.

  Une requête d'agrégation qui fait référence aux deux tables configurées nécessite au moins 150 valeurs distinctes d'identifier dans une ligne de sortie pour qu'elle soit affichée dans la sortie de la requête. Le résultat de la requête n'indique pas que les résultats sont supprimés en raison de la contrainte de sortie.

Example Contrôle restrictif : modèle d'analyse non approuvé

- Le collaborateur A a autorisé un modèle d'analyse avec une requête qui fait référence aux tables configurées du collaborateur A et du collaborateur B dans leur règle d'analyse personnalisée.

- Le collaborateur B n'a pas autorisé le modèle d'analyse.

  Le collaborateur B n'ayant pas autorisé le modèle d'analyse, le membre autorisé à effectuer une requête ne peut pas exécuter ce modèle d'analyse.

Types de règles d'analyse

Il existe trois types de règles d'analyse : les règles d'agrégation, les règles de liste et les règles personnalisées. Les tableaux suivants comparent les types de règles d'analyse. Chaque type comporte une section distincte qui décrit la spécification de la règle d'analyse.

> **Note**
>
> Il existe un type de règle d'analyse appelé règle d'analyse de table de mappage d'identifiants. Cependant, cette règle d'analyse est gérée par AWS Clean Rooms et ne peut pas être modifiée. Pour de plus amples informations, veuillez consulter Règle d'analyse des tables de mappage d'identifiants.

Les sections suivantes décrivent les cas d'utilisation et les contrôles pris en charge pour chaque type de règle d'analyse.

Cas d'utilisation pris en charge

Les tableaux suivants présentent un résumé comparatif des cas d'utilisation pris en charge pour chaque type de règle d'analyse.

Cas d'utilisation	Agrégation	List	Personnalisé
Analyses prises en charge	Requêtes qui regroupent des statistiques à l'aide de COUNTSUM, et des AVG fonctions selon des dimensions facultatives	Requêtes qui produisent des listes au niveau des lignes indiquant le chevauchement entre plusieurs tables	Toute analyse personnalisée, à condition que le modèle d'analyse ou le créateur de l'analyse aient été revus et autorisés

Cas d'utilisation	Agrégation	List	Personnalisé
Cas d'utilisation courants	Analyse des segments, mesure, attribution	Enrichissement, création de segments	Attribution directe, analyses incrémentielles, découverte de l'audience
SQLconstruit	• JOINdéclarations : INNER JOIN • Fonctions d'agrégation : COUNTSUM/ COUNTDIST INCTSUMDI STINCT,/et AVG • Fonctions scalaires : sous-ensemble limité	• JOINdéclarations : INNER JOIN • Fonctions scalaires : Aucune	La majorité des SQL fonctions et SQL des constructions disponibles avec la commande SELECT
Sous-requêtes et expressions de table communes () CTEs	Non	Non	Oui
Modèles d'analyse	Non	Non	Oui

Contrôles pris en charge

Les tableaux suivants présentent un résumé comparatif de la manière dont chaque type de règle d'analyse protège vos données sous-jacentes.

Contrôle	Agrégation	List	Personnalisé
Mécanisme de commande	Contrôler la manière dont les données de la table peuvent être utilisées dans une requête	Contrôler la manière dont les données de la table peuvent être utilisées dans une requête	Contrôler les requêtes autorisées à s'exécuter sur la table (Par exemple, autorisez uniquemen

Contrôle	Agrégation	List	Personnalisé
	(Par exemple, allow COUNT et SUM de la colonne hashed_email.)	(Par exemple, autorisez l'utilisation de la colonne hashed_email uniquement pour la jointure.)	t les requêtes définies dans les modèles d'analyse « Requête personnalisée 1 ».)
Techniques intégrées d'amélioration de la confidentialité	• Match à l'aveugle • Agrégation requise • Seuil d'agrégation minimum >= • 2 Structure de requête prédéfinie	• Match à l'aveugle • Chevauchement requis • Structure de requête prédéfinie • Analyses supplémentaires autorisées	• Confidentialité différentielle • Colonnes de sortie non autorisées
Vérifiez la requête avant qu'elle ne puisse être exécutée	Non	Non	Oui, en utilisant des modèles d'analyse

Pour plus d'informations sur les règles d'analyse disponibles dans AWS Clean Rooms, consultez les rubriques suivantes.

- Règle d'analyse d'agrégation
- Règle d'analyse des listes
- Règle d'analyse personnalisée dans AWS Clean Rooms

Règle d'analyse d'agrégation

DansAWS Clean Rooms, une règle d'analyse d'agrégation génère des statistiques agrégées à l'aide des fonctions COUNT, SUM et/ou AVG avec des dimensions facultatives. Lorsque la règle d'analyse d'agrégation est ajoutée à une table configurée, elle permet au membre habilité à effectuer des requêtes sur la table configurée.

La règle d'analyse d'agrégation prend en charge les cas d'utilisation tels que la planification de campagnes, la portée médiatique, la mesure de fréquence et l'attribution.

La structure et la syntaxe de requête prises en charge sont définies dansStructure et syntaxe des requêtes d'agrégation.

Les paramètres de la règle d'analyse, définis dansRègle d'analyse d'agrégation : contrôles des requêtes, incluent les contrôles de requête et les contrôles de résultats de requête. Ses contrôles de requête incluent la possibilité d'exiger qu'une table configurée soit jointe à au moins une table configurée appartenant au membre qui peut effectuer une requête, directement ou de manière transitive. Cette exigence vous permet de vous assurer que la requête est exécutée à l'intersection (INNERJOIN) de votre table et de la leur.

Structure et syntaxe des requêtes d'agrégation

Les requêtes sur les tables dotées d'une règle d'analyse d'agrégation doivent respecter la syntaxe suivante.

```
    --select_aggregate_function_expression
SELECT
aggregation_function(column_name) [[AS] column_alias ] [, ...]

    --select_grouping_column_expression
  [, {column_name|scalar_function(arguments)} [[AS] column_alias ]][, ...]

--table_expression
FROM table_name [[AS] table_alias ]
  [[INNER] JOIN table_name [[AS] table_alias] ON join_condition] [...]

--where_expression
[WHERE where_condition]

--group_by_expression
[GROUP BY {column_name|scalar_function(arguments)}, ...]]

--having_expression
[HAVING having_condition]

--order_by_expression
[ORDER BY {column_name|scalar_function(arguments)} [{ASC|DESC}]] [,...]]
```

Le tableau suivant explique chaque expression répertoriée dans la syntaxe précédente.

Expression	Définition	Exemples
select_aggregate_function_expression	Une liste séparée par des virgules contenant les expressions suivantes : • select_aggregation_function_expression • select_aggregate_expression **Note** Il doit y en avoir au moins un select_aggregation_function_expression dans leselect_aggregate_expression .	SELECT SUM(PRICE), user_segment
select_aggregation_function_expression	Une ou plusieurs fonctions d'agrégation prises en charge sont appliquées à une ou plusieurs colonnes. Seules les colonnes sont autorisées comme arguments des fonctions d'agrégation.	AVG(PRICE) COUNT(DISTINCT user_id)

Expression	Définition	Exemples
	Note Il doit y en avoir au moins un `select_aggregation_function_expression` dans le`select_aggregate_expression` .	

Expression	Définition	Exemples

select_grouping_column_expression	Expression qui peut contenir n'importe quelle expression utilisant les éléments suivants :
	• Nom des colonnes de la table
	• Fonctions scalaires prises en charge
	• Littéraux de chaîne
	• Littéraux numériques
	
	Note
	`select_aggregate_expression` peut créer un alias pour les colonnes avec ou sans le AS paramètre. Pour plus d'informations, consultez la référence AWS Clean Rooms SQL.
		`TRUNC(timestampColumn)`
		
		`UPPER(campaignName)`

Expression	Définition	Exemples
table_expression	Table, ou jointure de tables, reliant des expressions conditionnelles de jointure à`join_condition` . `join_condition` renvoie une valeur booléenne. Les `table_expression` supports : • Un JOIN type spécifique (INNERJOIN) • La condition de comparaison de l'égalité au sein d'un `join_condition` (=) • Opérateurs logiques (AND,OR).	`FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2`

Expression	Définition	Exemples

where_expression	Expression conditionnelle qui renvoie une valeur booléenne . Il peut être composé des éléments suivants :
	• Nom des colonnes de la table
	• Fonctions scalaires prises en charge
	• Operateurs mathématiques
	• Littéraux de chaîne
	• Littéraux numériques
	
	Les conditions de comparaison prises en charge sont (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Les opérateurs logiques pris en charge sont (`AND, OR`).
	
	`where_expression` C'est facultatif.
		`WHERE where_condition`
		
		`WHERE price > 100`
		
		`WHERE TRUNC(timestampColumn) = '1/1/2022'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

group_by_expression	Liste d'expressions séparées par des virgules qui répondent aux exigences du. `select_grouping_column_expression`	`GROUP BY TRUNC(timestampColumn), UPPER(campaignName), segment`

Expression	Définition	Exemples
having_expression	Expression conditionnelle qui renvoie une valeur booléenne . Ils disposent d'une fonction d'agrégation prise en charge appliquée à une seule colonne (par exemple,`SUM(price)`) et sont comparés à un littéral numérique. Les conditions prises en charge sont (`=, >, <, <=, >=, <>, !=`). Les opérateurs logiques pris en charge sont (`AND, OR`). `having_expression` C'est facultatif.	`HAVING SUM(SALES) > 500`

Expression	Définition	Exemples
order_by_expression	Liste d'expressions séparées par des virgules qui est compatible avec les mêmes exigences définies dans la section `select_aggregate_expression` définie précédemment. `order_by_expression` C'est facultatif. **Note** `order_by_expression` autorisations `ASC` et `DESC` paramètres. Pour plus d'informations, consultez la section Paramètres ASC DESC dans le manuel AWS Clean RoomsSQL Reference.	`ORDER BY SUM(SALES), UPPER(campaignName)`

En ce qui concerne la structure et la syntaxe des requêtes d'agrégation, tenez compte des points suivants :

- Les commandes SQL autres que ne SELECT sont pas prises en charge.
- Les sous-requêtes et les expressions de table communes (par exemple,WITH) ne sont pas prises en charge.
- Les opérateurs qui combinent plusieurs requêtes (par exemple,UNION) ne sont pas pris en charge.
- TOPLIMIT, et les OFFSET paramètres ne sont pas pris en charge.

Règle d'analyse d'agrégation : contrôles des requêtes

Grâce aux commandes de requête d'agrégation, vous pouvez contrôler la manière dont les colonnes de votre table sont utilisées pour interroger la table. Par exemple, vous pouvez contrôler quelle colonne est utilisée pour la jointure, quelle colonne peut être comptée ou quelle colonne peut être utilisée dans WHERE les instructions.

Les sections suivantes expliquent chaque contrôle.

Rubriques

Contrôles d'agrégation

À l'aide des contrôles d'agrégation, vous pouvez définir les fonctions d'agrégation à autoriser et les colonnes auxquelles elles doivent être appliquées. Les fonctions d'agrégation peuvent être utilisées dans les ORDER BY expressions SELECTHAVING, et.

Contrôle	Définition	Utilisation
`aggregateColumns`	Colonnes de colonnes de table configurées que vous autorisez à utiliser dans les fonctions d'agrégation.	`aggregateColumns` peut être utilisé dans une fonction d'agrégation dans les ORDER BY expressions SELECTHAV ING,, et. Certains `aggregate Columns` peuvent également être classés dans la catégorie « A » `joinColumn` (définis ultérieurement). Given ne `aggregate Column` peut pas également

Contrôle	Définition	Utilisation
		être classé dans la catégorie `dimensionColumn` (défini ultérieurement).
`function`	Les fonctions COUNT, SUM et AVG que vous autorisez à utiliser en plus de`aggregate Columns` .	`function`peut être appliqué à un `aggregateColumns` objet qui lui est associé.

Commandes de jointure

Une `JOIN` clause est utilisée pour combiner les lignes de deux tables ou plus, sur la base d'une colonne associée entre elles.

Vous pouvez utiliser les commandes de jointure pour contrôler la manière dont votre table peut être jointe aux autres tables d`utable_expression`. AWS Clean Roomsuniquement des supports INNERJOIN. INNERJOINles instructions ne peuvent utiliser que des colonnes explicitement classées comme telles `joinColumn` dans votre règle d'analyse, sous réserve des contrôles que vous définissez.

Ils INNER JOIN doivent opérer à `joinColumn` partir d'une table configurée et `joinColumn` à partir d'une autre table configurée dans la collaboration. C'est vous qui décidez quelles colonnes de votre tableau peuvent être utilisées`joinColumn`.

Chaque condition de correspondance contenue dans la ON clause est requise pour utiliser la condition de comparaison d'égalité (=) entre deux colonnes.

Plusieurs conditions de correspondance au sein d'une même ON clause peuvent être les suivantes :

- Combiné à l'aide de l'opérateur `AND` logique
- Séparé à l'aide de l'opérateur `OR` logique

> **Note**
>
> Toutes les JOIN conditions de match doivent correspondre à une ligne de chaque côté duJOIN. Toutes les conditions connectées par un opérateur OR ou un opérateur AND logique doivent également respecter cette exigence.

Voici un exemple de requête avec un opérateur AND logique.

```
SELECT some_col, other_col
FROM table1
    JOIN table2
    ON table1.id = table2.id AND table1.name = table2.name
```

Voici un exemple de requête avec un opérateur OR logique.

```
SELECT some_col, other_col
FROM table1
    JOIN table2
    ON table1.id = table2.id OR table1.name = table2.name
```

Contrôle	Définition	Utilisation
`joinColumns`	Les colonnes (le cas échéant) que vous souhaitez autoriser le membre autorisé à effectuer une requête à utiliser dans la INNER JOIN déclaration.	Un spécifique `joinColumn` peut également être classé dans la catégorie `aggregate Column` (voirContrôles d'agrégation). La même colonne ne peut pas être utilisée à la fois comme `joinColumn` et `dimension Columns` (voir plus loin). À moins qu'il n'ait également été classé comme `unaggregateColumn` , a ne `joinColumn` peut être

Contrôle	Définition	Utilisation
		utilisé dans aucune autre partie de la requête autre que le INNERJOIN.
`joinRequired`	Déterminez si vous avez besoin INNER JOIN d'une table configurée de la part du membre qui peut effectuer la requête.	Si vous activez ce paramètre , un INNER JOIN est requis. Si vous n'activez pas ce paramètre, un INNER JOIN est facultatif. En supposant que vous activiez ce paramètre, le membre autorisé à effectuer une requête doit inclure une table qu'il possède dans le INNERJOIN. Ils doivent joindre JOIN votre table à la leur, soit directement, soit de manière transitive (c'est-à-dire joindre leur table à une autre table, elle-même jointe à la vôtre).

Voici un exemple de transitivité.

```
ON
my_table.identifer = third_party_table.identifier
....
ON
third_party_table.identifier = member_who_can_query_table.id
```

> **Note**
>
> Le membre qui peut effectuer une requête peut également utiliser le `joinRequired` paramètre. Dans ce cas, la requête doit joindre sa table à au moins une autre table.

Contrôles dimensionnels

Les contrôles de dimension contrôlent la colonne le long de laquelle les colonnes d'agrégation peuvent être filtrées, groupées ou agrégées.

Contrôle	Définition	Utilisation
`dimensionColumns`	Les colonnes (le cas échéant) que vous autorisez le membre autorisé à effectuer une requête à utiliser dans SELECTWHERE, GROUPBY, et ORDERBY.	A `dimensionColumn` peut être utilisé dans SELECT (`select_grouping_column_expression`)WHERE, GROUPBY, et ORDERBY. La même colonne ne peut pas être à la fois a `dimensionColumn` `joinColumn` , a et/ou a`naggregateColumn` .

Fonctions scalaires

Les fonctions scalaires contrôlent les fonctions scalaires qui peuvent être utilisées sur les colonnes de dimension.

Contrôle	Définition	Utilisation
`scalarFunctions`	Les fonctions scalaires qui peuvent être utilisées `dimensionColumns` dans la requête.	Spécifie les fonctions scalaires (le cas échéant) auxquelles vous autorisez (par exempleCAST) l'`dimensionColumns` application. Les fonctions scalaires ne peuvent pas être utilisées par-dessus d'autres fonctions ou au sein d'autres fonctions. Les arguments des fonctions

Contrôle	Définition	Utilisation
		scalaires peuvent être des colonnes, des chaînes littérales ou des littéraux numériques.

Les fonctions scalaires suivantes sont prises en charge :

- Fonctions mathématiques : ABS, PLAFOND, PLANCHER, BOIS, LN, ROND, SQRT
- Fonctions de formatage des types de données — CAST, CONVERT, TO_CHAR, TO_DATE, TO_NUMBER, TO_TIMESTAMP
- Fonctions de chaîne : LOWER, UPPER, TRIM, RTRIM, SUBSTRING
  - Pour RTRIM, les jeux de caractères personnalisés à découper ne sont pas autorisés.
- Expressions conditionnelles — COALESCE
- Fonctions de date : EXTRACT, GETDATE, CURRENT_DATE, DATEADD
- Autres fonctions — TRUNC

Pour plus de détails, consultez la référence AWS Clean Rooms SQL.

Règle d'analyse d'agrégation : contrôles des résultats des requêtes

Avec les contrôles des résultats des requêtes d'agrégation, vous pouvez contrôler les résultats renvoyés en spécifiant une ou plusieurs conditions que chaque ligne de sortie doit remplir pour être renvoyée. AWS Clean Roomsprend en charge les contraintes d'agrégation sous la forme de`COUNT (DISTINCT column) >= X`. Ce formulaire exige que chaque ligne agrège au moins X valeurs distinctes d'un choix dans votre table configurée (par exemple, un nombre minimum de `user_id` valeurs distinctes). Ce seuil minimum est automatiquement appliqué, même si la requête soumise elle-même n'utilise pas la colonne spécifiée. Ils sont appliqués collectivement sur chaque table configurée dans la requête à partir des tables configurées de chaque membre de la collaboration.

Chaque table configurée doit comporter au moins une contrainte d'agrégation dans sa règle d'analyse. Les propriétaires de tables configurées peuvent en ajouter plusieurs `columnName` et `minimum` les associer, et elles sont appliquées collectivement.

Contraintes d'agrégation

Les contraintes d'agrégation contrôlent les lignes renvoyées dans les résultats de la requête. Pour être renvoyée, une ligne doit respecter le nombre minimum de valeurs distinctes spécifié dans chaque colonne spécifiée dans la contrainte d'agrégation. Cette exigence s'applique même si la colonne n'est pas explicitement mentionnée dans la requête ou dans d'autres parties de la règle d'analyse.

Contrôle	Définition	Utilisation
`columnName`	Le `aggregateColumn` qui est utilisé dans la condition que chaque ligne de sortie doit remplir.	Il peut s'agir de n'importe quelle colonne de la table configurée.
`minimum`	Le nombre minimum de valeurs distinctes associées `aggregateColumn` que la ligne de sortie doit avoir (par exemple, COUNT DISTINCT) pour qu'elle soit renvoyée dans les résultats de la requête.	La valeur `minimum` doit être au moins égale à 2.

Structure des règles d'analyse d'agrégation

L'exemple suivant montre une structure prédéfinie pour une règle d'analyse d'agrégation.

Dans l'exemple suivant, *`MyTable`*fait référence à votre table de données. Vous pouvez remplacer chaque *`espace réservé saisi par l'utilisateur`* par vos propres informations.

```
{
  "aggregateColumns": [
    {
      "columnNames": [MyTable column names], "function": [Allowed Agg Functions]
    },
  ],
  "joinRequired": ["QUERY_RUNNER"],
  "joinColumns": [MyTable column names],
```

```
  "dimensionColumns": [MyTable column names],
  "scalarFunctions": [Allowed Scalar functions],
  "outputConstraints": [
    {
      "columnName": [MyTable column names], "minimum": [Numeric value]
    },
  ]
}
```

Règle d'analyse d'agrégation - exemple

L'exemple suivant montre comment deux entreprises peuvent collaborer en AWS Clean Rooms utilisant l'analyse d'agrégation.

L'entreprise A possède des données sur les clients et les ventes. L'entreprise A souhaite comprendre l'activité de retour de produits. L'entreprise B est l'un des détaillants de l'entreprise A et possède des données sur les retours. L'entreprise B possède également des attributs de segment relatifs aux clients qui sont utiles à l'entreprise A (par exemple, achat de produits connexes, utilisation du service client du détaillant). L'entreprise B ne souhaite pas fournir de données de retour client au niveau des lignes ni d'informations sur les attributs. L'entreprise B souhaite uniquement activer un ensemble de requêtes pour que l'entreprise A obtienne des statistiques agrégées sur les clients qui se chevauchent à un seuil d'agrégation minimum.

L'entreprise A et l'entreprise B décident de collaborer afin que l'entreprise A puisse comprendre l'activité de retour des produits et fournir de meilleurs produits à l'entreprise B et à d'autres canaux.

Pour créer la collaboration et exécuter une analyse d'agrégation, les entreprises procèdent comme suit :

1. L'entreprise A crée une collaboration et crée une adhésion. La collaboration a la société B comme autre membre de la collaboration. L'entreprise A active la journalisation des requêtes dans la collaboration, et elle permet la journalisation des requêtes dans son compte.
2. L'entreprise B crée une adhésion à la collaboration. Il permet la journalisation des requêtes dans son compte.
3. La société A crée une table configurée pour les ventes.
4. La société A ajoute la règle d'analyse d'agrégation suivante au tableau des ventes configuré.

```
{
  "aggregateColumns": [
    {
```

```
      "columnNames": [
        "identifier"
      ],
      "function": "COUNT_DISTINCT"
    },
    {
      "columnNames": [
        "purchases"
      ],
      "function": "AVG"
    },
    {
      "columnNames": [
        "purchases"
      ],
      "function": "SUM"
    }
  ],
  "joinColumns": [
    "hashedemail"
  ],
  "dimensionColumns": [
    "demoseg",
    "purchasedate",
    "productline"
  ],
  "scalarFunctions": [
    "CAST",
    "COALESCE",
    "TRUNC"
  ],
  "outputConstraints": [
    {
      "columnName": "hashedemail",
      "minimum": 2,
      "type": "COUNT_DISTINCT"
    },
  ]
}
```

`aggregateColumns`— L'entreprise A souhaite compter le nombre de clients uniques entre les données de vente et les données de retours. L'entreprise A souhaite également additionner le nombre de `purchases` produits fabriqués pour le comparer au nombre de`returns`.

`joinColumns`— L'entreprise A souhaite utiliser pour faire correspondre `identifier` les clients à partir des données de vente aux clients à partir des données de retours. Cela aidera l'entreprise A à faire correspondre les retours aux bons achats. Cela aide également l'entreprise A à segmenter les clients qui se recoupent.

`dimensionColumns`— L'entreprise A filtre en `dimensionColumns` fonction du produit spécifique, compare les achats et les retours sur une certaine période, s'assure que la date de retour est postérieure à la date du produit et aide à segmenter les clients qui se recoupent.

`scalarFunctions`— L'entreprise A sélectionne une fonction `CAST` scalaire pour aider à mettre à jour les formats des types de données si nécessaire en fonction de la table configurée que l'entreprise A associe à la collaboration. Il ajoute également des fonctions scalaires pour aider à formater les colonnes si nécessaire.

`outputConstraints`— L'entreprise A définit des contraintes de sortie minimales. Il n'est pas nécessaire de restreindre les résultats car l'analyste est autorisé à voir les données au niveau des lignes depuis son tableau des ventes

> **Note**
>
> L'entreprise A n'est pas incluse `joinRequired` dans la règle d'analyse. Cela permet à leur analyste d'interroger seul le tableau des ventes.

5. La société B crée une table de retours configurée.
6. La société B ajoute la règle d'analyse d'agrégation suivante à la table des retours configurés.

```
{
  "aggregateColumns": [
    {
      "columnNames": [
        "identifier"
      ],
      "function": "COUNT_DISTINCT"
    },
    {
      "columnNames": [
        "returns"
      ],
      "function": "AVG"
```

```
    },
    {
      "columnNames": [
        "returns"
      ],
      "function": "SUM"
    }
  ],
  "joinColumns": [
    "hashedemail"
  ],
  "joinRequired": [
    "QUERY_RUNNER"
  ],
  "dimensionColumns": [
    "state",
    "popularpurchases",
    "customerserviceuser",
    "productline",
    "returndate"
  ],
  "scalarFunctions": [
    "CAST",
    "LOWER",
    "UPPER",
    "TRUNC"
  ],
  "outputConstraints": [
    {
      "columnName": "hashedemail",
      "minimum": 100,
      "type": "COUNT_DISTINCT"
    },
    {
      "columnName": "producttype",
      "minimum": 2,
      "type": "COUNT_DISTINCT"
    }
  ]
}
```

`aggregateColumns`— L'entreprise B permet à l'entreprise A de `returns` faire la somme pour comparer le nombre d'achats. Ils ont au moins une colonne d'agrégation car ils activent une requête d'agrégation.

`joinColumns`— L'entreprise B permet à l'entreprise A de se joindre à elle `identifier` pour faire correspondre les clients à partir des données de retour aux clients à partir des données de vente. `identifier`les données sont particulièrement sensibles et leur utilisation `joinColumn` garantit qu'elles ne seront jamais sorties dans une requête.

`joinRequired`— L'entreprise B exige que les requêtes sur les données de retour soient recoupées avec les données de vente. Ils ne veulent pas permettre à l'entreprise A d'interroger tous les individus de leur ensemble de données. Ils ont également convenu de cette restriction dans leur accord de collaboration.

`dimensionColumns`— L'entreprise B permet à l'entreprise A de filtrer et de regrouper par `statepopularpurchases`, et `customerserviceuser` qui sont des attributs uniques qui pourraient aider à effectuer l'analyse pour l'entreprise A. L'entreprise B permet à l'entreprise A d'utiliser `returndate` pour filtrer les résultats sur `returndate` ce qui se produit ensuite`purchasedate`. Grâce à ce filtrage, le résultat est plus précis pour évaluer l'impact du changement de produit.

`scalarFunctions`— La société B permet ce qui suit :

- TRUNC pour les dates
- INFÉRIEUR et SUPÉRIEUR au cas où ils `producttype` sont saisis dans un format différent dans leurs données
- CASTsi l'entreprise A doit convertir les types de données des ventes pour qu'ils soient identiques aux types de données des retours

La société A n'active pas d'autres fonctions scalaires car elle ne pense pas qu'elles soient nécessaires pour les requêtes.

`outputConstraints`— L'entreprise B impose des contraintes de production minimales `hashedemail` afin de réduire la capacité à réidentifier les clients. Cela ajoute également une contrainte de sortie minimale afin `producttype` de réduire la capacité de réidentifier les produits spécifiques qui ont été renvoyés. Certains types de produits peuvent être plus dominants en fonction des dimensions de la sortie (par exemple,`state`). Leurs contraintes de sortie seront

toujours appliquées, quelles que soient les contraintes de sortie ajoutées par l'entreprise A à ses données.

7. L'entreprise A crée une table de vente associée à la collaboration.
8. L'entreprise B crée une association de tables de retours à la collaboration.
9. L'entreprise A exécute des requêtes, comme dans l'exemple suivant, pour mieux comprendre le nombre de retours dans l'entreprise B par rapport au total des achats par site en 2022.

```
SELECT
  companyB.state,
  SUM(companyB.returns),
  COUNT(DISTINCT companyA.hashedemail)
FROM
  sales companyA
  INNER JOIN returns companyB ON companyA.identifier = companyB.identifier
WHERE
  companyA.purchasedate BETWEEN '2022-01-01' AND '2022-12-31' AND
  TRUNC(companyB.returndate) > companyA.purchasedate
GROUP BY
  companyB.state;
```

10. Les entreprises A et B examinent les journaux de requêtes. L'entreprise B vérifie que la requête est conforme à ce qui a été convenu dans l'accord de collaboration.

Résolution des problèmes liés aux règles d'analyse d'agrégation

Utilisez les informations présentées ici pour vous aider à diagnostiquer et à résoudre les problèmes courants liés à l'utilisation des règles d'analyse d'agrégation.

Problèmes

- Ma requête n'a renvoyé aucun résultat

Ma requête n'a renvoyé aucun résultat

Cela peut se produire lorsqu'aucun résultat ne correspond ou lorsque les résultats correspondants n'atteignent pas un ou plusieurs seuils d'agrégation minimaux.

Pour plus d'informations sur les seuils d'agrégation minimaux, consultezRègle d'analyse d'agrégation - exemple.

Règle d'analyse des listes

DansAWS Clean Rooms, une règle d'analyse de liste produit des listes au niveau des lignes indiquant le chevauchement entre la table configurée à laquelle elle est ajoutée et les tables configurées du membre qui peut effectuer la requête. Le membre habilité à effectuer des requêtes exécute des requêtes qui incluent une règle d'analyse de liste.

Le type de règle d'analyse de liste prend en charge les cas d'utilisation tels que l'enrichissement et la création d'audience.

Pour plus d'informations sur la structure de requête et la syntaxe prédéfinies pour cette règle d'analyse, consultezStructure prédéfinie des règles d'analyse des listes.

Les paramètres de la règle d'analyse de liste, définis dansRègle d'analyse des listes : contrôles des requêtes, comportent des contrôles de requête. Ses commandes de requête incluent la possibilité de sélectionner les colonnes qui peuvent être répertoriées dans la sortie. La requête doit comporter au moins une jointure avec une table configurée provenant du membre qui peut effectuer la requête, directement ou de manière transitive.

Il n'existe aucun contrôle des résultats de requête comme c'est le cas pour la règle d'analyse d'agrégation.

Les requêtes de liste ne peuvent utiliser que des opérateurs mathématiques. Ils ne peuvent pas utiliser d'autres fonctions (telles que l'agrégation ou le scalaire).

Rubriques

- Structure et syntaxe des requêtes de liste
- Règle d'analyse des listes : contrôles des requêtes
- Structure prédéfinie des règles d'analyse des listes
- Règle d'analyse des listes - exemple

Structure et syntaxe des requêtes de liste

Les requêtes sur les tables dotées d'une règle d'analyse de liste doivent respecter la syntaxe suivante.

```
--select_list_expression
```

```
SELECT
[TOP number ] DISTINCT column_name [[AS] column_alias ] [, ...]

--table_expression
FROM table_name [[AS] table_alias ]
  [[INNER] JOIN table_name [[AS] table_alias] ON join_condition] [...]

--where_expression
[WHERE where_condition]

--limit_expression
[LIMIT number]
```

Le tableau suivant explique chaque expression répertoriée dans la syntaxe précédente.

Expression	Définition	Exemples
select_list_expression	Liste séparée par des virgules contenant au moins un nom de colonne de table. Un DISTINCT paramètre est obligatoire. **Note** Ils select_list_expression peuvent aliaser les colonnes avec ou sans le AS paramètre. Il prend également en charge le TOP paramètre. Pour plus d'informations, consultez la référence AWS Clean Rooms SQL.	SELECT DISTINCT segment

Expression	Définition	Exemples
table_expression	Une table, ou une jointure de tables, `join_condition` à laquelle la connecter `join_condition` . `join_condition` renvoie une valeur booléenne. Les `table_expression` supports : • Un type de JOIN spécifique (INNERJOIN) • Les conditions de comparais on de l'égalité au sein d'un `join_condition` (=) • Opérateurs logiques (AND,OR).	`FROM consumer_table INNER JOIN provider_ table ON consumer_table.ide ntifier1 = provider_ table.identifier1 AND consumer_table .identifier2 = provider_table.ide ntifier2`

Expression	Définition	Exemples

where_expression	Expression conditionnelle qui renvoie une valeur booléenne . Il peut être composé des éléments suivants :
	• Nom des colonnes de la table
	• Operateurs mathématiques
	• Littéraux de chaîne
	• Littéraux numériques
	
	Les conditions de comparais on prises en charge sont (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Les opérateurs logiques pris en charge sont (`AND, OR`).
	
	`where_expression` C'est facultatif.
		`WHERE state + '_' + city = 'NY_NYC'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

limit_expression	Cette expression doit prendre un entier positif. Il peut également être échangé avec un paramètre TOP. `limit_expression` C'est facultatif.	`LIMIT 100`

En ce qui concerne la structure et la syntaxe des requêtes de liste, tenez compte des points suivants :

- Les commandes SQL autres que SELECT ne sont pas prises en charge.

- Les sous-requêtes et les expressions de table communes (par exemple,WITH) ne sont pas prises en charge
- Les BY clauses GROUP BY HAVING, et ORDER ne sont pas prises en charge
- Le paramètre OFFSET n'est pas pris en charge

Règle d'analyse des listes : contrôles des requêtes

Avec les commandes de requête de liste, vous pouvez contrôler la manière dont les colonnes de votre table sont utilisées pour interroger la table. Par exemple, vous pouvez contrôler quelle colonne est utilisée pour la jointure ou quelle colonne peut être utilisée dans l'instruction et la WHERE clause SELECT.

Les sections suivantes expliquent chaque contrôle.

Rubriques

- Commandes de jointure
- Contrôles de liste

Commandes de jointure

Avec les commandes Join, vous pouvez contrôler la manière dont votre table peut être jointe aux autres tables de la table_expression. AWS Clean Roomsne prend en charge que INNER JOIN. Dans la règle d'analyse de liste, au moins un INNER JOIN est requis et le membre qui peut effectuer une requête doit inclure une table qu'il possède dans le INNER JOIN. Cela signifie qu'ils doivent joindre votre table à la leur, directement ou de manière transitionnelle.

Voici un exemple de transitivité.

```
ON
my_table.identifer = third_party_table.identifier
....
ON
third_party_table.identifier = member_who_can_query_table.id
```

INNERLes instructions JOIN ne peuvent utiliser que des colonnes explicitement classées comme telles `joinColumn` dans votre règle d'analyse.

Le INNER JOIN doit fonctionner sur une table `joinColumn` à partir de votre table configurée et `joinColumn` à partir d'une autre table configurée dans la collaboration. Vous décidez quelles colonnes de votre tableau peuvent être utiliséesjoinColumn.

Chaque condition de correspondance contenue dans la ON clause est requise pour utiliser la condition de comparaison d'égalité (=) entre deux colonnes.

Plusieurs conditions de correspondance au sein d'une ON clause peuvent être les suivantes :

- Combiné à l'aide de l'opérateur AND logique
- Séparé à l'aide de l'opérateur OR logique

> **Note**
>
> Toutes les JOIN conditions de match doivent correspondre à une ligne de chaque côté duJOIN. Toutes les conditions connectées par un opérateur OR ou un opérateur AND logique doivent également respecter cette exigence.

Voici un exemple de requête avec un opérateur AND logique.

```
SELECT some_col, other_col
FROM table1
    JOIN table2
    ON table1.id = table2.id AND table1.name = table2.name
```

Voici un exemple de requête avec un opérateur OR logique.

```
SELECT some_col, other_col
FROM table1
    JOIN table2
    ON table1.id = table2.id OR table1.name = table2.name
```

Contrôle	Définition	Utilisation
`joinColumns`	Les colonnes que vous souhaitez autoriser le membre autorisé à effectuer une	La même colonne ne peut pas être classée à la fois comme a

Contrôle	Définition	Utilisation
	requête à utiliser dans l'instruction INNER JOIN.	`joinColumn` et `listColumn` (voir Contrôles de liste). `joinColumn` ne peut être utilisé dans aucune autre partie de la requête que INNER JOIN.

Contrôles de liste

Les contrôles de liste contrôlent les colonnes qui peuvent être répertoriées dans le résultat de la requête (c'est-à-dire utilisées dans l'instruction SELECT) ou utilisées pour filtrer les résultats (c'est-à-dire utilisées dans l'WHEREinstruction).

Contrôle	Définition	Utilisation
`listColumns`	Les colonnes que vous autorisez le membre qui peut effectuer une requête à utiliser dans le SELECT et WHERE	A `listColumn` peut être utilisé dans SELECT etWHERE. La même colonne ne peut pas être utilisée à la fois comme `listColumn` et`joinColumn` .

Structure prédéfinie des règles d'analyse des listes

L'exemple suivant inclut une structure prédéfinie qui montre comment exécuter une règle d'analyse de liste.

Dans l'exemple suivant, *`MyTable`*fait référence à votre table de données. Vous pouvez remplacer chaque *`espace réservé saisi par l'utilisateur`* par vos propres informations.

```
{
  "joinColumns": [MyTable column name(s)],
```

```
  "listColumns": [MyTable column name(s)],
}
```

Règle d'analyse des listes - exemple

L'exemple suivant montre comment deux entreprises peuvent collaborer en AWS Clean Rooms utilisant l'analyse de listes.

L'entreprise A dispose de données de gestion de la relation client (CRM). L'entreprise A souhaite obtenir des données sectorielles supplémentaires sur ses clients pour en savoir plus sur leurs clients et éventuellement utiliser des attributs comme données d'entrée dans d'autres analyses. L'entreprise B possède des données de segment composées d'attributs de segment uniques qu'elle a créés sur la base de ses données de première partie. L'entreprise B souhaite fournir les attributs de segment uniques à l'entreprise A uniquement pour les clients dont les données se chevauchent avec celles de l'entreprise A.

Les entreprises décident de collaborer afin que l'entreprise A puisse enrichir les données qui se chevauchent. L'entreprise A est le membre qui peut interroger, et l'entreprise B est le contributeur.

Pour créer une collaboration et exécuter une analyse de liste en collaboration, les entreprises procèdent comme suit :

1. L'entreprise A crée une collaboration et crée une adhésion. La collaboration a la société B comme autre membre de la collaboration. L'entreprise A active la journalisation des requêtes dans la collaboration, et elle active la journalisation des requêtes dans son compte.
2. L'entreprise B crée une adhésion à la collaboration. Il permet la journalisation des requêtes dans son compte.
3. L'entreprise A crée une table configurée pour le CRM
4. L'entreprise A ajoute la règle d'analyse à la table configurée par le client, comme indiqué dans l'exemple suivant.

```
{
  "joinColumns": [
    "identifier1",
    "identifier2"
  ],
  "listColumns": [
    "internalid",
```

```
    "segment1",
    "segment2",
    "customercategory"
  ]
}
```

`joinColumns`— L'entreprise A souhaite utiliser `hashedemail` et/ou `thirdpartyid` (obtenue auprès d'un fournisseur d'identité) associer des clients à partir de données CRM à des clients à partir de données de segment. Cela permettra de garantir que l'entreprise A associe des données enrichies aux bons clients. Ils disposent de deux JoinColumns pour potentiellement améliorer le taux de correspondance de l'analyse.

`listColumns`— L'entreprise A utilise `listColumns` pour obtenir des colonnes enrichies à côté d'une colonne `internalid` qu'elle utilise dans ses propres systèmes. Ils ajoutent `segment1` et limitent potentiellement l'enrichissement `customercategory` à des segments spécifiques en les utilisant dans des filtres. `segment2`

5. La société B crée une table configurée par segments.
6. L'entreprise B ajoute la règle d'analyse à la table des segments configurés.

```
{
  "joinColumns": [
    "identifier2"
  ],
  "listColumns": [
    "segment3",
    "segment4"
  ]
}
```

`joinColumns`— L'entreprise B permet à l'entreprise A de se joindre à elle pour `identifier2` faire correspondre les clients, qu'il s'agisse de données segmentées ou de données CRM. Les sociétés A et B ont travaillé avec le fournisseur d'identité pour `identifier2` déterminer laquelle correspondrait à cette collaboration. Ils n'en ont pas ajouté d'autres `joinColumns` parce qu'ils pensaient `identifier2` que c'était le taux de correspondance le plus élevé et le plus précis possible et qu'aucun autre identifiant n'était requis pour les requêtes.

`listColumns`— L'entreprise B permet à l'entreprise A d'enrichir ses données `segment3` et ses `segment4` attributs, qui sont des attributs uniques qu'elle a créés, collectés et sur lesquels elle s'est alignée (avec le client A) afin de participer à l'enrichissement des données. Ils souhaitent que

l'entreprise A obtienne ces segments pour le chevauchement au niveau des lignes, car il s'agit d'une collaboration d'enrichissement des données.

7. L'entreprise A crée une association de tables CRM pour la collaboration.
8. L'entreprise B crée une association de tables de segments pour la collaboration.
9. L'entreprise A exécute des requêtes, telles que la suivante, pour enrichir les données clients qui se recoupent.

```
SELECT companyA.internalid, companyB.segment3, companyB.segment4
INNER JOIN returns companyB
 ON companyA.identifier2 = companyB.identifier2
WHERE companyA.customercategory > 'xxx'
```

10. Les entreprises A et B examinent les journaux de requêtes. L'entreprise B vérifie que la requête est conforme à ce qui a été convenu dans l'accord de collaboration.

Règle d'analyse personnalisée dans AWS Clean Rooms

Dans AWS Clean Rooms, une règle d'analyse personnalisée est un nouveau type de règle d'analyse qui permet d'exécuter des requêtes personnalisées sur la table configurée. Les requêtes SQL personnalisées sont toujours limitées à la SELECT commande, mais elles peuvent utiliser davantage de constructions SQL que les requêtes d'agrégation et de liste (par exemple, les fonctions de fenêtre, OUTER JOIN, les CTE ou les sous-requêtes ; voir la référence AWS Clean Rooms SQL pour une liste complète). Les requêtes SQL personnalisées ne doivent pas nécessairement suivre une structure de requête telle que les requêtes d'agrégation et de liste.

La règle d'analyse personnalisée prend en charge des cas d'utilisation plus avancés que ceux qui peuvent être pris en charge par la règle d'agrégation et d'analyse de liste, tels que l'analyse d'attribution personnalisée, le benchmarking, l'analyse d'incrémentalité et la découverte d'audience. Cela s'ajoute à un surensemble des cas d'utilisation pris en charge par les règles d'agrégation et d'analyse de listes.

La règle d'analyse personnalisée prend également en charge la confidentialité différentielle. La confidentialité différentielle est un cadre mathématiquement rigoureux pour la protection de la confidentialité des données. Pour plus d'informations, consultez AWS Clean Rooms Confidentialité différentielle. Lorsque vous créez un modèle d'analyse, AWS Clean Rooms Differential Privacy vérifie le modèle pour déterminer s'il est compatible avec la structure de requête à usage général pour

AWS Clean Rooms Differential Privacy. Cette validation garantit que vous ne créez pas de modèle d'analyse non autorisé avec une table protégée par la confidentialité différentielle.

Pour configurer la règle d'analyse personnalisée, les propriétaires de données peuvent choisir d'autoriser l'exécution de requêtes personnalisées spécifiques, stockées dans des modèles d'analyse, sur leurs tables configurées. Les propriétaires de données examinent les modèles d'analyse avant de les ajouter au contrôle d'analyse autorisé dans la règle d'analyse personnalisée. Les modèles d'analyse sont disponibles et visibles uniquement dans la collaboration dans laquelle ils ont été créés (même si la table est associée à d'autres collaborations) et ne peuvent être exécutés que par le membre qui peut effectuer des requêtes dans cette collaboration.

Les membres peuvent également choisir d'autoriser d'autres membres (fournisseurs de requêtes) à créer des requêtes sans révision. Les membres ajoutent les comptes des fournisseurs de requêtes que les fournisseurs de requêtes autorisés contrôlent dans la règle d'analyse personnalisée. Si le fournisseur de requêtes est le membre habilité à effectuer des requêtes, il peut exécuter n'importe quelle requête directement sur la table configurée. Les fournisseurs de requêtes peuvent également créer des requêtes en créant des modèles d'analyse. Toutes les requêtes créées par les fournisseurs de requêtes sont automatiquement autorisées à s'exécuter sur la table dans toutes les collaborations dans lesquelles elles sont présentes et où la table est associée. Compte AWS

Les propriétaires de données peuvent uniquement autoriser les modèles d'analyse ou les comptes à créer des requêtes, et non les deux. Si le propriétaire des données le laisse vide, le membre autorisé à effectuer des requêtes ne peut pas exécuter de requêtes sur la table configurée.

Rubriques

- Structure prédéfinie des règles d'analyse personnalisées
- Exemple de règle d'analyse personnalisée
- Règle d'analyse personnalisée avec confidentialité différentielle

Structure prédéfinie des règles d'analyse personnalisées

L'exemple suivant inclut une structure prédéfinie qui vous montre comment exécuter une règle d'analyse personnalisée avec la confidentialité différentielle activée. La `userIdentifier` valeur est la colonne qui identifie de manière unique vos utilisateurs, telle que user_id. Lorsque la confidentialité différentielle est activée sur deux tables ou plus dans le cadre d'une collaboration AWS Clean Rooms , vous devez configurer la même colonne que la colonne d'identifiant utilisateur dans les deux règles d'analyse afin de maintenir une définition cohérente des utilisateurs entre les tables.

```
{
  "allowedAnalyses": ["ANY_QUERY"] | string[],
  "allowedAnalysisProviders": [],
  "differentialPrivacy": {
    "columns": [
      {
        "name": "userIdentifier"
      }
    ]
  }
}
```

Vous avez le choix entre les options suivantes :

- Ajoutez les ARN du modèle d'analyse au contrôle des analyses autorisées. Dans ce cas, le `allowedAnalysisProviders` contrôle n'est pas inclus.

  ```
  {
    allowedAnalyses: string[]
  }
  ```

- Ajoutez Compte AWS des identifiants de membre au `allowedAnalysisProviders` contrôle. Dans ce cas, vous ajoutez `ANY_QUERY` au `allowedAnalyses` contrôle.

  ```
  {
    allowedAnalyses: ["ANY_QUERY"],
    allowedAnalysisProviders: string[]
  }
  ```

Exemple de règle d'analyse personnalisée

L'exemple suivant montre comment deux entreprises peuvent collaborer à AWS Clean Rooms l'aide de la règle d'analyse personnalisée.

L'entreprise A possède des données sur les clients et les ventes. L'entreprise A souhaite comprendre l'augmentation des ventes d'une campagne publicitaire sur le site de l'entreprise B. L'entreprise B possède des données d'audience et des attributs de segment utiles à l'entreprise (par exemple, l'appareil utilisé pour visionner la publicité).

L'entreprise A souhaite exécuter une requête d'incrémentalité spécifique dans le cadre de la collaboration.

Pour créer une collaboration et exécuter une analyse personnalisée en collaboration, les entreprises procèdent comme suit :

1. L'entreprise A crée une collaboration et crée une adhésion. La collaboration a la société B comme autre membre de la collaboration. L'entreprise A active la journalisation des requêtes dans la collaboration, et elle active la journalisation des requêtes dans son compte.
2. L'entreprise B crée une adhésion à la collaboration. Il permet la journalisation des requêtes dans son compte.
3. L'entreprise A crée une table configurée pour le CRM
4. La société A ajoute une règle d'analyse personnalisée vide à la table configurée des ventes.
5. L'entreprise A associe la table configurée des ventes à la collaboration.
6. La société B crée une table configurée pour le nombre de vues.
7. La société B ajoute une règle d'analyse personnalisée vide à la table configurée par le nombre de vues.
8. La société B associe la table configurée en termes de nombre de vues à la collaboration.
9. L'entreprise A consulte le tableau des ventes et le tableau d'audience associés à la collaboration et crée un modèle d'analyse, en ajoutant la requête d'incrémentalité et le paramètre pour le mois de la campagne.

```
{
    "analysisParameters": [
    {
        "defaultValue": ""
        "type": "DATE"
        "name": "campaign_month"
    }
    ],
    "description": "Monthly incrementality query using sales and viewership data"
    "format": "SQL"
    "name": "Incrementality analysis"
    "source":
        "WITH labeleddata AS
        (
        SELECT hashedemail, deviceid, purchases, unitprice, purchasedate,
        CASE
```

```
            WHEN testvalue IN ('value1', 'value2', 'value3') THEN 0
            ELSE 1
        END AS testgroup
        FROM viewershipdata
        )
        SELECT labeleddata.purchases, provider.impressions
        FROM labeleddata
        INNER JOIN salesdata
          ON labeleddata.hashedemail = provider.hashedemail
        WHERE MONTH(labeleddata.purchasedate) > :campaignmonth
        AND testgroup = :group
       "
}
```

10 L'entreprise A ajoute son compte (par exemple, 444455556666) au contrôle du fournisseur d'analyse autorisé dans la règle d'analyse personnalisée. Ils utilisent le contrôle du fournisseur d'analyse autorisé car ils souhaitent autoriser l'exécution de toutes les requêtes qu'ils créent sur leur table configurée pour les ventes.

```
{
  "allowedAnalyses": [
    "ANY_QUERY"
  ],
  "allowedAnalysisProviders": [
    "444455556666"
  ]
}
```

11 L'entreprise B voit le modèle d'analyse créé dans la collaboration et en examine le contenu, y compris la chaîne de requête et le paramètre.

12 L'entreprise B détermine que le modèle d'analyse répond au cas d'utilisation de l'incrémentalité et répond à ses exigences de confidentialité quant à la manière dont sa table configurée d'audience peut être interrogée.

13 La société B ajoute l'ARN du modèle d'analyse au contrôle d'analyse autorisé dans la règle d'analyse personnalisée de la table d'audience. Ils utilisent le contrôle d'analyse autorisé car ils souhaitent uniquement autoriser l'exécution de la requête d'incrémentalité sur leur table configurée par affichage.

```
{
  "allowedAnalyses": [
```

```
    "arn:aws:cleanrooms:us-east-1:111122223333:membership/41327cc4-bbf0-43f1-b70c-
a160dddceb08/analysistemplate/1ff1bf9d-781c-418d-a6ac-2b80c09d6292"
  ]
}
```

14L'entreprise A exécute le modèle d'analyse et utilise la valeur du paramètre`05-01-2023`.

Règle d'analyse personnalisée avec confidentialité différentielle

Dans AWS Clean Rooms, la règle d'analyse personnalisée prend en charge la confidentialité différentielle. La confidentialité différentielle est un cadre mathématiquement rigoureux pour la protection de la confidentialité des données qui vous aide à protéger vos données contre les tentatives de réidentification.

La confidentialité différentielle prend en charge les analyses agrégées telles que la planification de campagnes publicitaires, les post-ad-campaign mesures, l'analyse comparative au sein d'un consortium d'institutions financières et les tests A/B pour la recherche dans le domaine de la santé.

La structure et la syntaxe de requête prises en charge sont définies dansStructure et syntaxe des requêtes.

Exemple de règle d'analyse personnalisée avec confidentialité différentielle

Examinez l'exemple de règle d'analyse personnalisée présenté dans la section précédente. Cet exemple montre comment vous pouvez utiliser la confidentialité différentielle pour protéger vos données contre les tentatives de réidentification tout en permettant à votre partenaire de tirer des informations critiques de vos données. Supposons que l'entreprise B, qui possède les données d'audience, souhaite protéger ses données en utilisant une confidentialité différentielle. Pour terminer la configuration de la confidentialité différentielle, l'entreprise B effectue les étapes suivantes :

1. L'entreprise B active la confidentialité différentielle tout en ajoutant une règle d'analyse personnalisée au tableau configuré par le nombre de vues. L'entreprise B sélectionne `viewershipdata.hashedemail` comme colonne d'identifiant utilisateur.
2. L'entreprise B ajoute une politique de confidentialité différentielle à la collaboration afin de rendre sa table de données d'audience disponible pour les requêtes. L'entreprise B sélectionne la politique par défaut pour terminer rapidement la configuration.

L'entreprise A, qui souhaite comprendre l'augmentation des ventes d'une campagne publicitaire sur le site de l'entreprise B, exécute le modèle d'analyse. La requête étant compatible avec la structure de requête à usage général de AWS Clean Rooms Differential Privacy, elle s'exécute correctement.

Structure et syntaxe des requêtes

Les requêtes contenant au moins une table dont la confidentialité différentielle est activée doivent respecter la syntaxe suivante.

```
query_statement:
    [cte, ...] final_select

 cte:
    WITH sub_query AS (
       inner_select
       [ UNION | INTERSECT | UNION_ALL | EXCEPT/MINUS ]
       [ inner_select ]
    )

 inner_select:
     SELECT [user_id_column, ] expression [, ...]
     FROM table_reference [, ...]
     [ WHERE condition ]
     [ GROUP BY user_id_column[, expression] [, ...] ]
     [ HAVING condition ]

 final_select:
     SELECT [expression, ...] | COUNT | COUNT_DISTINCT | SUM | AVG | STDDEV
     FROM table_reference [, ...]
     [ WHERE condition ]
     [ GROUP BY expression [, ...] ]
     [ HAVING COUNT | COUNT_DISTINCT | SUM | AVG | STDDEV | condition ]
     [ ORDER BY column_list ASC | DESC ]
     [ OFFSET literal ]
     [ LIMIT literal ]

 expression:
    column_name [, ...] | expression AS alias | aggregation_functions |
window_functions_on_user_id | scalar_function | CASE | column_name math_expression [,
expression]

 window_functions_on_user_id:
```

```
    function () OVER (PARTITION BY user_id_column, [column_name] [ORDER BY column_list
ASC|DESC])
```

> **Note**
>
> En ce qui concerne la structure et la syntaxe différentielles des requêtes de confidentialité, tenez compte des points suivants :
>
> - Les sous-requêtes ne sont pas prises en charge.
> - Les expressions de table communes (CTE) doivent émettre la colonne d'identifiant utilisateur si une table ou un CTE implique des données protégées par une confidentialité différentielle. Les filtres, les regroupements et les agrégations doivent être effectués au niveau de l'utilisateur.
> - Final_select autorise les fonctions d'agrégation COUNT DISTINCT, COUNT, SUM, AVG et STDDEV.

Pour plus de détails sur les mots clés SQL pris en charge pour une confidentialité différentielle, consultezSQLfonctionnalités de la confidentialité AWS Clean Rooms différentielle.

Règle d'analyse des tables de mappage d'identifiants

Dans AWS Clean Rooms, une règle d'analyse de table de mappage d'identifiants n'est pas une règle d'analyse autonome. Ce type de règle d'analyse est géré AWS Clean Rooms et utilisé pour joindre des données d'identité disparates afin de faciliter les requêtes. Il est automatiquement ajouté aux tables de mappage des identifiants et ne peut pas être modifié. Elle hérite des comportements des autres règles d'analyse de la collaboration, à condition que ces règles d'analyse soient homogènes.

La règle d'analyse des tables de mappage d'identifiants renforce la sécurité d'une table de mappage d'identifiants. Cela empêche un membre de la collaboration de sélectionner ou d'inspecter directement la population ne se chevauchant pas entre les ensembles de données des deux membres à l'aide de la table de mappage des identifiants. La règle d'analyse de la table de mappage d'identifiants est utilisée pour protéger les données sensibles de la table de mappage d'identifiants lorsqu'elles sont utilisées implicitement dans des requêtes avec d'autres règles d'analyse.

Avec la règle d'analyse de la table de mappage d'identifiants, AWS Clean Rooms applique un chevauchement des deux côtés de la table de mappage d'identifiants développéeSQL. Cela vous permet d'effectuer les tâches suivantes :

- Utilisez le chevauchement de la table de mappage des identifiants dans JOIN les instructions.

  AWS Clean Rooms autorise une INNER RIGHT jointure ou une jointure sur la table de mappage des identifiants si elle respecte le chevauchement. LEFT
- Utilisez les colonnes de la table de mappage dans JOIN les instructions.

  Vous ne pouvez pas utiliser les colonnes de la table de mappage dans les instructions suivantes :SELECT,, WHERE HAVINGGROUP BY, ou ORDER BY (sauf si les protections sont modifiées sur l'association d'espace de noms d'ID source ou sur l'association d'espace de noms d'ID cible).
- En version étendueSQL, prend AWS Clean Rooms également en charge OUTER JOINJOIN, implicite et CROSSJOIN. Ces jointures ne peuvent pas satisfaire aux exigences de chevauchement. AWS Clean Rooms Utilisez-le plutôt `requireOverlap` pour spécifier les colonnes qui doivent être jointes.

La structure et la syntaxe de requête prises en charge sont définies dans. Structure et syntaxe des requêtes de la table de mappage d'identifiants

Les paramètres de la règle d'analyse, définis dansContrôles des requêtes des règles d'analyse des tables de mappage d'identifiants, incluent les contrôles des requêtes et les contrôles des résultats des requêtes. Ses contrôles de requête incluent la possibilité d'exiger le chevauchement de la table de mappage des identifiants dans JOIN les instructions (c'est-à-dire,`requireOverlap`).

Rubriques

- Structure et syntaxe des requêtes de la table de mappage d'identifiants
- Contrôles des requêtes des règles d'analyse des tables de mappage d'identifiants
- Structure prédéfinie des règles d'analyse des tables de mappage d'identifiants
- Règle d'analyse des tables de mappage d'identifiants — exemple

Structure et syntaxe des requêtes de la table de mappage d'identifiants

Les requêtes sur les tables dotées d'une règle d'analyse des tables de mappage d'ID doivent respecter la syntaxe suivante.

```
--select_list_expression
SELECT
```

```
provider.data_col, consumer.data_col

--table_expression
FROM provider

JOIN idMappingTable idmt ON provider.id = idmt.sourceId

JOIN consumer ON consumer.id = idmt.targetId
```

Tables de collaboration

Les tableaux suivants représentent les tables configurées qui existent dans une AWS Clean Rooms collaboration. La colonne id des tables cr_drivers_license et cr_insurance représente une colonne correspondant à la table de mappage des identifiants.

cr_drivers_license

id	nom_pilote	état_d'enregistrement
1	Eduard	TX
2	Dana	MA
3	Gweneth	IL

cr_insurance

id	courriel_du titulaire de la police	numéro_politique
a	eduardo@internal.company.com	17f9d04e-f5be-4426-bdc4-250ed59c6529
b	gwen@internal.company.com	3f0092db-2316-48a8-8d44-09cf8f6e6c64
c	rosa@internal.company.com	d7692e84-3d3c-47b8-b46d-a0d5345f0601

Table de mappage des identifiants

Le tableau suivant représente une table de mappage d'identifiants existante qui correspond aux tables cr_drivers_license et cr_insurance. Toutes les entrées ne seront pas disponibles IDs pour les deux tables de collaboration.

cr_drivers_license_id	cr_insurance_id
1	a
2	null
3	b
null	c

La règle d'analyse de la table de mappage d'identifiants autorise uniquement l'exécution de requêtes sur l'ensemble de données qui se chevauchent, qui se présente comme suit :

cr_drivers_license_id	cr_insurance_id	nom_pilote	état_d'enregistrement	courriel_du titulaire de la police	numéro_politique
1	a	Eduard	TX	eduardo@internal.company.com	17f9d04e-f5be-4426-bdc4-250ed59c6529
3	b	Gweneth	IL	gwen@internal.company.com	3f0092db-2316-48a8-8d44-09cf8f6e6c64

Exemples de requêtes

Les exemples suivants montrent des emplacements valides pour les jointures de tables de mappage d'identifiants :

```
-- Single ID mapping table
SELECT
    [ select_items ]
FROM
    cr_drivers_license cr_dl
    [ INNER | LEFT | RIGHT ] JOIN cr_identity_mapping_table idmt ON
 idmt.cr_drivers_license_id = cr_dl.id
    [ INNER | LEFT | RIGHT ] JOIN cr_insurance cr_in            ON
 idmt.cr_insurance_id       = cr_in.id
;

-- Single ID mapping table (Subquery)
SELECT
    [ select_items ]
FROM (
    SELECT
        [ select_items ]
    FROM
        cr_drivers_license cr_dl
        [ INNER | LEFT | RIGHT ] JOIN cr_identity_mapping_table idmt ON
 idmt.cr_drivers_license_id = cr_dl.id
        [ INNER | LEFT | RIGHT ] JOIN cr_insurance cr_in            ON
 idmt.cr_insurance_id       = cr_in.id
)
;

-- Single ID mapping table (CTE)
WITH
    matched_ids AS (
        SELECT
            [ select_items ]
        FROM
            cr_drivers_license cr_dl
            [ INNER | LEFT | RIGHT ] JOIN cr_identity_mapping_table idmt ON
 idmt.cr_drivers_license_id = cr_dl.id
            [ INNER | LEFT | RIGHT ] JOIN cr_insurance cr_in            ON
 idmt.cr_insurance_id       = cr_in.id
    )
SELECT
    [ select_items ]
FROM
    matched_ids
;
```

Considérations

En ce qui concerne la structure et la syntaxe des requêtes de la table de mappage d'identifiants, tenez compte des points suivants :

- Vous ne pouvez pas le modifier.
- Il est appliqué par défaut à la table de mappage des identifiants.
- Il utilise une association d'espaces de noms d'ID source et cible au sein de la collaboration.
- La table de mappage des identifiants est configurée par défaut pour fournir des protections par défaut à la colonne provenant de l'espace de noms des identifiants. Vous pouvez modifier cette configuration afin que la colonne provenant de l'espace de noms ID (soit`targetID`) `sourceID` soit autorisée n'importe où dans la requête. Pour de plus amples informations, veuillez consulter Utilisation des espaces de noms d'ID dans AWS Clean Rooms.
- La règle d'analyse des tables de mappage d'identifiants hérite des SQL restrictions des autres règles d'analyse de la collaboration.

Contrôles des requêtes des règles d'analyse des tables de mappage d'identifiants

Avec les commandes de requête de table de mappage d'ID, vous AWS Clean Rooms contrôlez la manière dont les colonnes de votre table sont utilisées pour interroger la table. Par exemple, il contrôle quelles colonnes sont utilisées pour la jointure et quelles colonnes doivent être superposées. La règle d'analyse des tables de mappage d'identifiants inclut également des fonctionnalités qui vous permettent d'autoriser la projection du `sourceIDtargetID`, ou des deux, sans avoir besoin deJOIN.

Le tableau suivant explique chaque contrôle.

Contrôle	Définition	Utilisation
`joinColumns`	Les colonnes que le membre autorisé à interroger peut utiliser dans la INNER JOIN déclaration.	Vous ne pouvez pas utiliser `joinColumns` dans d'autres parties de la requête que INNERJOIN.

Contrôle	Définition	Utilisation
		Pour de plus amples informations, veuillez consulter Commandes de jointure.
`dimensionColumns`	Les colonnes (le cas échéant) que le membre autorisé à interroger peut utiliser dans les instructions SELECT IN et GROUP BY.	A `dimensionColumn` peut être utilisé dans SELECT et GROUPBY. A `dimensionColumn` peut apparaître sous la forme`joinKeys`. Vous ne pouvez utiliser la JOIN clause `dimension Columns` in que si vous la spécifiez entre crochets.
`queryContraints:RequireOverlap`	Les colonnes de la table de mappage d'identifiants qui doivent être jointes pour que la requête puisse être exécutée.	Ces colonnes doivent être utilisées pour JOIN la table de mappage des identifiants et une table de collaboration.

Structure prédéfinie des règles d'analyse des tables de mappage d'identifiants

La structure prédéfinie d'une règle d'analyse de table de mappage d'identifiants est assortie de protections par défaut appliquées au et. `sourceID` `targetID` Cela signifie que la colonne avec les protections appliquées doit être utilisée dans les requêtes.

Vous pouvez configurer la règle d'analyse de la table de mappage d'identifiants de la manière suivante :

- À la fois `sourceID` et `targetID` protégé

Dans cette configuration, le `sourceID` et ne `targetID` peuvent pas être projetés tous les deux. Le `sourceID` et `targetID` doit être utilisé dans un JOIN lorsque la table de mappage des identifiants est référencée.

- `targetID`Protégé uniquement

  Dans cette configuration, le ne `targetID` peut pas être projeté. Le `targetID` doit être utilisé JOIN lorsque la table de mappage des identifiants est référencée. Le `sourceID` peut être utilisé dans une requête.

- `sourceID`Protégé uniquement

  Dans cette configuration, le ne `sourceID` peut pas être projeté. Le `sourceID` doit être utilisé dans une table de mappage d'identifiants JOIN lorsque celle-ci est référencée. Le `targetID` peut être utilisé dans une requête.

- Ni l'`sourceID`un ni l'`targetID`autre

  Dans cette configuration, la table de mappage des identifiants n'est soumise à aucune application spécifique pouvant être utilisée dans la requête.

L'exemple suivant montre une structure prédéfinie pour une règle d'analyse de table de mappage d'identifiants avec les protections par défaut appliquées au et. `sourceID` `targetID` Dans cet exemple, la règle d'analyse de la table de mappage d'identifiants autorise uniquement une INNER JOIN opération à la fois sur la `sourceID` colonne et sur la `targetID` colonne.

```
{
  "joinColumns": [
    "source_id",
    "target_id"
  ],
  "queryConstraints": [
    {
      "requireOverlap": {
        "columns": [
          "source_id",
          "target_id"
        ]
      }
    }
  ],
  "dimensionColumns": [] // columns that can be used in SELECT and JOIN
```

```
}
```

L'exemple suivant montre une structure prédéfinie pour une règle d'analyse de table de mappage d'identifiants avec des protections appliquées au. `targetID` Dans cet exemple, la règle d'analyse de la table de mappage d'identifiants autorise uniquement une INNER JOIN opération sur la `sourceID` colonne.

```
{
  "joinColumns": [
    "source_id",
    "target_id"
  ],
  "queryConstraints": [
    {
      "requireOverlap": {
        "columns": [
          "target_id"
        ]
      }
    }
  ],
  "dimensionColumns": [
    "source_id"
  ]
}
```

L'exemple suivant montre une structure prédéfinie pour une règle d'analyse de table de mappage d'identifiants avec des protections appliquées au. `sourceID` Dans cet exemple, la règle d'analyse de la table de mappage d'identifiants autorise uniquement une INNER JOIN opération sur la `targetID` colonne.

```
{
  "joinColumns": [
    "source_id",
    "target_id"
  ],
  "queryConstraints": [
    {
      "requireOverlap": {
        "columns": [
          "source_id"
        ]
```

```
      }
    }
  ],
  "dimensionColumns": [
    "target_id"
  ]
}
```

L'exemple suivant montre une structure prédéfinie pour une règle d'analyse de table de mappage d'identifiants sans protection appliquée au ou. `sourceID` `targetID` Dans cet exemple, la règle d'analyse de la table de mappage d'identifiants autorise une INNER JOIN opération à la fois sur la `sourceID` colonne et sur la `targetID` colonne.

```
{
  "joinColumns": [
    "source_id",
    "target_id"
  ],
  "queryConstraints": [
    {
      "requireOverlap": {
        "columns": []
      }
    }
  ],
  "dimensionColumns": [
    "source_id",
    "target_id"
  ]
}
```

Règle d'analyse des tables de mappage d'identifiants — exemple

Plutôt que de rédiger une longue déclaration en cascade faisant référence à des informations personnellement identifiables (PII), les entreprises peuvent par exemple utiliser la règle d'analyse des tables de mappage d'identifiants pour utiliser le LiveRamp transcodage multipartite. L'exemple suivant montre comment vous pouvez collaborer en AWS Clean Rooms utilisant la règle d'analyse des tables de mappage d'identifiants.

L'entreprise A est un annonceur qui dispose de données sur les clients et les ventes, qui seront utilisées comme source. La société A effectue également le transcodage pour le compte des parties à la collaboration et apporte les LiveRamp informations d'identification.

L'entreprise B est un éditeur qui possède des données sur les événements, qui seront utilisées comme cible.

> **Note**
>
> La société A ou la société B peuvent fournir des informations d'identification pour le LiveRamp transcodage et effectuer le transcodage.

Pour créer une collaboration permettant d'analyser la table de mappage des identifiants en collaboration, les entreprises procèdent comme suit :

1. L'entreprise A crée une collaboration et crée une adhésion. Elle ajoute la société B, qui crée également une adhésion à la collaboration.
2. La société A associe une source d'espace de noms d'ID existante ou en crée une nouvelle en Résolution des entités AWS utilisant la AWS Clean Rooms console.

   L'entreprise A crée une table configurée avec ses données de vente et une colonne saisie sur le `sourceId` dans la table de mappage des identifiants.

   La source de l'espace de noms ID fournit les données à transcoder.
3. La société B associe une cible d'espace de noms ID existante ou en crée une nouvelle en Résolution des entités AWS utilisant la AWS Clean Rooms console.

   L'entreprise B crée une table configurée avec ses données d'événements et une colonne saisie sur le `targetId` dans la table de mappage des identifiants.

   La cible de l'espace de noms ID ne fournit pas de données à transcoder, mais uniquement des métadonnées relatives à la LiveRamp configuration.
4. L'entreprise A découvre les deux espaces de noms d'identification associés à la collaboration et crée et remplit une table de mappage d'identifiants.
5. L'entreprise A exécute une requête sur les deux ensembles de données en les joignant dans la table de mappage des identifiants.

```
--- this would be valid for Custom or List
```

```
SELECT provider.data_col, consumer.data_col
FROM provider
  JOIN idMappingTable-123123123123-myMappingWFName idmt
     ON provider.id = idmt.sourceId
  JOIN consumer
     ON consumer.id = idmt.targetId
```

AWS Clean Rooms Confidentialité différentielle

AWS Clean Rooms La confidentialité différentielle vous aide à protéger la vie privée de vos utilisateurs grâce à une technique basée sur des mathématiques qui est mise en œuvre avec des commandes intuitives en quelques clics. En tant que fonctionnalité entièrement gérée, aucune expérience préalable en matière de confidentialité différentielle n'est nécessaire pour vous aider à empêcher la réidentification de vos utilisateurs. AWS Clean Rooms ajoute automatiquement une quantité de bruit soigneusement calibrée aux résultats de la requête lors de l'exécution afin de protéger vos données au niveau individuel.

AWS Clean Rooms La confidentialité différentielle prend en charge un large éventail de requêtes analytiques et convient parfaitement à une grande variété de cas d'utilisation, dans lesquels une petite quantité d'erreur dans les résultats des requêtes ne compromet pas l'utilité de votre analyse. Grâce à elle, vos partenaires peuvent générer des informations critiques sur les campagnes publicitaires, les décisions d'investissement, la recherche clinique, etc., le tout sans nécessiter de configuration supplémentaire de la part de vos partenaires.

AWS Clean Rooms La confidentialité différentielle protège contre le débordement ou les erreurs de diffusion non valides qui utilisent des fonctions scalaires ou des symboles d'opérateurs mathématiques de manière malveillante.

Pour plus d'informations sur la confidentialité AWS Clean Rooms différentielle, consultez les rubriques suivantes.

Rubriques

Confidentialité différentielle

La confidentialité différentielle ne permet que des informations agrégées et masque la contribution des données individuelles à ces informations. La confidentialité différentielle protège les données de

collaboration du membre qui peut recevoir des résultats en découvrant une personne en particulier. Sans confidentialité différentielle, le membre qui peut recevoir des résultats peut tenter de déduire des données utilisateur individuelles en ajoutant ou en supprimant des enregistrements concernant un individu et en observant la différence entre les résultats des requêtes.

Lorsque la confidentialité différentielle est activée, une quantité spécifiée de bruit est ajoutée aux résultats de la requête pour masquer la contribution des utilisateurs individuels. Si le membre qui peut recevoir des résultats essaie d'observer la différence entre les résultats de la requête après avoir supprimé des enregistrements concernant un individu de son ensemble de données, la variabilité du résultat de la requête empêche l'identification des données de l'individu. AWS Clean Rooms La confidentialité différentielle utilise le SampCertsampler, une implémentation d'échantillonneur correcte et éprouvée développée par. AWS

Comment AWS Clean Rooms fonctionne la confidentialité différentielle

Le flux de travail dans lequel vous souhaitez activer la confidentialité différentielle AWS Clean Rooms nécessite les étapes supplémentaires suivantes lors de l'exécution du flux de travail pour AWS Clean Rooms :

1. Vous activez la confidentialité différentielle lorsque vous ajoutez une règle d'analyse personnalisée.
2. Vous configurez la politique de confidentialité différentielle pour la collaboration afin que vos tables de données protégées par une confidentialité différentielle soient disponibles pour les requêtes.

Une fois ces étapes terminées, le membre habilité à effectuer des requêtes peut commencer à exécuter des requêtes sur des données protégées par la confidentialité différentielle. AWS Clean Rooms renvoie des résultats conformes à la politique de confidentialité différentielle. AWS Clean Rooms La confidentialité différentielle permet de suivre le nombre estimé de requêtes restantes que vous pouvez exécuter, comme la jauge d'essence d'une voiture qui indique le niveau de carburant actuel de la voiture. Le nombre de requêtes que le membre autorisé peut exécuter est limité par le budget de confidentialité et le bruit ajouté par requête, paramètres définis dans lePolitique de confidentialité différentielle.

Considérations

Lorsque vous utilisez la confidentialité différentielle dans AWS Clean Rooms, tenez compte des points suivants :

- Le membre qui peut recevoir les résultats ne peut pas utiliser la confidentialité différentielle. Ils configureront une règle d'analyse personnalisée avec la confidentialité différentielle désactivée pour leurs tables configurées.
- Le membre qui peut effectuer une requête ne peut pas joindre les tables de deux fournisseurs de données ou plus lorsque la confidentialité différentielle est activée dans les deux cas.

Politique de confidentialité différentielle

La politique de confidentialité différentielle contrôle le nombre de fonctions d'agrégation que le membre qui peut interroger est autorisé à exécuter dans le cadre d'une collaboration. Le budget de confidentialité définit une ressource commune limitée qui est appliquée à toutes les tables d'une collaboration. Le bruit ajouté par requête détermine le taux d'épuisement du budget de confidentialité.

Une politique de confidentialité différentielle est requise pour que vos tables protégées par la confidentialité différentielle soient disponibles pour les requêtes. Il s'agit d'une étape unique dans le cadre d'une collaboration qui inclut deux contributions :

- Budget de confidentialité — Quantifié en termes d'epsilon, le budget de confidentialité contrôle le niveau de protection de la vie privée. Il s'agit d'une ressource commune limitée qui est appliquée à toutes vos tables protégées par une confidentialité différentielle dans le cadre de la collaboration, car l'objectif est de préserver la confidentialité de vos utilisateurs dont les informations peuvent être présentes dans plusieurs tables.

  Le budget de confidentialité est consommé chaque fois qu'une requête est exécutée sur vos tables. Lorsque le budget de confidentialité est totalement épuisé, le membre de la collaboration qui peut effectuer des requêtes ne peut pas exécuter de requêtes supplémentaires tant qu'il n'est pas augmenté ou actualisé. En établissant un budget de confidentialité plus important, le membre qui peut recevoir les résultats peut réduire son incertitude quant aux individus contenus dans les données. Choisissez un budget de confidentialité qui équilibre vos exigences en matière de collaboration et vos besoins en matière de confidentialité, après avoir consulté les décideurs commerciaux.

Vous pouvez sélectionner Actualiser le budget de confidentialité tous les mois pour créer automatiquement un nouveau budget de confidentialité chaque mois calendaire, si vous prévoyez d'intégrer régulièrement de nouvelles données à la collaboration. Le choix de cette option permet de révéler des quantités arbitraires d'informations sur les lignes de données lorsqu'elles sont demandées à plusieurs reprises lors des actualisations. Évitez de choisir cette option si les mêmes lignes doivent être consultées à plusieurs reprises entre les actualisations du budget de confidentialité.

- Le bruit ajouté par requête est mesuré en fonction du nombre d'utilisateurs dont vous souhaitez masquer les contributions. Cette valeur détermine le taux d'épuisement du budget de confidentialité. Une valeur de bruit plus élevée réduit le taux d'épuisement du budget de confidentialité et permet donc d'exécuter davantage de requêtes sur vos données. Cependant, cela doit être contrebalancé par la publication d'informations de données moins précises. Tenez compte de la précision souhaitée pour les informations sur la collaboration lorsque vous définissez cette valeur.

Vous pouvez utiliser la politique de confidentialité différentielle par défaut pour terminer rapidement la configuration ou personnaliser votre politique de confidentialité différentielle en fonction de votre cas d'utilisation. AWS Clean Rooms La confidentialité différentielle fournit des commandes intuitives pour configurer la politique. AWS Clean Rooms La confidentialité différentielle vous permet de prévisualiser l'utilitaire en termes de nombre d'agrégations possibles pour toutes les requêtes portant sur vos données et d'estimer le nombre de requêtes pouvant être exécutées dans le cadre d'une collaboration sur les données.

Vous pouvez utiliser les exemples interactifs pour comprendre l'impact des différentes valeurs du budget de confidentialité et du bruit ajouté par requête sur les résultats des différents types de SQL requêtes. En général, vous devez trouver un équilibre entre vos besoins en matière de confidentialité, le nombre de requêtes que vous souhaitez autoriser et l'exactitude de ces requêtes. Un budget de confidentialité réduit ou une augmentation du bruit ajouté par requête permet de mieux protéger la confidentialité des utilisateurs, mais fournit des informations moins pertinentes à vos partenaires de collaboration.

Si vous augmentez le budget de confidentialité tout en conservant le même paramètre de bruit ajouté par requête, le membre autorisé à effectuer une requête peut exécuter davantage d'agrégations sur vos tables dans le cadre de la collaboration. Vous pouvez augmenter le budget de confidentialité à tout moment au cours de la collaboration. Si vous réduisez le budget de confidentialité tout en conservant le même paramètre de bruit ajouté par requête, le membre autorisé à effectuer une

requête peut exécuter moins d'agrégations. Vous ne pouvez pas réduire le budget consacré à la confidentialité une fois que le membre habilité à interroger a commencé à analyser vos données.

Si vous augmentez le niveau de bruit ajouté par requête tout en conservant le même niveau d'entrée relatif au budget de confidentialité, le membre autorisé à effectuer des requêtes peut exécuter davantage d'agrégations sur vos tables dans le cadre de la collaboration. Si vous réduisez le bruit ajouté par requête tout en conservant le même montant d'entrée relatif au budget de confidentialité, le membre autorisé à effectuer une requête peut exécuter moins d'agrégations. Vous pouvez augmenter ou diminuer le bruit ajouté par requête à tout moment au cours de la collaboration.

La politique de confidentialité différentielle est gérée par les API actions du modèle de budget de confidentialité.

SQLfonctionnalités de la confidentialité AWS Clean Rooms différentielle

AWS Clean Rooms La confidentialité différentielle utilise une structure de requête polyvalente pour prendre en charge les requêtes complexesSQL. Les modèles d'analyse personnalisés sont validés par rapport à cette structure afin de garantir qu'ils peuvent être exécutés sur des tables protégées par une confidentialité différentielle. Le tableau suivant indique les fonctions prises en charge. Pour plus d'informations, consultez Structure et syntaxe des requêtes.

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Fonctions d'agrégation	• ANY_ VALUE fonction • APPROXIMATEPERCENTILE_DISC fonction • AVGfonction • COUNTet COUNT DISTINCT fonctions • LISTAGGfonction • MAXfonction • MEDIANfonction	Soutenu à la condition que l'CTEsutilisation de tables protégées par la confidentialité différentielle doit aboutir à des données contenant des enregistrements au niveau de l'utilisateur. Vous devez écrire l'SELECTexpression dans ceux qui CTEs	Agrégations prises en charge : AVGCOUNT, COUNTDISTINCT,STDDEV, etSUM.

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
	• MINfonction • PERCENTILE_ CONT fonction • STDDEVPOP fonctions STDDEV _ SAMP et _ • SUMet SUM DISTINCT fonctions • VARPOPfonctions VAR _ SAMP et _	utilisent le `SELECT userIdentifierColumn...' format.	
CTEs	WITHclause, WITH sous-requête de clause	Soutenu à la condition que l'CTEsutilisation de tables protégées par la confidentialité différentielle doit aboutir à des données contenant des enregistrements au niveau de l'utilisateur. Vous devez écrire l'SELECTexpression dans ceux qui CTEs utilisent le `SELECT userIdentifierColumn...' format.	N/A

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Sous-requêtes	• SELECT • HAVING • JOIN • JOINétat • FROM • WHERE	Vous pouvez avoir n'importe quelle sous-requête qui ne fait pas référence à des relations de confidentialité différentielles dans ces constructions. Toute sous-requête ne peut faire référence à des relations de confidentialité différentielles que dans une JOIN clause FROM and.	
Clauses d'adhésion	• INNER JOIN • LEFT JOIN • RIGHT JOIN • FULL JOIN • [JOIN] Opérateur OR • CROSS JOIN	Pris en charge à condition que seules JOIN les fonctions qui sont des jointures égales sur les colonnes d'identifiant utilisateur soient prises en charge et soient obligatoires lors de l'interrogation de deux tables ou plus avec la confidentialité différentielle activée. Assurez-vous que les conditions d'équijointure obligatoires sont correctes. Vérifiez que le propriétaire de la table a configuré la même colonne d'identifiant utilisateur dans toutes les tables afin que la définition d'un utilisateur reste cohérente d'une table à l'autre. CROSSJOINles fonctions ne sont pas prises en charge lors de la combinaison de deux ou plusieurs relations lorsque la confidentialité différentielle est activée.	
Définir les opérateurs	UNION, UNIONALL, INTERSECT, EXCEPT | MINUS (ce sont des synonymes)	Tous sont pris en charge	Non pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Fonctions de fenêtrage	Fonctions d’agrégation • AVGfonction de fenêtre • COUNTfonction de fenêtre • CUME_ fonction DIST de fenêtre • DENSE_ fonction RANK de fenêtre • FIRST_ fonction VALUE de fenêtre • LAGfonction de fenêtre • LAST_ fonction VALUE de fenêtre • LEADfonction de fenêtre • MAXfonctions de fenêtre • MEDIANfonctions de fenêtre • MINfonctions de fenêtre • NTH_ fonction VALUE de fenêtre • RATIOfonction de fenêtre _TO_ REPORT	Tous sont pris en charge à condition que la colonne d'identifiant utilisateur de la clause de partition de la fonction de fenêtre soit requise lorsque vous interrogez une relation avec la confidentialité différentielle activée.	Non pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
	• STDDEVfonctions de POP fenêtre STDDEV_SAMP et _ (STDDEV_SAMP et STDDEV sont des synonymes) • SUMfonctions de fenêtre • VARfonctions de POP fenêtre VAR_SAMP et _ (VAR_SAMP et VARIANCE sont des synonymes) Fonctions de classement • DENSE_ fonction RANK de fenêtre • NTILEfonction de fenêtre • PERCENT_ fonction RANK de fenêtre • RANKfonction de fenêtre • ROW_ fonction NUMBER de fenêtre		

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Expressions conditionnelles	• CASEexpression de condition • COALESCEexpression • GREATESTet LEAST fonctions • NVLet COALESCE fonctions • NVL2fonction • NULLIFfonction	Tous sont pris en charge	Tous sont pris en charge
Conditions	• Condition de comparaison • Conditions logiques • Conditions de correspondance de modèles • BETWEENconditions d'autonomie • Condition null	`EXISTS`et `IN` ne peuvent pas être utilisés car ils nécessitent des sous-requêtes. Tous les autres sont pris en charge.	Tous sont pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Fonctions date-heure	• Fonctions date et heure dans les transactions • Opérateur de concaténation • ADD_ MONTHS fonctions • CONVERT_ TIMEZONE fonction • CURRENT_ DATE fonction • DATEADDfonction • DATEDIFFfonction • DATE_ PART fonctions • DATE_ TRUNC fonction • EXTRACTfonction • GETDATEfonction • TIMEOFDAY fonctions • Fonction TO_ TIMESTAMP • Parties de date pour les fonctions de date ou d’horodat age	Tous sont pris en charge	Tous sont pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Fonctions de chaîne	• opérateur || (concaténation) • BTRIMfonction • CHAR_ LENGTH fonction • CHARACTER_ LENGTH fonction • CHARINDEX fonction • CONCATfonction • LEFTet RIGHT fonctions • LENfonction • LENGTHfonction • LOWERfonction • LPADet RPAD fonctions • LTRIMfonction • POSITIONfonctions • REGEXP_ COUNT fonction • REGEXP_ INSTR fonction • REGEXP_ REPLACE fonction • REGEXP_ SUBSTR fonction • REPEATfonction • REPLACEfonction	Tous sont pris en charge	Tous sont pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
	• REPLICATE fonction • REVERSEfonction • RTRIMfonction • SOUNDEXfonction • SPLIT_ PART fonction • STRPOSfonction • SUBSTRING fonction • TEXTLENfonction • TRANSLATE fonction • TRIMfonctions • UPPERfonction		
Fonctions de formatage des types de données	• CASTfonction • À_ CHAR • Fonction TO_ DATE • À_ NUMBER • Chaînes de format datetime • Chaînes de format numériques	Tous sont pris en charge	Tous sont pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Fonctions de hachage	• MD5fonction • SHAfonction • SHA1fonction • SHA2fonction • MURMUR3_32_HASH	Tous sont pris en charge	Tous sont pris en charge
Symboles d'opérateurs mathématiques	+, -, *,/, % et @	Tous sont pris en charge	Tous sont pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Fonctions mathématiques	• ABSfonction • ACOSfonction • ASINfonction • ATANfonction • ATAN2fonction • CBRTfonction • CEILING(ouCEIL) fonction • COSfonction • COTfonction • DEGREESfonction • DEXPfonction • LTRIMfonction • DLOG1fonction • DLOG10 fonction • EXPfonction • FLOORfonction • Fonction LN • LOGfonction • MODfonction • Fonction PI • POWERfonction • RADIANSfonction • RANDOMfonction • ROUNDfonction • SIGNfonction • SINfonction • SQRTfonctions	Tous sont pris en charge	Tous sont pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
	• TRUNCfonction		
SUPERfonctions d'information de type	• DECIMAL_ PRECISION fonction • DECIMAL_ SCALE fonction • Fonction IS_ ARRAY • Fonction IS_ BIGINT • Fonction IS_ CHAR • Fonction IS_ DECIMAL • Fonction IS_ FLOAT • Fonction IS_ INTEGER • Fonction IS_ OBJECT • Fonction IS_ SCALAR • Fonction IS_ SMALLINT • Fonction IS_ VARCHAR • JSON_ TYPEOF fonction	Tous sont pris en charge	Tous sont pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
VARBYTEfonctions	• FROM_ HEX fonction • FROM_ VARBYTE fonction • Fonction TO_ HEX • Fonction TO_ VARBYTE	Tous sont pris en charge	Tous sont pris en charge
JSON	• CAN_ JSON _ PARSE fonction • JSON_ EXTRACT _ ARRAY _ ELEMENT _ TEXT fonction • JSON_ EXTRACT _ PATH _ TEXT fonction • JSON_ PARSE fonction • JSON_ SERIALIZE fonction • JSONFonction _ SERALIZE VARBYTE _TO_	Tous sont pris en charge	Tous sont pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Fonctions de tableau	• Fonction array • Fonction array_concat • Fonction array_flatten • Fonction get_array_length • Fonction split_to_array • Fonction subarray	Non pris en charge	Non pris en charge
Prolongé GROUP par	GROUPING SETS, ROLLUP, CUBE	Non pris en charge	Non pris en charge
Opération de tri	ORDERPAR	Supportée à la condition qu'une clause ORDER BY ne soit prise en charge dans la clause de partition d'une fonction de fenêtre que lors de l'interrogation de tables avec la confidentialité différentielle activée.	Pris en charge
Limites de lignes	LIMIT, OFFSET	Non pris en charge CTEs lors de l'utilisation de tables protégées par la confidentialité différentielle	Tous sont pris en charge

Nom court	SQLconstruit	Expressions de table courantes (CTEs)	SELECTClause finale
Aliasing de tables et de colonnes		Pris en charge	Pris en charge
Fonctions mathématiques sur les fonctions d'agrégation		Pris en charge	Pris en charge
Fonctions scalaires au sein de fonctions d'agrégation		Pris en charge	Pris en charge

Alternatives courantes pour les constructions non prises en charge SQL

Catégorie	SQLconstruire	Autrement
Fonctions de fenêtrage	• LISTAGG • PERCENTILE_CONT • PERCENTILE_DISC	Vous pouvez utiliser la fonction d'agrégation équivalente avec GROUP BY.
Symboles d'opérateurs mathématiques	• $column ||/ 2 • $column |/ 2 • $column ^ 2	• CBRT • SQRT • POWER($column, 2)
Fonctions scalaires	• SYSDATE • $column : :entier • convertir (type, $column)	• CURRENT_DATE • CAST$column sous forme d'entier • CASTType $column AS
Littéraux	INTERVAL« 1 » SECOND	INTERVAL« 1 » SECOND
Limitation des lignes	TOPn	LIMITn

Catégorie	SQLconstruire	Autrement
Joindre	• USING • NATURAL	La clause ON doit contenir explicitement un critère de jointure.

Conseils et exemples de requêtes relatives à la confidentialité différentielle

AWS Clean Rooms La confidentialité différentielle utilise une structure de requête polyvalente pour prendre en charge une grande variété de SQL constructions telles que Common Table Expressions (CTEs) pour la préparation des données et les fonctions d'agrégation couramment utilisées telles que`COUNT`, ou. `SUM` Afin de masquer la contribution de tout utilisateur potentiel à vos données en ajoutant du bruit aux résultats des requêtes agrégées au moment de l'exécution, la confidentialité AWS Clean Rooms différentielle exige que les fonctions d'agrégation finales `SELECT statement` soient exécutées sur des données au niveau de l'utilisateur.

L'exemple suivant utilise deux tables nommées `socialco_impressions` et `socialco_users` provenant d'un éditeur multimédia qui souhaite protéger les données en utilisant une confidentialité différentielle tout en collaborant avec une marque sportive utilisant `athletic_brand_sales` des données. L'éditeur multimédia a configuré la `user_id` colonne comme colonne d'identifiant utilisateur tout en activant la confidentialité différentielle dans AWS Clean Rooms. L'annonceur n'a pas besoin d'une protection différentielle de la confidentialité et souhaite exécuter une requête en utilisant CTEs des données combinées. Comme il CTE utilise des tables protégées de manière différentielle, l'annonceur inclut la colonne d'identifiant d'utilisateur de ces tables protégées dans la liste des CTE colonnes et joint les tables protégées dans la colonne d'identifiant d'utilisateur.

```
WITH matches_table AS(
     SELECT si.user_id, si.campaign_id, s.sale_id, s.sale_price
     FROM socialco_impressions si
     JOIN socialco_users su
         ON su.user_id = si.user_id
     JOIN athletic_brand_sales s
         ON s.emailsha256 = su.emailsha256
     WHERE s.timestamp > si.timestamp

UNION ALL
```

```
    SELECT si.user_id, si.campaign_id, s.sale_id, s.sale_price
    FROM socialco_impressions si
    JOIN socialco_users su
        ON su.user_id = si.user_id
    JOIN athletic_brand_sales s
        ON s.phonesha256 = su.phonesha256
    WHERE s.timestamp > si.timestamp
)

SELECT COUNT (DISTINCT user_id) as unique_users
FROM matches_table
GROUP BY campaign_id
ORDER BY COUNT (DISTINCT user_id) DESC
LIMIT 5
```

De même, si vous souhaitez exécuter des fonctions de fenêtre sur des tables de données protégées par la confidentialité différentielle, vous devez inclure la colonne d'identifiant utilisateur dans la `PARTITION BY` clause.

```
ROW_NUMBER() OVER (PARTITION BY conversion_id, user_id ORDER BY match_type, match_age)
 AS row
```

Limites de la confidentialité AWS Clean Rooms différentielle

AWS Clean Rooms La confidentialité différentielle ne permet pas de résoudre les situations suivantes :

1. AWS Clean Rooms La confidentialité différentielle ne traite pas des attaques temporelles. Par exemple, ces attaques sont possibles dans les scénarios où un utilisateur individuel fournit un grand nombre de lignes et où l'ajout ou la suppression de cet utilisateur modifie de manière significative le temps de calcul de la requête.
2. AWSClean Rooms Differential Privacy ne garantit pas une confidentialité différentielle lorsqu'une SQL requête peut entraîner un débordement ou des erreurs de diffusion non valides au moment de l'exécution en raison de l'utilisation de certaines SQL structures. Le tableau suivant répertorie certaines SQL constructions, mais pas toutes, susceptibles de générer des erreurs d'exécution et devant être vérifiées dans les modèles d'analyse. Nous vous recommandons d'approuver les modèles d'analyse qui minimisent les risques de telles erreurs d'exécution et de consulter régulièrement les journaux de requêtes pour déterminer si les requêtes sont conformes à l'accord de collaboration.

Les SQL constructions suivantes sont vulnérables aux erreurs de débordement :

- Fonctions d'agrégation - AVGLISTAVG,, PERCENTILE _COUNT, PERCENTILE _DISC,SUM/ SUM_ DISTINCT
- Fonctions de formatage des types de données - TO_TIMESTAMP, TO_ DATE
- Fonctions de date et d'heure - ADD _ MONTHSDATEADD, DATEDIFF
- Fonctions mathématiques - +, -, *,/, POWER
- Fonctions de chaîne - ||CONCAT,REPEAT, REPLICATE
- Fonctions de fenêtre -AVG,LISTAGG, PERCENTILE _COUNT, PERCENTILE _DISC, RATIO REPORT _TO_, SUM

La fonction de formatage CAST des types de données est vulnérable aux erreurs de conversion non valides.

Vous pouvez configurer CloudWatch pour créer un filtre métrique pour un groupe de journaux, puis créer une CloudWatch alarme sur ce filtre métrique afin de recevoir des alertes en cas de dépassement potentiel ou d'erreur de casting. Plus précisément, vous devez surveiller les codes d'erreur`CastError`,`OverflowError`,`ConversionError`. La présence de ces codes d'erreur indique une attaque potentielle par canal secondaire, mais peut également indiquer une requête erronéeSQL.

Pour de plus amples informations, veuillez consulter Connexion à une requête AWS Clean Rooms.

AWS Clean Rooms ML

AWS Clean Rooms ML

AWS Clean Rooms Le ML fournit une méthode préservant la confidentialité permettant à deux parties d'identifier des utilisateurs similaires dans leurs données sans avoir à partager leurs données entre elles. La première partie apporte les données d'entraînement AWS Clean Rooms afin de créer et de configurer un modèle similaire et de l'associer à une collaboration. Les données de départ sont ensuite transmises à la collaboration pour créer un segment similaire aux données d'entraînement.

Pour une explication plus détaillée de son fonctionnement, voirEmplois multi-comptes.

- Fournisseur de données de formation : partie qui fournit les données de formation, crée et configure un modèle similaire, puis associe ce modèle similaire à une collaboration.
- Fournisseur de données sur les semences : partie qui fournit les données sur les semences, génère un segment similaire et exporte son segment similaire.
- Données d'entraînement : données du fournisseur de données de formation, utilisées pour générer un modèle similaire. Les données d'entraînement sont utilisées pour mesurer la similitude des comportements des utilisateurs.

  Les données d'entraînement doivent contenir un ID utilisateur, un ID d'élément et une colonne d'horodatage. Les données d'entraînement peuvent éventuellement contenir d'autres interactions sous forme de caractéristiques numériques ou catégoriques. Des exemples d'interactions sont une liste de vidéos regardées, d'articles achetés ou d'articles lus.
- Données de départ : données du fournisseur de données de départ, utilisées pour créer un segment similaire. Les données de départ peuvent être fournies directement ou provenir des résultats d'une AWS Clean Rooms requête. Le résultat du segment similaire est un ensemble d'utilisateurs issu des données d'entraînement qui ressemble le plus aux utilisateurs initiaux.
- Modèle similaire : modèle d'apprentissage automatique des données d'entraînement utilisé pour rechercher des utilisateurs similaires dans d'autres ensembles de données.

  Lorsque vous utilisez leAPI, le terme modèle d'audience est utilisé de la même manière que le modèle similaire. Par exemple, vous utilisez le CreateAudienceModelAPIpour créer un modèle similaire.
- Segment similaire : sous-ensemble des données d'entraînement qui ressemble le plus aux données de départ.

Lorsque vous utilisez leAPI, vous créez un segment similaire avec le StartAudienceGenerationJobAPI.

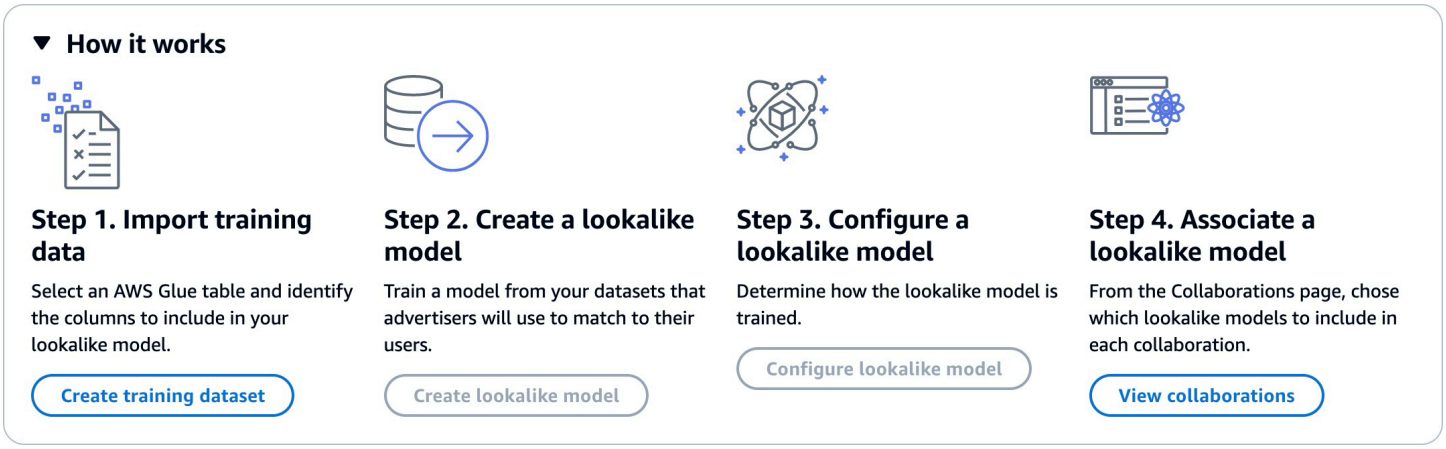
Les données du fournisseur de données de formation ne sont jamais partagées avec le fournisseur de données de départ et les données du fournisseur de données de départ ne sont jamais partagées avec le fournisseur de données de formation. La sortie du segment similaire est partagée avec le fournisseur de données de formation, mais jamais avec le fournisseur de données de départ.

Pour plus d'informations sur les modèles similaires, consultez les rubriques suivantes.

Rubriques

- Comment fonctionne le AWS Clean Rooms ML

Comment fonctionne le AWS Clean Rooms ML



Clean Rooms ML nécessite que deux parties, un fournisseur de données de formation et un fournisseur de données de base, travaillent de manière séquentielle AWS Clean Rooms pour intégrer leurs données dans une collaboration. Voici le flux de travail que le fournisseur de données de formation doit effectuer en premier :

1. Les données du fournisseur de données de formation doivent être stockées dans une table de catalogue de AWS Glue données répertoriant les interactions entre les utilisateurs et les éléments. Les données d'entraînement doivent au minimum contenir une colonne d'ID utilisateur, une colonne d'identifiant d'interaction et une colonne d'horodatage.
2. Le fournisseur de données de formation enregistre les données de formation auprès de AWS Clean Rooms.

3. Le fournisseur de données de formation crée un modèle similaire qui peut être partagé avec plusieurs fournisseurs de données initiales. Le modèle similaire est un réseau neuronal profond dont l'entraînement peut prendre jusqu'à 24 heures. Il n'est pas automatiquement réentraîné et nous vous recommandons de le réentraîner chaque semaine.
4. Le fournisseur de données de formation configure le modèle de similarité, notamment en indiquant s'il convient de partager les indicateurs de pertinence et l'emplacement des segments de sortie sur Amazon S3. Le fournisseur de données de formation peut créer plusieurs modèles similaires configurés à partir d'un seul modèle similaire.
5. Le fournisseur de données de formation associe le modèle d'audience configuré à une collaboration partagée avec un fournisseur de données de départ.

Il s'agit du flux de travail que le fournisseur de données de départ doit ensuite effectuer :

1. Les données du fournisseur de données de base peuvent être stockées dans un compartiment Amazon S3 et peuvent provenir des résultats d'une requête.
2. Le fournisseur de données de départ ouvre la collaboration qu'il partage avec le fournisseur de données de formation.
3. Le fournisseur de données de départ crée un segment similaire à partir de l'onglet Clean Rooms ML de la page de collaboration.
4. Le fournisseur de données de base peut évaluer les indicateurs de pertinence, s'ils ont été partagés, et exporter le segment similaire pour une utilisation en dehors AWS Clean Rooms.

Protection de la vie privée du AWS Clean Rooms ML

Clean Rooms ML est conçu pour réduire le risque d'attaques par inférence d'adhésion, dans le cadre desquelles le fournisseur de données de formation peut savoir qui figure dans les données de départ et le fournisseur de données de départ peut savoir qui figure dans les données d'entraînement. Plusieurs mesures sont prises pour empêcher cette attaque.

Tout d'abord, les fournisseurs de données de départ n'observent pas directement les résultats de Clean Rooms ML et les fournisseurs de données de formation ne peuvent jamais observer les données de départ. Les fournisseurs de données de départ peuvent choisir d'inclure les données de départ dans le segment de sortie.

Ensuite, le modèle similaire est créé à partir d'un échantillon aléatoire des données d'entraînement. Cet échantillon inclut un nombre important d'utilisateurs qui ne correspondent pas à l'audience

initiale. Ce processus rend plus difficile de déterminer si un utilisateur ne figurait pas dans les données, ce qui constitue un autre moyen de déduire son appartenance.

De plus, plusieurs clients de semences peuvent être utilisés pour chaque paramètre de la formation d'un modèle similaire spécifique à une graine. Cela limite le surajustement du modèle, et donc ce qui peut être déduit à propos d'un utilisateur. Par conséquent, nous recommandons que la taille minimale des données de départ soit de 500 utilisateurs.

Enfin, les indicateurs au niveau des utilisateurs ne sont jamais fournis aux fournisseurs de données de formation, ce qui élimine toute autre possibilité d'attaque par inférence d'adhésion.

Exigences relatives aux données de formation pour Clean Rooms ML

Pour réussir à créer un modèle similaire, vos données d'entraînement doivent répondre aux exigences suivantes :

- Les données d'entraînement doivent être au JSON format ParquetCSV, ou.
- Vos données d'entraînement doivent être cataloguées dans. AWS Glue Pour plus d'informations, consultez Mise en route avec AWS Glue Data Catalog dans le Guide du développeur AWS Glue . Nous vous recommandons d'utiliser AWS Glue des robots d'exploration pour créer vos tables, car le schéma est déduit automatiquement.
- Le compartiment Amazon S3 qui contient les données d'entraînement et les données de départ se trouve dans la même AWS région que vos autres ressources Clean Rooms ML.
- Les données d'entraînement doivent contenir au moins 100 000 utilisateurs uniques IDs ayant chacun au moins deux interactions avec des éléments.
- Les données d'entraînement doivent contenir au moins 1 million d'enregistrements.
- Le schéma spécifié dans l'`CreateTrainingDataset`action doit être aligné sur le schéma défini lors de la création de la AWS Glue table.
- Les champs obligatoires, tels que définis dans le tableau fourni, sont définis dans l'`CreateTrainingDataset`action.

Type de champ	Types de données pris en charge	Obligatoire	Description
USER_ID	chaîne, int, bigint	Oui	Un identifiant unique pour chaque utilisateur l'ensemble de données. Il doit s'agir d'une va d'information non personnellement identifiabl (PII). Il peut s'agir d'un identifiant haché ou d' identifiant client.
ITEM_ID	chaîne, int, bigint	Oui	Un identifiant unique pour chaque élément av lequel un utilisateur interagit.
TIMESTAMP	bigint, int, horodatage	Oui	Heure à laquelle un utilisateur a interagi avec l'élément. Les valeurs doivent être au format Epoch Time d'Unix en secondes.
CATEGORICAL_FEATURE	chaîne, int, float, bigint, double, booléen, tableau	Non	Capture les données catégoriques relatives à l'utilisateur ou à l'article. Cela peut inclure des éléments tels que le type d'événement (tel qu clic ou un achat), les données démographiqu de l'utilisateur (groupe d'âge, sexe, anonymis localisation de l'utilisateur (ville, pays, anonym), la catégorie d'article (vêtements ou apparei électroniques, par exemple) ou la marque de l'article.
NUMERICAL_FEATURE	double, float, int, bigint	Non	Capture les données numériques relatives à l'utilisateur ou à l'article. Cela peut inclure des éléments tels que l'historique des achats des utilisateurs (montant total dépensé), le prix de l'article, le nombre de fois où un article a été ou les évaluations des utilisateurs pour les ar

- Vous pouvez éventuellement fournir jusqu'à 10 caractéristiques catégorielles ou numériques au total.

Voici un exemple d'ensemble de données d'entraînement valide au CSV format.

```
     USER_ID,ITEM_ID,TIMESTAMP, EVENT_TYPE(CATEGORICAL FEATURE),EVENT_VALUE (NUMERICAL
 FEATURE)
196,242,881250949,click,15
186,302,891717742,click,13
22,377,878887116,click,10
244,51,880606923,click,20
166,346,886397596,click,10
```

Exigences relatives aux données de base pour Clean Rooms ML

Les données de départ d'un modèle similaire peuvent provenir soit directement d'un compartiment Amazon S3, soit des résultats d'une SQL requête.

Les données sur les semences fournies directement doivent répondre aux exigences suivantes :

- Les données de départ doivent être au format de JSON lignes avec une liste d'utilisateursIDs.
- La taille de la graine doit être comprise entre 25 et 500 000 utilisateurs uniquesIDs.
- Le nombre minimum d'utilisateurs de départ doit correspondre à la valeur de taille de départ minimale correspondante que vous avez spécifiée lors de la création du modèle d'audience configuré.

Voici un exemple d'ensemble de données d'entraînement valide au CSV format.

```
{"user_id": "abc"}
{"user_id": "def"}
{"user_id": "ghijkl"}
{"user_id": "123"}
{"user_id": "456"}
{"user_id": "7890"}
```

AWS Clean Rooms Métriques d'évaluation du modèle ML

Clean Rooms ML calcule le score de rappel et de pertinence pour déterminer les performances de votre modèle. Recall compare la similitude entre les données similaires et les données

d'entraînement. Le score de pertinence est utilisé pour déterminer la taille de l'audience, et non pour déterminer si le modèle est performant.

Le rappel est une mesure impartiale de la similitude entre le segment similaire et les données d'entraînement. Le rappel est le pourcentage d'utilisateurs les plus similaires (par défaut, les 20 % les plus similaires) à partir d'un échantillon de données de formation inclus dans l'audience initiale par la tâche de génération d'audience. Les valeurs sont comprises entre 0 et 1. Des valeurs plus élevées indiquent une meilleure audience. Une valeur de rappel approximativement égale au pourcentage maximal de bacs indique que le modèle d'audience est équivalent à une sélection aléatoire.

Nous considérons qu'il s'agit d'un meilleur indicateur d'évaluation que l'exactitude, la précision et les scores F1, car Clean Rooms ML n'a pas correctement étiqueté les utilisateurs réellement négatifs lors de la création de son modèle.

Le score de pertinence au niveau du segment est une mesure de similarité avec des valeurs allant de -1 (le moins similaire) à 1 (le plus similaire). Clean Rooms ML calcule un ensemble de scores de pertinence pour différentes tailles de segment afin de vous aider à déterminer la meilleure taille de segment pour vos données. Les scores de pertinence diminuent de façon monotone à mesure que la taille du segment augmente ; par conséquent, à mesure que la taille du segment augmente, il peut être moins similaire aux données initiales. Lorsque le score de pertinence au niveau du segment atteint 0, le modèle prédit que tous les utilisateurs du segment similaire appartiennent à la même distribution que les données initiales. L'augmentation de la taille de sortie est susceptible d'inclure dans le segment similaire des utilisateurs qui ne proviennent pas de la même distribution que les données de départ.

Les scores de pertinence sont normalisés au sein d'une même campagne et ne doivent pas être utilisés pour comparer les campagnes. Les scores de pertinence ne doivent pas être utilisés comme preuve provenant d'une source unique pour un résultat commercial. En effet, ceux-ci sont influencés par de multiples facteurs complexes en plus de la pertinence, tels que la qualité des stocks, le type d'inventaire et le calendrier des publicités.

Les scores de pertinence ne doivent pas être utilisés pour juger de la qualité de la graine, mais plutôt pour déterminer si elle peut être augmentée ou diminuée. Considérez les exemples suivants :

- Tous les scores sont positifs : cela indique que le nombre d'utilisateurs prédits comme similaires est supérieur au nombre d'utilisateurs inclus dans le segment similaire. Cela est courant pour les données sur les semences qui font partie d'un vaste marché, comme pour tous ceux qui ont acheté du dentifrice au cours du dernier mois. Nous vous recommandons de consulter des données sur

des semences plus petites, comme celles de tous ceux qui ont acheté du dentifrice plus d'une fois au cours du dernier mois.

- Tous les scores sont négatifs ou négatifs pour la taille de segment de sosie souhaitée : cela indique que Clean Rooms ML prédit qu'il n'y a pas assez d'utilisateurs similaires dans la taille de segment de sosie souhaitée. Cela peut être dû au fait que les données sur les semences sont trop spécifiques ou que le marché est trop petit. Nous recommandons soit d'appliquer moins de filtres aux données sur les semences, soit d'élargir le marché. Par exemple, si les données initiales concernaient des clients ayant acheté une poussette et un siège auto, vous pourriez étendre le marché aux clients ayant acheté plusieurs produits pour bébés.

Les fournisseurs de données de formation déterminent si les scores de pertinence sont exposés et les compartiments dans lesquels les scores de pertinence sont calculés.

Travailler avec AWS Clean Rooms ML

Un modèle de similarité est un modèle de données d'un fournisseur de données de formation qui permet à un fournisseur de données de départ de créer un segment similaire des données du fournisseur de données de formation qui ressemble le plus à ses données de départ. Pour créer un modèle de similarité utilisable dans une collaboration, vous devez importer vos données de formation, créer un modèle de similarité, configurer ce modèle de similarité, puis l'associer à une collaboration.

Une fois que le fournisseur de données de formation a fini de créer le modèle ML, le fournisseur de données de départ peut créer et exporter le segment de départ.

Rubriques

- Utilisation de modèles similaires (fournisseur de données de formation)
- Utilisation de segments similaires (fournisseur de données de départ)

Utilisation de modèles similaires (fournisseur de données de formation)

Importer des données d'entraînement

Avant de créer un modèle similaire, vous devez spécifier la AWS Glue table contenant les données d'entraînement. Clean Rooms ML ne stocke pas de copie de ces données, mais uniquement des métadonnées qui lui permettent d'accéder aux données.

Pour importer des données d'entraînement dans AWS Clean Rooms

1. Connectez-vous à la AWS Clean Rooms 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, choisissez ML Modeling.
3. Dans l'onglet Ensembles de données d'entraînement, choisissez Créer un jeu de données d'entraînement.
4. Sur la page Créer un jeu de données d'entraînement, pour les détails du jeu de données d'entraînement, entrez un nom et une description facultative.
5. Choisissez la source de données d'entraînement en sélectionnant la base de données et la table que vous souhaitez configurer dans les listes déroulantes.

   > **Note**
   >
   > Pour vérifier que ce tableau est correct, effectuez l'une des opérations suivantes :
   >
   > - Choisissez Afficher dans AWS Glue.
   > - Activez Afficher le schéma pour afficher le schéma.

6. Pour les détails de la formation, choisissez la colonne Identifiant utilisateur, la colonne Identifiant de l'article et la colonne Horodatage dans les listes déroulantes. Les données d'entraînement doivent contenir ces trois colonnes. Vous pouvez également sélectionner les autres colonnes que vous souhaitez inclure dans les données d'entraînement.

   Les données de la colonne Horodatage doivent être au format Unix Epoch en secondes.
7. (Facultatif) Si vous avez des colonnes supplémentaires à entraîner, choisissez le nom et le type de colonne dans les listes déroulantes.
8. Dans Accès aux services, vous devez spécifier un rôle de service qui peut accéder à vos données et fournir une KMS clé si celles-ci sont cryptées. Choisissez Créer et utiliser un nouveau rôle de service et Clean Rooms ML créera automatiquement un rôle de service et ajoutera la politique d'autorisation nécessaire. Choisissez Utiliser un rôle de service existant et saisissez-le dans le champ Nom du rôle de service si vous souhaitez utiliser un rôle de service spécifique.

   Si vos données sont cryptées, entrez votre KMS clé dans le AWS KMS keychamp ou cliquez sur Créer une AWS KMS key pour générer une nouvelle KMS clé.

9. Si vous souhaitez activer les balises pour le jeu de données d'entraînement, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
10. Choisissez Créer un jeu de données d'entraînement.

Pour l'APIaction correspondante, voir CreateTrainingDataset.

Création d'un modèle similaire

Après avoir créé un jeu de données d'entraînement, vous êtes prêt à créer un modèle similaire. Vous pouvez créer de nombreux modèles similaires à partir d'un seul jeu de données d'entraînement.

Vous devez créer une base de données par défaut dans votre rôle AWS Glue Data Catalog ou inclure l'`glue:createDatabase`autorisation dans le rôle fourni.

Pour créer un modèle similaire dans AWS Clean Rooms

1. Connectez-vous à la AWS Clean Rooms 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, choisissez ML Modeling.
3. Dans l'onglet Modèles similaires, choisissez Créer un modèle similaire.
4. Sur la page Créer un modèle similaire, pour les détails du modèle similaire, entrez un nom et une description facultative.

    a. Choisissez le jeu de données d'entraînement que vous souhaitez modéliser dans la liste déroulante.

    > **Note**
    >
    > Pour vérifier qu'il s'agit du bon jeu de données d'entraînement, activez Afficher les détails du jeu de données d'entraînement pour afficher les détails.
    > Pour créer un nouveau jeu de données d'entraînement, choisissez Créer un jeu de données d'entraînement.

    b. (Facultatif) Entrez dans une fenêtre d'entraînement.
5. Si vous souhaitez activer les paramètres de chiffrement personnalisés pour le modèle similaire, choisissez Personnaliser les paramètres de chiffrement, puis entrez la KMS clé.
6. Si vous souhaitez activer les balises pour le modèle similaire, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

7. Choisissez Créer un modèle similaire.

> **Note**
>
> La formation des modèles peut prendre de plusieurs heures à deux jours.

Pour l'APIaction correspondante, voir CreateAudienceModel.

Configuration d'un modèle similaire

Après avoir créé un modèle similaire, vous êtes prêt à le configurer pour une utilisation dans le cadre d'une collaboration. Vous pouvez créer plusieurs modèles similaires configurés à partir d'un seul modèle similaire.

Pour configurer un modèle similaire dans AWS Clean Rooms

1. Connectez-vous à la AWS Clean Rooms 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, choisissez ML Modeling.
3. Dans l'onglet Modèles similaires configurés, choisissez Configurer le modèle similaire.
4. Sur la page Configurer le modèle similaire, pour les détails du modèle similaire configuré, entrez un nom et une description facultative.

    a. Choisissez le modèle Lookalike que vous souhaitez configurer dans la liste déroulante.

    > **Note**
    >
    > Pour vérifier qu'il s'agit du bon modèle similaire, activez Afficher les détails du modèle similaire pour afficher les détails.
    > Pour créer un nouveau modèle similaire, choisissez Créer un modèle similaire.

    b. Choisissez la taille de graine minimale correspondante que vous souhaitez. Il s'agit du nombre minimum d'utilisateurs dans les données du fournisseur de données de départ qui se chevauchent avec les utilisateurs dans les données de formation. Cette valeur doit être supérieure à 0.

5. Pour que les métriques soient partagées avec d'autres membres, choisissez si vous souhaitez que le fournisseur de données de base de votre collaboration reçoive les métriques du modèle, y compris les scores de pertinence.
6. Pour l'emplacement de destination du segment Lookalike, entrez le compartiment Amazon S3 dans lequel le segment Lookalike est exporté. Ce compartiment doit être situé dans la même région que vos autres ressources.
7. Pour l'accès au service, choisissez le nom du rôle de service existant qui sera utilisé pour accéder à cette table.
8. Pour la configuration avancée de la taille des bacs, spécifiez le type de taille de l'audience sous la forme d'un nombre absolu ou d'un pourcentage.
9. Si vous souhaitez activer les balises pour la ressource de table configurée, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
10. Choisissez Configurer le modèle similaire.

Pour l'APIaction correspondante, voir CreateConfiguredAudienceModel.

Associer un modèle similaire configuré

Après avoir configuré un modèle similaire, vous pouvez l'associer à une collaboration.

Pour associer un modèle similaire configuré dans AWS Clean Rooms

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Dans l'onglet Avec adhésion active, choisissez une collaboration.
4. Dans l'onglet ML Modeling, sous R eady-to-use lookalike models, choisissez Associate lookalike model.
5. Sur la page Associer un modèle similaire configuré, pour les détails de l'association du modèle similaire configuré :

    a. Entrez un nom pour le modèle d'audience configuré associé.

    b. Entrez une description de la table.

    La description permet de différencier les autres modèles d'audience configurés associés portant des noms similaires.

6. Pour Modèle similaire configuré, choisissez un modèle similaire configuré dans la liste déroulante.
7. Choisissez Associer.

Pour l'APIaction correspondante, voir CreateConfiguredAudienceModelAssociation.

Mettre à jour un modèle similaire configuré

Après avoir associé un modèle similaire configuré à une collaboration, vous pouvez le mettre à jour pour modifier des informations telles que le nom, les métriques à partager ou la position Amazon S3 en sortie.

Pour mettre à jour un modèle similaire configuré associé dans AWS Clean Rooms

1. Connectez-vous à la AWS Clean Rooms 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, choisissez ML modeling.
3. Dans l'onglet Modèles similaires configurés, sous Modèles eady-to-use similaires R, choisissez un modèle similaire configuré et sélectionnez Modifier.
4. Sur la page Modifier, pour les détails de l'association de modèles similaires configurés :
    a. Mettez à jour le nom et la description facultative.
    b. Choisissez le modèle Lookalike que vous souhaitez configurer dans la liste déroulante.
    c. Choisissez la taille de graine minimale correspondante que vous souhaitez. Il s'agit du nombre minimum d'utilisateurs dans les données du fournisseur de données de départ qui se chevauchent avec les utilisateurs dans les données de formation. Cette valeur doit être supérieure à 0.
5. Pour que les métriques soient partagées avec d'autres membres, choisissez si vous souhaitez que le fournisseur de données de base de votre collaboration reçoive les métriques du modèle, y compris les scores de pertinence.
6. Pour l'emplacement de destination du segment Lookalike, entrez le compartiment Amazon S3 dans lequel le segment Lookalike est exporté. Ce compartiment doit être situé dans la même région que vos autres ressources.
7. Pour l'accès au service, choisissez le nom du rôle de service existant qui sera utilisé pour accéder à cette table.

8. Pour la configuration avancée de la taille des bacs, choisissez la manière dont vous souhaitez configurer les tailles des bacs d'audience.
9. Sélectionnez Enregistrer les modifications.

Pour l'APIaction correspondante, voir UpdateConfiguredAudienceModel.

Utilisation de segments similaires (fournisseur de données de départ)

Création d'un segment similaire

Un segment similaire est un sous-ensemble des données d'apprentissage qui ressemble le plus aux données de départ.

Pour créer un segment similaire dans AWS Clean Rooms

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Dans l'onglet Avec adhésion active, choisissez une collaboration.
4. Dans l'onglet ML Modeling, choisissez Create lookalike segment.
5. Sur la page Créer un segment de similitude, pour Modèle de similitude configuré associé, choisissez le modèle de similitude configuré associé à utiliser pour ce segment de similitude.
6. Pour les détails du segment Lookalike, entrez un nom et une description facultative.
7. Pour les profils Seed, choisissez votre méthode Seed en sélectionnant une option, puis en prenant l'action recommandée.

Option	Action recommandée
Source d'entrée Amazon S3	1. Sélectionnez un emplacement Amazon S3. 2. (Facultatif) Choisissez Inclure les profils de départ dans la sortie.
SQLrequête	Rédigez une SQL requête et utilisez ses résultats comme données de départ,

Option	Action recommandée
Modèle d'analyse	Choisissez un modèle d'analyse dans la liste déroulante et utilisez les résultats créés par un modèle d'analyse.

8. Pour l'accès au service, choisissez le nom du rôle de service existant qui sera utilisé pour accéder à cette table.
9. Si vous souhaitez activer les balises pour le jeu de données d'entraînement, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
10. Choisissez Créer un segment similaire.

Pour l'APIaction correspondante, voir StartAudienceGenerationJob.

Exporter un segment similaire

Après avoir créé un segment similaire, vous pouvez exporter ces données vers un compartiment Amazon S3.

Pour exporter un segment similaire dans AWS Clean Rooms

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Dans l'onglet Avec adhésion active, choisissez une collaboration.
4. Dans l'onglet ML Modeling, sous Segments similaires, sélectionnez un segment similaire et choisissez Exporter.
5. Pour Exporter un modèle similaire, pour Exporter les détails du modèle similaire, entrez un nom et une description facultative.
6. Pour Taille du segment, choisissez la taille que vous souhaitez pour le segment exporté.
7. Cliquez sur Exporter.

Pour l'APIaction correspondante, voir StartAudienceExportJob.

Maintenant que vous avez créé un modèle similaire et exporté un segment de départ, vous êtes prêt à visualiser les données exportées dans S3.

Informatique cryptographique pour Clean Rooms

L'informatique cryptographique pour Clean Rooms (C3R) est une fonctionnalité AWS Clean Rooms qui peut être utilisée en plus des règles d'analyse. Avec C3R, les entreprises peuvent rassembler des données sensibles pour tirer de nouvelles informations de l'analyse des données tout en limitant cryptographiquement ce que les parties prenantes peuvent apprendre au cours du processus. Le C3R peut être utilisé par deux ou plusieurs parties qui souhaitent collaborer avec leurs données sensibles, mais doivent uniquement utiliser des données cryptées dans le cloud.

Le client de chiffrement C3R est un outil de chiffrement côté client que vous pouvez utiliser pour chiffrer vos données à utiliser. AWS Clean Rooms Lorsque vous utilisez le client de chiffrement C3R, les données restent protégées cryptographiquement pendant leur utilisation dans le cadre d'une AWS Clean Rooms collaboration. Comme dans le cas d'une AWS Clean Rooms collaboration normale, les données d'entrée sont des tables de base de données relationnelles, et le calcul est exprimé sous forme de requête SQL. Cependant, C3R ne prend en charge qu'un sous-ensemble limité de requêtes SQL sur des données chiffrées.

Plus précisément, C3R prend en charge le SQL JOIN et les SELECT instructions relatives aux données protégées par cryptographie. Chaque colonne de la table d'entrée peut être utilisée dans exactement l'un des types d'instructions SQL suivants :

- Les colonnes protégées par cryptographie pour être utilisées dans JOIN des instructions sont appelées fingerprintcolonnes.
- Les colonnes protégées par cryptographie pour être utilisées dans SELECT des instructions sont appelées sealedcolonnes.
- Les colonnes qui ne sont pas protégées cryptographiquement pour être utilisées dans SELECT des instructions JOIN OR sont appelées cleartextcolonnes.

Dans certains cas, les GROUP BY instructions sont prises en charge sur fingerprint des colonnes. Pour plus d'informations, consultez Fingerprintcolonnes. Actuellement, C3R ne prend pas en charge l'utilisation d'autres constructions SQL sur des données chiffrées, telles que des WHERE clauses ou des fonctions d'agrégation telles que SUM etAVERAGE, même si elles seraient autrement autorisées par les règles d'analyse pertinentes.

Le C3R est conçu pour protéger les données contenues dans les cellules individuelles d'un tableau. En utilisant la configuration par défaut de C3R, les données sous-jacentes qu'un client met à la disposition de tiers dans le cadre d'une collaboration restent cryptées tant que le contenu est utilisé

dans le cadre AWS Clean Rooms de cette collaboration. C3R utilise le cryptage AES-GCM standard pour toutes les sealed colonnes et une fonction pseudo-aléatoire standard, connue sous le nom de code d'authentification des messages basé sur le hachage (HMAC), pour protéger les colonnes. fingerprint

Même si C3R chiffre les données de vos tables, les informations suivantes peuvent toujours être déduites :

- Informations sur les tables elles-mêmes, notamment le nombre de colonnes, les noms des colonnes et le nombre de lignes de votre tableau.
- Comme pour la plupart des formes de chiffrement standard, C3R n'essaie pas de masquer la longueur des valeurs chiffrées. C3R offre la possibilité de compléter des valeurs chiffrées pour masquer la longueur exacte des textes en clair. Cependant, une limite supérieure de la longueur des textes en clair dans chaque colonne pourrait tout de même être révélée à une autre partie.
- Informations au niveau de la journalisation, telles que le moment où une ligne particulière a été ajoutée à une table C3R cryptée.

Pour plus d'informations sur le C3R, consultez les rubriques suivantes.

Rubriques

Considérations relatives à l'utilisation de l'informatique cryptographique pour Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) vise à optimiser la protection des données. Toutefois, certains cas d'utilisation peuvent bénéficier de niveaux inférieurs de protection des

données en échange de fonctionnalités supplémentaires. Vous pouvez faire ces compromis spécifiques en modifiant C3R à partir de sa configuration la plus sécurisée. En tant que client, vous devez être conscient de ces compromis et déterminer s'ils sont adaptés à votre cas d'utilisation. Les compromis à prendre en compte sont les suivants :

Rubriques

- Autoriser les données mixtes cleartext et cryptées dans vos tables
- Autoriser les valeurs répétées dans les fingerprint colonnes
- Assouplissement des restrictions relatives au fingerprint nom des colonnes
- Déterminer comment NULL les valeurs sont représentées

Pour plus d'informations sur la façon de définir les paramètres de ces scénarios, consultezParamètres de calcul cryptographique.

Autoriser les données mixtes cleartext et cryptées dans vos tables

Le chiffrement de toutes les données côté client garantit une protection maximale des données. Cela limite toutefois certains types de requêtes (par exemple, la fonction d'SUMagrégation). Le risque lié à l'autorisation des cleartext données est qu'il est possible que toute personne ayant accès aux tables cryptées puisse déduire certaines informations sur les valeurs cryptées. Cela pourrait être fait en effectuant une analyse statistique des données cleartext et des données associées.

Par exemple, imaginez que vous disposiez des colonnes de `City` et`State`. La `City` colonne est chiffrée cleartext et `State` elle est cryptée. Lorsque vous voyez la valeur `Chicago` dans la `City` colonne, cela vous permet de déterminer avec une forte probabilité que `State` c'est le cas`Illinois`. En revanche, si une colonne l'est `City` et l'autre l'est`EmailAddress`, il cleartext `City` est peu probable que a révèle quoi que ce soit à propos d'un chiffré`EmailAddress`.

Pour plus d'informations sur le paramètre de ce scénario, consultezParamètre Autoriser cleartext les colonnes.

Autoriser les valeurs répétées dans les fingerprint colonnes

Pour l'approche la plus sûre, nous supposons que chaque fingerprint colonne contient exactement une instance d'une variable. Aucun élément ne peut être répété dans une fingerprint colonne. Le client de chiffrement C3R mappe ces cleartext valeurs en valeurs uniques impossibles à distinguer des valeurs aléatoires. Il est donc impossible de déduire des informations les concernant à cleartext partir de ces valeurs aléatoires.

Le risque de valeurs répétées dans une fingerprint colonne est que les valeurs répétées se traduisent par des valeurs répétées d'apparence aléatoire. Ainsi, toute personne ayant accès aux tables cryptées pourrait, en théorie, effectuer une analyse statistique des fingerprint colonnes susceptible de révéler des informations sur cleartext les valeurs.

Encore une fois, supposons que la fingerprint colonne soit`State`, et que chaque ligne du tableau corresponde à un ménage américain. En effectuant une analyse de fréquence, on pourrait déduire quel état est `California` et lequel est `Wyoming` avec une probabilité élevée. Cette inférence est possible car il `California` compte beaucoup plus de résidents que. `Wyoming` En revanche, supposons que la fingerprint colonne porte sur un identifiant de ménage et que chaque ménage apparaisse dans la base de données entre 1 et 4 fois dans une base de données contenant des millions d'entrées. Il est peu probable qu'une analyse de fréquence révèle des informations utiles.

Pour plus d'informations sur le paramètre de ce scénario, consultezParamètre Autoriser les doublons.

Assouplissement des restrictions relatives au fingerprint nom des colonnes

Par défaut, nous supposons que lorsque deux tables sont jointes à l'aide de fingerprint colonnes chiffrées, ces colonnes portent le même nom dans chaque table. La raison technique de ce résultat est que, par défaut, nous dérivons une clé cryptographique différente pour chiffrer chaque fingerprint colonne. Cette clé est dérivée d'une combinaison de la clé secrète partagée pour la collaboration et du nom de colonne. Si nous essayons de joindre deux colonnes portant des noms de colonne différents, nous dérivons des clés différentes et nous ne pouvons pas calculer une jointure valide.

Pour résoudre ce problème, vous pouvez désactiver la fonctionnalité qui déduit les clés du nom de chaque colonne. Le client de chiffrement C3R utilise ensuite une clé dérivée unique pour toutes les fingerprint colonnes. Le risque est qu'un autre type d'analyse de fréquence puisse être effectué qui pourrait révéler des informations.

Utilisons à nouveau l'`State`exemple `City` et. Si nous dérivons les mêmes valeurs aléatoires pour chaque fingerprint colonne (en n'incorporant pas le nom de la colonne). `New York`possède la même valeur aléatoire dans les `State` colonnes `City` et. New York est l'une des rares villes des États-Unis où le `City` nom est le même que le `State` nom. En revanche, si votre ensemble de données contient des valeurs complètement différentes dans chaque colonne, aucune information n'est divulguée.

Pour plus d'informations sur le paramètre de ce scénario, consultezParamètre JOIN d'autorisation des colonnes avec des noms différents.

Déterminer comment NULL les valeurs sont représentées

L'option qui s'offre à vous est de savoir s'il faut traiter les NULL valeurs de manière cryptographique (chiffrement et HMAC) comme toute autre valeur. Si vous ne traitez pas NULL les valeurs comme les autres valeurs, des informations peuvent être révélées.

Supposons, par exemple, que NULL la `Middle Name` colonne cleartext indique les personnes sans deuxième prénom. Si vous ne chiffrez pas ces valeurs, vous divulguez les lignes de la table cryptée qui sont utilisées pour les personnes sans deuxième prénom. Ces informations peuvent être un signal d'identification pour certaines personnes dans certaines populations. Mais si vous traitez des NULL valeurs de manière cryptographique, certaines requêtes SQL agissent différemment. Par exemple, les GROUP BY clauses ne regrouperont pas fingerprint NULL les valeurs dans fingerprint des colonnes.

Pour plus d'informations sur le paramètre de ce scénario, consultezParamètre de conservation NULL des valeurs.

Types de fichiers et de données pris en charge dans Cryptographic Computing pour Clean Rooms

Le client de chiffrement C3R reconnaît les types de fichiers suivants :

- fichiers CSV
- Parquetfichiers

Vous pouvez utiliser l'`--fileFormat`indicateur du client de chiffrement C3R pour spécifier un format de fichier de manière explicite. Lorsqu'il est explicitement spécifié, le format de fichier n'est pas déterminé par l'extension du fichier.

Rubriques

- fichiers CSV
- Parquetfichiers
- Chiffrement de valeurs autres que des chaînes

fichiers CSV

Un fichier portant une extension .csv est supposé être au format CSV et contenir du texte codé en UTF-8. Le client de chiffrement C3R traite toutes les valeurs comme des chaînes.

Propriétés prises en charge dans les fichiers .csv

Le client de chiffrement C3R nécessite que les fichiers .csv possèdent les propriétés suivantes :

- Peut contenir ou non une ligne d'en-tête initiale qui nomme chaque colonne de manière unique.
- Délimité par des virgules. (Actuellement, les délimiteurs personnalisés ne sont pas pris en charge.)
- Texte codé en UTF-8.

Suppression des espaces blancs dans les entrées .csv

Les espaces blancs de début et de fin sont supprimés des entrées .csv.

NULLEncodage personnalisé pour un fichier .csv

Un fichier .csv peut utiliser un NULL encodage personnalisé.

Avec le client de chiffrement C3R, vous pouvez spécifier des codages personnalisés pour les NULL entrées dans les données d'entrée à l'aide de l'`--csvInputNULLValue=<csv-input-null>`indicateur. Le client de chiffrement C3R peut utiliser des encodages personnalisés dans le fichier de sortie généré pour les entrées NULL à l'aide de l'`--csvOutputNULLValue=<csv-output-null>`indicateur.

> **Note**
>
> Une NULL entrée est considérée comme manquant de contenu, en particulier dans le contexte d'un format tabulaire plus riche tel qu'un tableau SQL. Bien que le format .csv ne prenne pas explicitement en charge cette caractérisation pour des raisons historiques, il est courant de considérer qu'une entrée vide contenant uniquement des espaces blancs est considérée NULL comme telle. Il s'agit donc du comportement par défaut du client de chiffrement C3R et il peut être personnalisé selon les besoins.

Comment les entrées .csv sont interprétées par C3R

Le tableau suivant fournit des exemples de la manière dont les entrées .csv sont rassemblées (cleartextcleartextpour plus de clarté) en fonction des valeurs (le cas échéant) fournies pour les indicateurs `--csvInputNULLValue=<csv-input-null>` et`--csvOutputNULLValue=<csv-output-null>`. Les espaces blancs de début et de fin situés en dehors des guillemets sont supprimés avant que C3R n'interprète le sens d'une valeur.

<csv-input-null>	**<csv-output-null>**	Entrée d'entrée	Entrée de sortie
Aucun	Aucun	`,AnyProduct,`	`,AnyProduct,`
Aucun	Aucun	`, AnyProduct ,`	`,AnyProduct,`
Aucun	Aucun	`,"AnyProduct",`	`,AnyProduct,`
Aucun	Aucun	`, "AnyProduct" ,`	`,AnyProduct,`
Aucun	Aucun	`,,`	`,,`
Aucun	Aucun	`, ,`	`,,`
Aucun	Aucun	`,"",`	`,,`
Aucun	Aucun	`," ",`	`," ",`
Aucun	Aucun	`, " " ,`	`," ",`
`"AnyProduct"`	`"NULL"`	`,AnyProduct,`	`,NULL,`
`"AnyProduct"`	`"NULL"`	`, AnyProduct ,`	`,NULL,`
`"AnyProduct"`	`"NULL"`	`,"AnyProduct",`	`,NULL,`
`"AnyProduct"`	`"NULL"`	`, "AnyProduct" ,`	`,NULL,`
Aucun	`"NULL"`	`,,`	`,NULL,`

<csv-input-null>	**<csv-output-null>**	Entrée d'entrée	Entrée de sortie
Aucun	"NULL"	, ,	,NULL,
Aucun	"NULL"	,"",	,NULL,
Aucun	"NULL"	," ",	," ",
Aucun	"NULL"	, " " ,	," ",
""	"NULL"	,,	,NULL,
""	"NULL"	, ,	,NULL,
""	"NULL"	,"",	,"",
""	"NULL"	," ",	," ",
""	"NULL"	, " " ,	," ",
"\"\""	"NULL"	,,	,,
"\"\""	"NULL"	, ,	,,
"\"\""	"NULL"	,"",	,NULL,
"\"\""	"NULL"	," ",	," ",
"\"\""	"NULL"	, " " ,	," ",

Fichier CSV sans en-têtes

Il n'est pas nécessaire que le fichier .csv source comporte des en-têtes dans la première ligne qui nomment chaque colonne de manière unique. Toutefois, un fichier .csv sans ligne d'en-tête nécessite un schéma de chiffrement positionnel. Le schéma de chiffrement positionnel est requis au lieu du schéma mappé classique utilisé à la fois pour les fichiers .csv avec une ligne d'en-tête et pour les fichiers. Parquet

Un schéma de chiffrement positionnel spécifie les colonnes de sortie par position plutôt que par nom. Un schéma de chiffrement mappé associe les noms des colonnes source aux noms des colonnes

cibles. Pour plus d'informations, notamment une discussion détaillée et des exemples des deux formats de schéma, consultezSchémas de tables cartographiées et positionnelles.

Parquetfichiers

Un fichier avec une .parquet extension est supposé être au Apache Parquet format.

Types de Parquet données pris en charge

Le client de chiffrement C3R peut traiter toutes les données non complexes (c'est-à-dire de type primitif) dans un Parquet fichier qui représente un type de données pris en charge par. AWS Clean Rooms

Toutefois, seules les colonnes de chaîne peuvent être utilisées pour les sealed colonnes.

Les types de données Parquet suivants sont pris en charge :

- `Binary`type primitif avec les annotations logiques suivantes :
  - Aucun si le `--parquetBinaryAsString` est défini (type de `STRING` données)
  - `Decimal(scale, precision)`(type de `DECIMAL` données)
  - `String`(type de `STRING` données)
- `Boolean`type de données primitif sans annotation logique (type de `BOOLEAN` données)
- `Double`type de données primitif sans annotation logique (type de `DOUBLE` données)
- `Fixed_Len_Binary_Array`type primitif avec annotation `Decimal(scale, precision)` logique (type de `DECIMAL` données)
- `Float`type de données primitif sans annotation logique (type de `FLOAT` données)
- `Int32`type primitif avec les annotations logiques suivantes :
  - Aucun (type de `INT` données)
  - `Date`(type de `DATE` données)
  - `Decimal(scale, precision)`(type de `DECIMAL` données)
  - `Int(16, true)`(type de `SMALLINT` données)
  - `Int(32, true)`(type de `INT` données)
- `Int64`type de données primitif avec les annotations logiques suivantes :
  - Aucun (type de `BIGINT` données)
  - `Decimal(scale, precision)`(type de `DECIMAL` données)

- `Int(64, true)`(type de `BIGINT` données)
- `Timestamp(isUTCAdjusted, TimeUnit.MILLIS)`(type de `TIMESTAMP` données)
- `Timestamp(isUTCAdjusted, TimeUnit.MICROS)`(type de `TIMESTAMP` données)
- `Timestamp(isUTCAdjusted, TimeUnit.NANOS)`(type de `TIMESTAMP` données)

Chiffrement de valeurs autres que des chaînes

Actuellement, seules les valeurs de chaîne sont prises en charge pour les sealed colonnes.

Pour les fichiers .csv, le client de chiffrement C3R traite toutes les valeurs comme du texte codé en UTF-8 et ne tente pas de les interpréter différemment avant le chiffrement.

Pour les colonnes d'empreintes digitales, les types sont regroupés en classes d'équivalence. Une classe d'équivalence est un ensemble de types de données dont l'égalité peut être comparée sans ambiguïté via un type de données représentatif.

Les classes d'équivalence permettent d'attribuer des empreintes identiques à la même valeur sémantique, quelle que soit la représentation d'origine. Cependant, la même valeur dans deux classes d'équivalence ne produira pas la même colonne d'empreintes digitales.

Par exemple, la même empreinte digitale `42` sera attribuée à la `INTEGRAL` valeur, qu'il s'agisse à l'origine d'un `SMALLINTINT`, ou`BIGINT`. De plus, la `INTEGRAL` valeur ne `0` correspondra jamais à la `BOOLEAN` valeur `FALSE` (qui est représentée par la valeur`0`).

Les classes d'équivalence suivantes et les types de AWS Clean Rooms données correspondants sont pris en charge par les colonnes d'empreintes digitales :

Classe d'équivalence	Type de AWS Clean Rooms données pris en charge
`BOOLEAN`	`BOOLEAN`
`DATE`	`DATE`
`INTEGRAL`	`BIGINT`, `INT`, `SMALLINT`
`STRING`	`CHAR`, `STRING`, `VARCHAR`

Noms de colonnes dans Cryptographic Computing pour Clean Rooms

Par défaut, les noms des colonnes sont importants dans Cryptographic Computing forClean Rooms.

Si la valeur du paramètre Autoriser les colonnes avec JOIN des noms différents est fausse, les noms des colonnes sont utilisés lors du chiffrement des fingerprint colonnes. C'est pourquoi, par défaut, les collaborateurs doivent se coordonner à l'avance et utiliser les mêmes noms de colonnes cibles pour les données qui utiliseront JOIN des instructions dans les requêtes. Par défaut, les colonnes chiffrées JOIN avec des noms différents ne fonctionnent avec succès JOIN sur aucune valeur.

Si la valeur du paramètre Autoriser les colonnes avec JOIN des noms différents est vraie, les JOIN instructions entre colonnes chiffrées en tant que fingerprint colonnes aboutissent. Le chiffrement des données avec ce paramètre peut permettre une certaine inférence des cleartext valeurs. Par exemple, si une ligne possède la même valeur de code d'authentification de message basé sur le hachage (HMAC) à la fois dans la `City` colonne et dans la `State` colonne, la valeur peut être. `New York`

Normalisation des noms d'en-têtes de colonnes

Les noms des en-têtes de colonnes sont normalisés par le client de chiffrement C3R. Tous les espaces blancs de début et de fin sont supprimés et le nom de la colonne est mis en minuscules pour la sortie transformée.

La normalisation est appliquée avant tous les autres calculs, calculs ou autres opérations susceptibles d'être affectés par les noms de colonnes. Le fichier de sortie émis contient uniquement les noms normalisés.

Types de colonnes dans le calcul cryptographique pour Clean Rooms

Cette rubrique fournit des informations sur les types de colonnes dans Cryptographic Computing forClean Rooms.

Rubriques

- Fingerprintcolonnes
- Colonnes étanches

- Cleartextcolonnes

Fingerprintcolonnes

Fingerprintles colonnes sont des colonnes protégées cryptographiquement pour être utilisées dans JOIN des instructions.

Les données des fingerprint colonnes ne peuvent pas être déchiffrées. Seules les données provenant de colonnes scellées peuvent être déchiffrées.

Fingerprintles colonnes ne doivent être utilisées que dans les clauses et fonctions SQL suivantes :

- JOIN (INNER, OUTER, LEFT, RIGHT, or FULL)par rapport aux autres fingerprint colonnes :
  - Si la valeur du `allowJoinsOnColumnsWithDifferentNames` paramètre est définie sur`false`, les deux fingerprint colonnes du JOIN doivent également porter le même nom.
- `SELECT COUNT()`
- `SELECT COUNT(DISTINCT )`
- `GROUP BY`(À utiliser uniquement si la collaboration a défini la valeur du `preserveNulls` paramètre sur`true`.)

Les requêtes qui enfreignent ces contraintes peuvent donner des résultats incorrects.

Colonnes étanches

Les colonnes scellées sont des colonnes protégées cryptographiquement pour être utilisées dans SELECT des instructions.

Les colonnes scellées ne doivent être utilisées que dans les clauses et fonctions SQL suivantes :

- `SELECT`
- `SELECT ... AS`
- `SELECT COUNT()`

> **Note**
>
> `SELECT COUNT(DISTINCT )` n'est pas pris en charge.

Les requêtes qui enfreignent ces contraintes peuvent donner des résultats incorrects.

Remplissage des données pour une sealed colonne avant le chiffrement

Lorsque vous spécifiez qu'une colonne doit être une sealed colonne, C3R vous demande quel type de rembourrage choisir. Le remplissage des données avant le chiffrement est facultatif. Sans rembourrage (type de padnone), la longueur des données cryptées indique la taille ducleartext. Dans certaines circonstances, la taille du cleartext peut exposer le texte en clair. Avec le rembourrage (un pad de type `fixed` ou`max`), toutes les valeurs sont d'abord rembourrées à une taille commune, puis cryptées. Avec le rembourrage, la longueur des données cryptées ne fournit aucune information sur la cleartext longueur d'origine, si ce n'est le fait de donner une limite supérieure à sa taille.

Si vous souhaitez un remplissage pour une colonne et que la longueur maximale en octets des données de cette colonne est connue, utilisez le `fixed` rembourrage. Utilisez une `length` valeur au moins égale à la longueur en octets de la valeur la plus longue de cette colonne.

> **Note**
>
> Une erreur se produit et le chiffrement échoue si une valeur est supérieure à la valeur fournie`length`.

Si vous souhaitez un remplissage pour une colonne et que la longueur maximale en octets des données de cette colonne n'est pas connue, utilisez le `max` rembourrage. Ce mode de remplissage rembourre toutes les données à la longueur de la valeur la plus longue plus des `length` octets supplémentaires.

> **Note**
>
> Vous souhaiterez peut-être chiffrer les données par lots ou mettre régulièrement à jour vos tables avec de nouvelles données. Sachez que le `max` remplissage remplira les entrées à la longueur (plus l'`length`octet) de l'entrée en texte brut la plus longue d'un lot donné. Cela signifie que la longueur du texte chiffré peut varier d'un lot à l'autre. Par conséquent, si vous connaissez la longueur maximale en octets d'une colonne, vous devez utiliser à la `fixed` place de. `max`

Cleartextcolonnes

Cleartextles colonnes sont des colonnes qui ne sont pas protégées cryptographiquement pour être utilisées dans SELECT des instructions JOIN or.

Cleartextles colonnes peuvent être utilisées dans n'importe quelle partie de la requête SQL.

Paramètres de calcul cryptographique

Les paramètres de calcul cryptographique sont disponibles pour les collaborations utilisant Cryptographic Computing for Clean Rooms (C3R) lors de la création d'une collaboration. Vous pouvez créer une collaboration à l'aide de la AWS Clean Rooms console ou de l'`CreateCollaboration`API. Dans la console, vous pouvez définir des valeurs pour les paramètres dans Paramètres de calcul cryptographique après avoir activé l'option Support de calcul cryptographique. Pour plus d'informations, consultez les rubriques suivantes.

Rubriques

- Paramètre Autoriser cleartext les colonnes
- Paramètre Autoriser les doublons
- Paramètre JOIN d'autorisation des colonnes avec des noms différents
- Paramètre de conservation NULL des valeurs

Paramètre Autoriser cleartext les colonnes

Dans la console, vous pouvez définir le paramètre Autoriser les cleartext colonnes lors de la création d'une collaboration afin de spécifier si cleartext les données sont autorisées dans une table contenant des données chiffrées.

Le tableau suivant décrit les valeurs du paramètre Autoriser cleartext les colonnes.

Valeur de paramètre	Description
Non	Cleartextles colonnes ne sont pas autorisées dans la table cryptée. Toutes les données sont protégées par cryptographie.
Oui	Cleartextles colonnes sont autorisées dans la table cryptée.

Valeur de paramètre	Description
	Cleartextles colonnes ne sont pas protégées par cryptographie et sont incluses en tant quecleartext. Vous devez prendre note de ce que les cleartext données de vos lignes peuvent révéler à propos des autres données du tableau. Pour fonctionner SUM ou AVG sur des colonnes spécifiques, les colonnes doivent être insérées cleartext.

À l'aide de l'opération `CreateCollaboration` API, pour le `dataEncryptionMetadata` paramètre, vous pouvez définir la valeur de `allowCleartext` to `true` ou`false`. Pour plus d'informations sur les opérations d'API, consultez la référence des AWS Clean Rooms API.

Cleartextles colonnes correspondent aux colonnes classées selon le schéma spécifique cleartext à la table. Les données de ces colonnes ne sont pas cryptées et peuvent être utilisées de quelque manière que ce soit. Cleartextles colonnes peuvent être utiles si les données ne sont pas sensibles et/ou si une plus grande flexibilité est requise par rapport à une sealed colonne ou à une fingerprint colonne cryptée.

Paramètre Autoriser les doublons

Dans la console, vous pouvez définir le paramètre Autoriser les doublons lors de la création d'une collaboration afin de spécifier si les colonnes chiffrées pour les JOIN requêtes peuvent contenir des NULL non-valeurs dupliquées.

> **Important**
>
> Les paramètres Autoriser les doublons, Autoriser les colonnes portant JOIN des noms différents et Préserver NULL les valeurs ont des effets distincts mais connexes.

Le tableau suivant décrit les valeurs du paramètre Autoriser les doublons.

Valeur de paramètre	Description
Non	Les valeurs répétées ne sont pas autorisées dans une fingerprint colonne. Toutes les valeurs d'une seule fingerprint colonne doivent être uniques.
Oui	Les valeurs répétées sont autorisées dans une fingerprint colonne. Si vous devez joindre des colonnes contenant des valeurs répétées, définissez cette valeur sur Oui. Lorsque cette option est définie sur Oui, les modèles de fréquence apparaissant dans les fingerprint colonnes de la table C3R ou des résultats peuvent impliquer des informations supplémentaires sur la structure des cleartext données.

À l'aide de l'opération `CreateCollaboration` API, pour le `dataEncryptionMetadata` paramètre, vous pouvez définir la valeur de `allowDuplicates` to `true` ou`false`. Pour plus d'informations sur les opérations d'API, consultez la référence des AWS Clean Rooms API.

Par défaut, si des données chiffrées doivent être utilisées dans les JOIN requêtes, le client de chiffrement C3R exige que ces colonnes ne contiennent aucune valeur dupliquée. Cette exigence vise à renforcer la protection des données. Ce comportement permet de garantir que les modèles répétés dans les données ne sont pas observables. Toutefois, si vous souhaitez utiliser des données chiffrées dans des JOIN requêtes et que vous n'êtes pas préoccupé par les valeurs dupliquées, le paramètre Autoriser les doublons peut désactiver cette vérification conservatrice.

Paramètre JOIN d'autorisation des colonnes avec des noms différents

Dans la console, vous pouvez définir le paramètre Autoriser les colonnes JOIN portant des noms différents lors de la création d'une collaboration afin de spécifier si les JOIN instructions entre des colonnes portant des noms différents sont prises en charge.

Pour plus d'informations, consultez Normalisation des noms d'en-têtes de colonnes .

Le tableau suivant décrit les valeurs du paramètre Autoriser JOIN les colonnes portant des noms différents.

Valeur de paramètre	Description
Non	Les jointures de fingerprint colonnes portant des noms différents ne sont pas prises en charge. JOINles instructions ne fournissent des résultats précis que pour les colonnes portant le même nom. **Important** La valeur Non renforce la sécurité des informations mais oblige les participants à la collaboration à se mettre d'accord au préalable sur les noms des colonnes. Si deux colonnes portent des noms différents lorsqu'elles sont cryptées sous forme JOINde fingerprint colonnes et que l'option Autoriser les colonnes portant des noms différents est définie sur Non, les JOIN instructions sur ces colonnes ne produisent aucun résultat. Cela est dû au fait qu'aucune valeur n'est partagée entre eux après le chiffrement.
Oui	Les jointures de fingerprint colonnes portant des noms différents sont prises en charge. Pour plus de flexibilité, les utilisateurs peuvent définir cette valeur sur Oui, ce qui autorise les JOIN instructions sur les colonnes quel que soit le nom de la colonne. S'il est défini sur Oui, le client de chiffrement C3R ne prend pas en compte le nom de colonne lors de la protection des fingerprint colonnes. Par conséquent, les valeurs communes aux différentes fingerprint colonnes sont observables dans le tableau C3R. Par exemple, si une ligne possède la même JOIN valeur chiffrée à la fois dans une `City` colonne et dans une `State` colonne, il peut être raisonnable de déduire que cette valeur est `New York` la même.

À l'aide de l'opération `CreateCollaboration` API, pour le `dataEncryptionMetadata` paramètre, vous pouvez définir la valeur de `allowJoinsOnColumnsWithDifferentNames` to `true` ou`false`. Pour plus d'informations sur les opérations d'API, consultez la référence des AWS Clean Rooms API.

Par défaut, le chiffrement des fingerprint colonnes est affecté par le `targetHeader` paramètre pour cette colonne, défini dansÉtape 4 : générer un schéma de chiffrement pour un fichier tabulaire . Par conséquent, la même cleartext valeur possède des représentations cryptées différentes dans chaque fingerprint colonne pour laquelle elle est cryptée.

Ce paramètre peut être utile pour empêcher l'inférence de cleartext valeurs dans certains cas. Par exemple, le fait de voir la même valeur cryptée dans `City` des fingerprint colonnes `State` peut être utilisé pour déduire raisonnablement que la valeur est`New York`. Cependant, l'utilisation de ce paramètre nécessite une coordination supplémentaire à l'avance, de sorte que toutes les colonnes à joindre dans les requêtes portent des noms communs.

Vous pouvez utiliser le paramètre Autoriser JOIN les colonnes portant des noms différents pour assouplir cette restriction. Lorsque la valeur du paramètre est définie sur`Yes`, toutes les colonnes cryptées peuvent JOIN être utilisées ensemble, quel que soit leur nom.

Paramètre de conservation NULL des valeurs

Dans la console, vous pouvez définir le paramètre Conserver NULL les valeurs lors de la création d'une collaboration pour indiquer qu'aucune valeur n'est présente pour cette colonne.

Le tableau suivant décrit les valeurs du paramètre Conserver NULL les valeurs.

Valeur de paramètre	Description
Non	NULLles valeurs ne sont pas préservées. NULLles valeurs n'apparaissent pas comme NULL dans une table cryptée. NULLles valeurs apparaissent sous forme de valeurs aléatoire s uniques dans une table C3R.
Oui	NULLles valeurs sont préservées. NULLles valeurs apparaiss ent comme NULL dans une table cryptée. Si vous avez besoin d'une sémantique SQL pour les NULL valeurs, vous pouvez définir cette valeur sur Oui. Par conséquent, NULL les entrées

Valeur de paramètre	Description
	apparaissent comme NULL dans la table C3R, que la colonne soit cryptée ou non et quel que soit le paramètre défini pour Autoriser les doublons.

À l'aide de l'opération `CreateCollaboration` API, pour le `dataEncryptionMetadata` paramètre, vous pouvez définir la valeur de `preserveNulls` to `true` ou`false`. Pour plus d'informations sur les opérations d'API, consultez la référence des AWS Clean Rooms API.

Lorsque le paramètre Conserver NULL les valeurs est défini sur Non pour la collaboration :

1. NULLles entrées dans `cleartext` les colonnes restent inchangées.
2. NULLles entrées dans les `fingerprint` colonnes cryptées sont cryptées sous forme de valeurs aléatoires afin de masquer leur contenu. Le fait de rejoindre une colonne cryptée avec des NULL entrées dans la cleartext colonne ne produit aucune correspondance pour aucune des NULL entrées. Aucune correspondance n'est établie car ils reçoivent chacun leur propre contenu aléatoire unique.
3. NULLles entrées dans les `sealed` colonnes cryptées sont cryptées.

Lorsque la valeur du paramètre Conserver les NULL valeurs est définie sur Oui pour la collaboration, les NULL entrées de toutes les colonnes restent inchangées, que la colonne NULL soit cryptée ou non.

Le paramètre Conserver NULL les valeurs est utile dans des scénarios tels que l'enrichissement des données, dans lesquels vous souhaitez partager un manque d'informations exprimé sous la formeNULL. Le paramètre Conserver NULL les valeurs est également utile au fingerprint format HMAC si vous avez des NULL valeurs dans la colonne que vous souhaitez JOIN ouGROUP BY.

Si la valeur des paramètres Autoriser les doublons et Préserver NULL les valeurs est définie sur Non, la présence de plusieurs NULL entrées dans une fingerprint colonne génère une erreur et arrête le chiffrement. Si la valeur de l'un des paramètres est définie sur Oui, aucune erreur de ce type ne se produit.

Drapeaux facultatifs dans le calcul cryptographique pour Clean Rooms

Les sections suivantes décrivent les indicateurs facultatifs que vous pouvez définir lorsque vous cryptez des données à l'aide du client de chiffrement C3R pour personnaliser et tester des fichiers tabulaires.

Rubriques

`--csvInputNULLValue`drapeau

Vous pouvez utiliser l'`--csvInputNULLValue`indicateur pour spécifier des codages personnalisés pour les NULL entrées dans les données d'entrée lorsque vous cryptez des données à l'aide du client de chiffrement C3R.

Le tableau suivant récapitule l'utilisation et les paramètres de cet indicateur.

Utilisation	Paramètres
Facultatif. Les utilisateurs peuvent spécifier des codages personnalisés pour les NULL entrées dans les données d'entrée.	Encodage des NULL valeurs défini par l'utilisa teur dans le fichier CSV d'entrée

Une NULL entrée est une entrée considérée comme manquant de contenu, en particulier dans le contexte d'un format tabulaire plus riche tel qu'un tableau SQL. Bien que le format .csv ne prenne pas explicitement en charge cette caractérisation pour des raisons historiques, il est courant de considérer qu'une entrée vide contenant uniquement des espaces blancs l'est. NULL Il s'agit donc du comportement par défaut du client de chiffrement C3R et il peut être personnalisé selon les besoins.

`--csvOutputNULLValue`drapeau

Vous pouvez utiliser l'`--csvOutputNULLValue`indicateur pour spécifier des codages personnalisés pour les NULL entrées dans les données de sortie lorsque vous cryptez des données à l'aide du client de chiffrement C3R.

Le tableau suivant récapitule l'utilisation et les paramètres de cet indicateur.

Utilisation	Paramètres
Facultatif. Les utilisateurs peuvent spécifier des encodages personnalisés dans le fichier de sortie généré pour les NULL entrées.	Encodage des NULL valeurs défini par l'utilisa teur dans le fichier CSV de sortie

Une NULL entrée est une entrée considérée comme manquant de contenu, en particulier dans le contexte d'un format tabulaire plus riche tel qu'un tableau SQL. Bien que le format .csv ne prenne pas explicitement en charge cette caractérisation pour des raisons historiques, il est courant de considérer qu'une entrée vide contenant uniquement des espaces blancs l'est. NULL Il s'agit donc du comportement par défaut du client de chiffrement C3R et il peut être personnalisé selon les besoins.

`--enableStackTraces`drapeau

Lorsque vous chiffrez des données à l'aide du client de chiffrement C3R, utilisez l'`--enableStackTraces`indicateur pour fournir des informations contextuelles supplémentaires afin de signaler les erreurs lorsque C3R rencontre une erreur.

AWS ne collecte pas les erreurs. Si vous rencontrez une erreur, utilisez le stack trace pour résoudre vous-même l'erreur ou envoyez le stack trace à AWS Support pour obtenir de l'aide.

Le tableau suivant récapitule l'utilisation et les paramètres de cet indicateur.

Utilisation	Paramètres
Facultatif. Utilisé pour fournir des informations contextuelles supplémentaires afin de signaler les erreurs lorsque le client de chiffrement C3R rencontre une erreur.	Aucun

`--dryRun`drapeau

Les commandes du client de chiffrement C3R crypter et déchiffrer incluent un indicateur facultatif. `--dryRun` L'indicateur prend tous les arguments fournis par l'utilisateur et vérifie leur validité et leur cohérence.

Vous pouvez utiliser l'`--dryRun`indicateur pour vérifier si votre fichier de schéma est valide et cohérent avec le fichier d'entrée correspondant.

Le tableau suivant récapitule l'utilisation et les paramètres de cet indicateur.

Utilisation	Paramètres
Facultatif. Demande au client de chiffrement C3R d'analyser les paramètres et de vérifier les fichiers, mais n'effectue aucun chiffrement ni déchiffrement.	Aucun

`--tempDir`drapeau

Vous pouvez utiliser un répertoire temporaire car les fichiers chiffrés peuvent parfois être plus volumineux que les fichiers non chiffrés, en fonction de leurs paramètres. Les ensembles de données doivent également être chiffrés par collaboration pour fonctionner correctement.

Lorsque vous chiffrez des données à l'aide de C3R, utilisez l'`--tempDir`indicateur pour spécifier l'emplacement où les fichiers temporaires peuvent être créés lors du traitement de l'entrée.

Le tableau suivant récapitule l'utilisation et les paramètres de cet indicateur.

Utilisation	Paramètres
Les utilisateurs peuvent spécifier l'emplacement où les fichiers temporaires peuvent être créés lors du traitement de l'entrée.	Par défaut, c'est le répertoire temporaire du système.

Requêtes avec calcul cryptographique pour Clean Rooms

Cette rubrique fournit des informations sur l'écriture de requêtes utilisant des tables de données chiffrées à l'aide de l'informatique cryptographique pourClean Rooms.

Rubriques

Requêtes qui se rattachent à NULL

Avoir une branche de requête sur une NULL instruction signifie utiliser une syntaxe similaire à`IF x IS NULL THEN 0 ELSE 1`.

Les requêtes peuvent toujours se baser sur NULL des instructions en cleartext colonnes.

Les requêtes peuvent se baser sur NULL des instructions en sealed fingerprint colonnes et en colonnes uniquement lorsque la valeur du paramètre Conserver les valeurs NULL (`preserveNulls`) est définie sur`true`.

Les requêtes qui enfreignent ces contraintes peuvent donner des résultats incorrects.

Mappage d'une colonne source vers plusieurs colonnes cibles

Une colonne source peut être mappée à plusieurs colonnes cibles. Par exemple, vous pouvez vouloir les deux JOIN et SELECT sur une colonne.

Pour plus d'informations, consultez Utiliser les mêmes données pour JOIN les deux SELECT requêtes.

Utiliser les mêmes données pour JOIN les deux SELECT requêtes

Si les données d'une colonne ne sont pas sensibles, elles peuvent apparaître dans une colonne cleartext cible, ce qui permet de les utiliser à n'importe quelle fin.

Si les données d'une colonne sont sensibles et doivent être utilisées à la fois pour les SELECT requêtes JOIN et, mappez cette colonne source à deux colonnes cibles dans le fichier de sortie. Une

colonne est chiffrée avec la colonne `type` sous forme de fingerprint colonne, et une colonne est chiffrée avec la colonne `type` sous forme de colonne scellée. La génération de schéma interactive du client de chiffrement C3R suggère des suffixes d'en-tête de et. `_fingerprint` `_sealed` Ces suffixes d'en-tête peuvent constituer une convention utile pour différencier rapidement de telles colonnes.

Directives pour le client de chiffrement C3R

Le client de chiffrement C3R est un outil qui permet aux entreprises de rassembler des données sensibles afin de tirer de nouvelles informations de l'analyse des données. L'outil limite cryptographiquement ce qui peut être appris par n'importe quelle partie et AWS au cours du processus. Bien que cela soit d'une importance vitale, le processus de sécurisation cryptographique des données peut entraîner une surcharge importante en termes de ressources de calcul et de stockage. Il est donc important de comprendre les inconvénients liés à l'utilisation de chaque paramètre et de savoir comment optimiser les paramètres tout en maintenant les garanties cryptographiques souhaitées. Cette rubrique se concentre sur les implications en termes de performances des différents paramètres du client et des schémas de chiffrement C3R.

Tous les paramètres de chiffrement du client de chiffrement C3R fournissent des garanties cryptographiques différentes. Les paramètres de collaboration sont les plus sécurisés par défaut. L'activation de fonctionnalités supplémentaires lors de la création d'une collaboration affaiblit les garanties de confidentialité, ce qui permet d'effectuer des activités telles que l'analyse des fréquences sur le texte chiffré. Pour plus d'informations sur la manière dont ces paramètres sont utilisés et sur leurs implications, consultezInformatique cryptographique.

Rubriques

- Implications sur les performances pour les types de colonnes
- Résolution des problèmes liés aux augmentations imprévues de la taille du texte chiffré

Implications sur les performances pour les types de colonnes

C3R utilise trois types de colonnes : cleartextfingerprint, etsealed. Chacun de ces types de colonnes fournit des garanties cryptographiques différentes et a des utilisations prévues différentes. Dans les sections suivantes, les implications du type de colonne sur les performances sont abordées ainsi que l'impact de chaque paramètre sur les performances.

Rubriques

- Cleartextcolonnes
- Fingerprintcolonnes
- Sealedcolonnes

Cleartextcolonnes

Cleartextles colonnes ne sont pas modifiées par rapport à leur format d'origine et ne sont en aucun cas traitées cryptographiquement. Ce type de colonne ne peut pas être configuré et n'a aucune incidence sur les performances de stockage ou de calcul.

Fingerprintcolonnes

Fingerprintles colonnes sont destinées à être utilisées pour joindre des données sur plusieurs tables. À cette fin, la taille du texte chiffré obtenu doit toujours être la même. Toutefois, ces colonnes sont affectées par les paramètres de collaboration. Fingerprintles colonnes peuvent avoir différents degrés d'impact sur la taille du fichier de sortie en fonction du cleartext contenu de l'entrée.

Rubriques

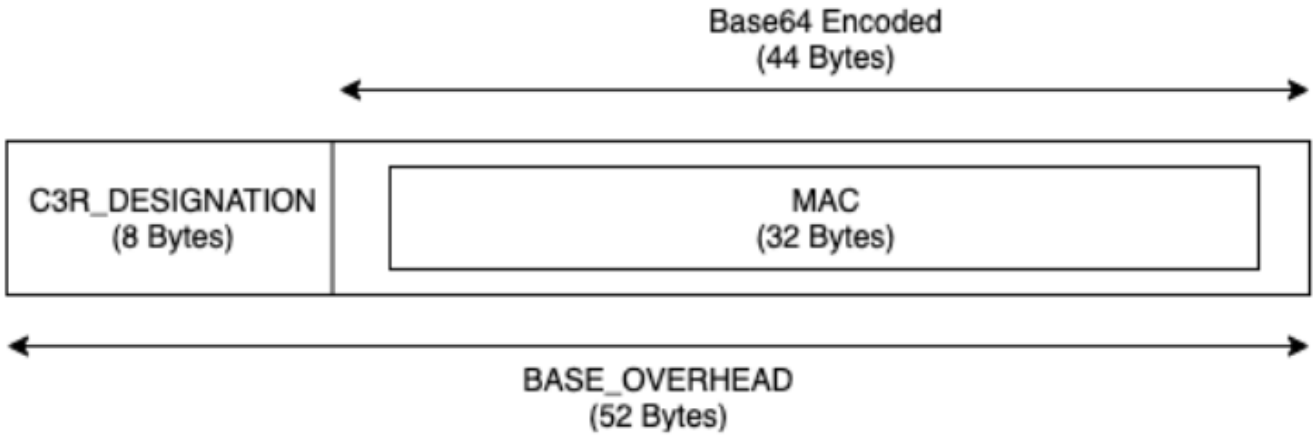
- Frais généraux de base pour les fingerprint colonnes
- Paramètres de collaboration pour les fingerprint colonnes
- Exemple de données pour une fingerprint colonne
- fingerprintColonnes de dépannage

Frais généraux de base pour les fingerprint colonnes

Il existe un surcoût de base pour les fingerprint colonnes. Cette surcharge est constante et remplace la taille des cleartext octets.

Les données des fingerprint colonnes sont traitées cryptographiquement par le biais d'une fonction HMAC (Hash Based Message Authentication Code), qui transforme les données en un code d'authentification de message (MAC) de 32 octets. Ces données sont ensuite traitées via un encodeur base64, ce qui ajoute environ 33 % à la taille des octets. Il est précédé d'une désignation C3R à 8 octets pour désigner le type de colonne à laquelle appartiennent les données et la version du client qui les a produites. Le résultat final est de 52 octets. Ce résultat est ensuite multiplié par le nombre de lignes pour obtenir le surcoût total de base (utilisez le nombre total de `null` valeurs non égales s'il `preserveNulls` est défini sur true).

L'image suivante montre comment *BASE_OVERHEAD* = C3R_DESIGNATION + *(MAC * 1.33)*



Le texte chiffré de sortie dans les fingerprint colonnes sera toujours de 52 octets. Cela peut entraîner une diminution significative de la capacité de stockage si les cleartext données d'entrée dépassent en moyenne plus de 52 octets (par exemple, les adresses postales complètes). Cela peut représenter une augmentation significative du stockage si les cleartext données d'entrée sont en moyenne inférieures à 52 octets (par exemple, l'âge du client).

Paramètres de collaboration pour les fingerprint colonnes

Paramètre **`preserveNulls`**

Lorsque le paramètre au niveau de la collaboration `preserveNulls` est `false` (par défaut), chaque `null` valeur est remplacée par 32 octets uniques et aléatoires et traitée comme si ce n'était pas le cas. `null` Le résultat est que chaque `null` valeur est désormais de 52 octets. Cela peut ajouter des exigences de stockage importantes pour les tables contenant très peu de données par rapport à ce paramètre `true` et à ce que `null` les valeurs sont transmises sous forme `null` de.

Si vous n'avez pas besoin des garanties de confidentialité de ce paramètre et que vous préférez conserver `null` les valeurs de vos ensembles de données, activez le `preserveNulls` paramètre au moment de la création de la collaboration. Le `preserveNulls` paramètre ne peut pas être modifié une fois la collaboration créée.

Exemple de données pour une fingerprint colonne

Voici un exemple de jeu de données d'entrée et de sortie pour une fingerprint colonne avec des paramètres à reproduire. D'autres paramètres de collaboration n'ont `allowDuplicates` pas d'impact sur les résultats et peuvent être définis au fur `true` et à mesure que `allowCleartext` `false` vous essayez de reproduire localement.

Exemple de secret partagé : `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Exemple d'identifiant de collaboration : `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

allowJoinsOnColumnsWithDifferentNames: `True` ce paramètre n'a aucune incidence sur les performances ou les exigences de stockage. Toutefois, ce paramètre rend le choix du nom de colonne non pertinent lors de la reproduction des valeurs indiquées dans les tableaux suivants.

Exemple 1

Entrée	`null`
`preserveNulls`	`TRUE`
Sortie	`null`
Déterministe	`Yes`
Octets d'entrée	0
Octets de sortie	0

Exemple 2

Entrée	`null`
`preserveNulls`	`FALSE`
Sortie	`01:hmac:3lkFjthvV3IUu6mMvFc1a +XAHwgw/ElmOq4p3Yg25kk=`
Déterministe	No
Octets d'entrée	0
Octets de sortie	52

Exemple 3

Entrée	`empty string`

`preserveNulls`	-
Sortie	`01:hmac:oKTgi3Gba+eUb3JteSz 2EMgXUkF1WgM77UP0Ydw5kPQ=`
Déterministe	`Yes`
Octets d'entrée	0
Octets de sortie	52

Exemple 4

Entrée	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Sortie	`01:hmac:kU/IqwG7FMmzzshr0B9 scomE0UJUEE7j9keTctplGww=`
Déterministe	`Yes`
Octets d'entrée	26
Octets de sortie	52

Exemple 5

Entrée	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Sortie	`01:hmac:ks3htnQbw2vdhCRFF6J NzW5LMndJaHG57uvE26mBtSs=`
Déterministe	`Yes`

Octets d'entrée	62
Octets de sortie	52

fingerprintColonnes de dépannage

Pourquoi le texte chiffré de mes fingerprint colonnes est-il plusieurs fois supérieur à la taille du texte cleartext qui y est inscrit ?

Le texte chiffré d'une fingerprint colonne a toujours une longueur de 52 octets. Si vos données d'entrée étaient petites (par exemple, l'âge des clients), elles indiqueront une augmentation significative de leur taille. Cela peut également se produire si le `preserveNulls` paramètre est réglé sur`false`.

Pourquoi le texte chiffré de mes fingerprint colonnes est-il plusieurs fois plus petit que la taille du texte cleartext qui y figure ?

Le texte chiffré d'une fingerprint colonne a toujours une longueur de 52 octets. Si vos données d'entrée sont volumineuses (par exemple, les adresses complètes des clients), leur taille diminuera considérablement.

Comment savoir si j'ai besoin des garanties cryptographiques fournies par **`preserveNulls`** ?

Malheureusement, la réponse est que cela dépend. Au minimum, the section called “Paramètres” il convient de vérifier la manière dont le `preserveNulls` paramètre protège vos données. Cependant, nous vous recommandons de faire référence aux exigences de traitement des données de votre organisation et à tout contrat applicable à la collaboration correspondante.

Pourquoi dois-je supporter la surcharge de base64 ?

Pour garantir la compatibilité avec les formats de fichiers tabulaires tels que CSV, le codage base64 est nécessaire. Bien que certains formats de fichier Parquet puissent prendre en charge les représentations binaires des données, il est important que tous les participants à une collaboration représentent les données de la même manière afin de garantir des résultats de requête corrects.

Sealedcolonnes

Sealedles colonnes sont destinées à être utilisées pour transférer des données entre les membres d'une collaboration. Le texte chiffré de ces colonnes n'est pas déterministe et a un impact significatif

sur les performances et le stockage en fonction de la configuration des colonnes. Ces colonnes peuvent être configurées individuellement et ont souvent le plus grand impact sur les performances du client de chiffrement C3R et sur la taille du fichier de sortie qui en résulte.

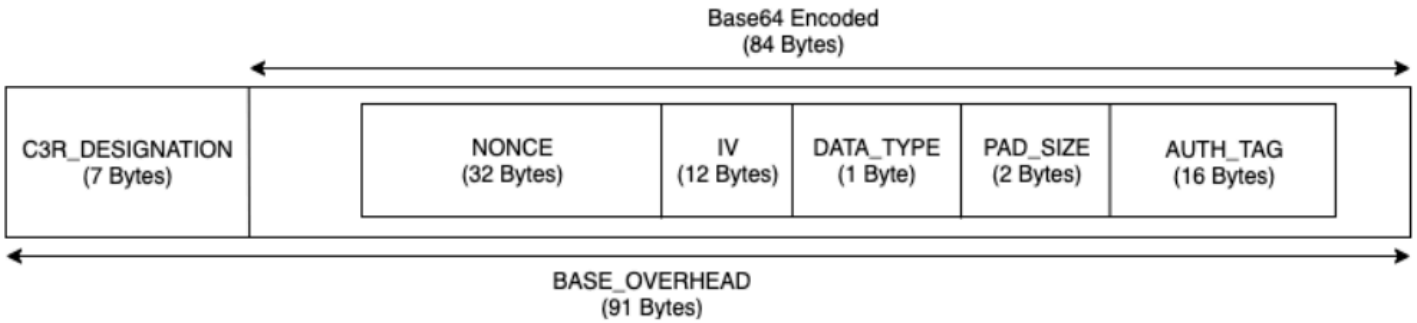
Rubriques

Frais généraux de base pour les sealed colonnes

Il existe un surcoût de base pour les sealed colonnes. Cette surcharge est constante et s'ajoute à la taille des octets cleartext et de remplissage (le cas échéant).

Avant tout chiffrement, les données des sealed colonnes sont précédées d'un caractère de 1 octet désignant le type de données contenues. Si le rembourrage est sélectionné, les données sont ensuite complétées et ajoutées avec 2 octets indiquant la taille du pad. Une fois ces octets ajoutés, les données sont traitées cryptographiquement à l'aide d'AES-GCM et stockées avec les IV (12 octets), nonce (32 octets) et Auth Tag (16 octets). Ces données sont ensuite traitées via un encodeur base64, ce qui ajoute environ 33 % à la taille des octets. Les données sont précédées d'une désignation C3R de 7 octets pour indiquer le type de colonne auquel elles appartiennent et la version du client utilisée pour les produire. Le résultat est un surdébit de base final de 91 octets. Ce résultat peut ensuite être multiplié par le nombre de lignes pour obtenir le surcoût total de base (utilisez le nombre total de valeurs non nulles s'il `preserveNulls` est défini sur true).

L'image suivante montre comment *`BASE_OVERHEAD = C3R_DESIGNATION + ((NONCE + IV + DATA_TYPE + PAD_SIZE + AUTH_TAG) * 1.33)`*



Paramètres de collaboration pour les sealed colonnes

Paramètre **preserveNulls**

Lorsque le paramètre au niveau de la collaboration `preserveNulls` est `false` (par défaut), chaque `null` valeur est unique, aléatoire de 32 octets et traitée comme si ce n'était pas le cas. `null` Le résultat est que chaque `null` valeur est désormais de 91 octets (plus si elle est complétée). Cela peut ajouter des exigences de stockage importantes pour les tables contenant très peu de données par rapport à ce paramètre `true` et à ce que `null` les valeurs sont transmises sous forme `null` de.

Si vous n'avez pas besoin des garanties de confidentialité de ce paramètre et que vous préférez conserver `null` les valeurs de vos ensembles de données, activez le `preserveNulls` paramètre au moment de la création de la collaboration. Le `preserveNulls` paramètre ne peut pas être modifié une fois la collaboration créée.

sealedColonnes des paramètres du schéma : types de rembourrage

Rubriques

- Type de pad none
- Type de pad fixed
- Type de pad max

Type de pad **none**

La sélection d'un type de pad `none` n'ajoute aucun rembourrage à la surcharge de base décrite précédemment cleartext et n'ajoute aucune surcharge supplémentaire à la surcharge de base décrite précédemment. L'absence de rembourrage permet d'obtenir la taille de sortie la plus économe en espace. Cependant, il n'offre pas les mêmes garanties de confidentialité que les types de rembourrage `fixed` et de `max` rembourrage. Cela est dû au fait que la taille du sous-jacent cleartext est perceptible à partir de la taille du texte chiffré.

Type de pad **fixed**

La sélection d'un type de pad `fixed` est une mesure de protection de la vie privée qui permet de masquer la longueur des données contenues dans une colonne. Cela se fait en complétant le tout dans le champ cleartext fourni `pad_length` avant qu'il ne soit crypté. Toute donnée dépassant cette taille entraîne l'échec du client de chiffrement C3R.

Étant donné que le remplissage est ajouté cleartext avant d'être chiffré, AES-GCM dispose d'un mappage 1 à 1 entre les octets du texte chiffré. cleartext Le codage base64 ajoutera 33 %. La surcharge de stockage supplémentaire du rembourrage peut être calculée en soustrayant la longueur moyenne du de la valeur cleartext du `pad_length` et en la multipliant par 1,33. Le résultat est le surcoût moyen de remplissage par enregistrement. Ce résultat peut ensuite être multiplié par le nombre de lignes pour obtenir la surcharge de remplissage totale (utilisez le nombre total de `null` valeurs non égales si la valeur `preserveNulls` est définie sur`true`).

*PADDING_OVERHEAD = (PAD_LENGTH - AVG_CLEARTEXT_LENGTH) * 1.33 * ROW_COUNT*

Nous vous recommandons de sélectionner le minimum `pad_length` qui englobe la plus grande valeur d'une colonne. Par exemple, si la valeur la plus élevée est de 50 octets, une valeur `pad_length` de 50 est suffisante. Une valeur supérieure à cette valeur ne fera qu'augmenter la charge de stockage.

Le rembourrage fixe n'entraîne aucune surcharge de calcul significative.

Type de pad **`max`**

La sélection d'un type de pad `max` est une mesure de protection de la vie privée qui permet de masquer la longueur des données contenues dans une colonne. Cela se fait en ajoutant le tout cleartext à la plus grande valeur de la colonne, plus le montant supplémentaire, `pad_length` avant qu'il ne soit chiffré. En général, `max` le remplissage fournit les mêmes garanties que le remplissage `fixed` d'un seul ensemble de données, tout en permettant de ne pas connaître la plus grande cleartext valeur de la colonne. Cependant, le `max` remplissage peut ne pas fournir les mêmes garanties de confidentialité que le `fixed` remplissage entre les mises à jour, car la valeur la plus élevée des ensembles de données individuels peut être différente.

Nous vous recommandons de sélectionner une valeur supplémentaire `pad_length` de 0 lorsque vous utilisez le `max` rembourrage. Cette longueur permet à toutes les valeurs d'avoir la même taille que la plus grande valeur de la colonne. Une valeur supérieure à cette valeur ne fera qu'augmenter la charge de stockage.

Si la cleartext valeur la plus élevée est connue pour une colonne donnée, nous vous recommandons d'utiliser plutôt le type `fixed` pad. L'utilisation `fixed` du rembourrage assure la cohérence entre les ensembles de données mis à jour. L'`max`utilisation du remplissage permet de compléter chaque sous-ensemble de données à la valeur la plus élevée figurant dans le sous-ensemble.

Exemple de données pour une sealed colonne

Voici un exemple de jeu de données d'entrée et de sortie pour une sealed colonne avec des paramètres à reproduire. D'autres paramètres de collaboration tels que `allowCleartextallowJoinsOnColumnsWithDifferentNames`, et `allowDuplicates` n'ont pas d'impact sur les résultats et peuvent être définis au fur `true` et à mesure que `false` vous essayez de reproduire localement. Bien qu'il s'agisse des paramètres de base à reproduire, la sealed colonne n'est pas déterministe et les valeurs changent à chaque fois. L'objectif est d'afficher les octets entrants par rapport aux octets sortants. Les `pad_length` valeurs d'exemple ont été choisies intentionnellement. Ils montrent que le `fixed` rembourrage donne les mêmes valeurs que le `max` rembourrage avec les `pad_length` paramètres minimaux recommandés ou lorsqu'un rembourrage supplémentaire est souhaité.

Exemple de secret partagé : `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Exemple d'identifiant de collaboration : `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

Rubriques

Type de pad **none**

Exemple 1

Entrée	`null`
`preserveNulls`	`TRUE`
Sortie	`null`
Déterministe	`Yes`
Octets d'entrée	0
Octets de sortie	0

Exemple 2

Entrée	`null`
`preserveNulls`	`FALSE`
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSPbNIJfG3iXmu6cbCUrizuV`
Déterministe	No
Octets d'entrée	0
Octets de sortie	91

Exemple 3

Entrée	`empty string`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSPEM6qR8DWC2PB2GMlX41YK`
Déterministe	No
Octets d'entrée	0
Octets de sortie	91

Exemple 4

Entrée	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-

Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9sGL5VLDQeHzh6DmPpyWNuI=`
Déterministe	No
Octets d'entrée	26
Octets de sortie	127

Exemple 5

Entrée	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Déterministe	No
Octets d'entrée	62
Octets de sortie	175

Type de tampon **`fixed`** (exemple 1)

Dans cet exemple, `pad_length` c'est 62 et la plus grande entrée est 62 octets.

Exemple 1

Entrée	`null`
`preserveNulls`	`TRUE`
Sortie	`null`
Déterministe	`Yes`
Octets d'entrée	0
Octets de sortie	0

Exemple 2

Entrée	`null`
`preserveNulls`	`FALSE`
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=`
Déterministe	No
Octets d'entrée	0
Octets de sortie	175

Exemple 3

Entrée	`empty string`
`preserveNulls`	-

Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=`
Déterministe	No
Octets d'entrée	0
Octets de sortie	175

Exemple 4

Entrée	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`
Déterministe	No
Octets d'entrée	26
Octets de sortie	175

Exemple 5

Entrée	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqdP4/ QOQ3cXb/pbvPcnnohrHIGSX54ua+1/ JfcVjc=`
Déterministe	No
Octets d'entrée	62
Octets de sortie	175

Type de tampon **`fixed`** (exemple 2)

Dans cet exemple, `pad_length` c'est 162 et la plus grande entrée est 62 octets.

Exemple 1

Entrée	`null`
`preserveNulls`	`TRUE`
Sortie	`null`
Déterministe	`Yes`
Octets d'entrée	0
Octets de sortie	0

Exemple 2

Entrée	`null`
`preserveNulls`	`FALSE`
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb`
Déterministe	No
Octets d'entrée	0
Octets de sortie	307

Exemple 3

Entrée	`empty string`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp`

	pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT
Déterministe	No
Octets d'entrée	0
Octets de sortie	307

Exemple 4

Entrée	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf
Déterministe	No
Octets d'entrée	26
Octets de sortie	307

Exemple 5

Entrée	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/QOQ3cXb/pbvPcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i``
Déterministe	No
Octets d'entrée	62
Octets de sortie	307

Type de tampon **`max`** (exemple 1)

Dans cet exemple, la valeur `pad_length` est 0 et la plus grande entrée est de 62 octets.

Exemple 1

Entrée	`null`
`preserveNulls`	`TRUE`
Sortie	`null`
Déterministe	`Yes`

Octets d'entrée	0
Octets de sortie	0

Exemple 2

Entrée	`null`
`preserveNulls`	`FALSE`
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/ hCz7oaIneVsrcoNpATs0GzbnLkor4L+/ aSuA=`
Déterministe	No
Octets d'entrée	0
Octets de sortie	175

Exemple 3

Entrée	`empty string`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcoLB53l07VZp A6OwkuXu29CA=`

Déterministe	No
Octets d'entrée	0
Octets de sortie	175

Exemple 4

Entrée	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`
Déterministe	No
Octets d'entrée	26
Octets de sortie	175

Exemple 5

Entrée	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8t`

	`RFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Déterministe	`No`
Octets d'entrée	62
Octets de sortie	175

Type de tampon **`max`** (exemple 2)

Dans cet exemple, `pad_length` c'est 100 et la plus grande entrée est 62 octets.

Exemple 1

Entrée	`null`
`preserveNulls`	`TRUE`
Sortie	`null`
Déterministe	`Yes`
Octets d'entrée	0
Octets de sortie	0

Exemple 2

Entrée	`null`
`preserveNulls`	`FALSE`
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcnkB0xbLWD7z`

	NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb
Déterministe	No
Octets d'entrée	0
Octets de sortie	307

Exemple 3

Entrée	`empty string`
`preserveNulls`	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT
Déterministe	No
Octets d'entrée	0
Octets de sortie	307

Exemple 4

Entrée	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf`
Déterministe	No
Octets d'entrée	26
Octets de sortie	307

Exemple 5

Entrée	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Sortie	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/QOQ3cXb/pbvPcnkB0xbLWD7z`

	`NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i`
Déterministe	No
Octets d'entrée	62
Octets de sortie	307

sealedColonnes de dépannage

Pourquoi le texte chiffré de mes sealed colonnes est-il plusieurs fois supérieur à la taille du texte cleartext qui y est inscrit ?

Cela dépend de plusieurs facteurs. D'une part, le texte chiffré d'une Cleartext colonne a toujours une longueur d'au moins 91 octets. Si vos données d'entrée étaient petites (par exemple, l'âge des clients), elles indiqueront une augmentation significative de leur taille. Ensuite, si vous avez `preserveNulls` défini ce paramètre sur `false` et que vos données d'entrée contenaient un grand nombre de `null` valeurs, chacune de ces `null` valeurs aura été transformée en 91 octets de texte chiffré. Enfin, si vous utilisez le remplissage, par définition, des octets sont ajoutés aux cleartext données avant qu'elles ne soient chiffrées.

La plupart de mes données dans une sealed colonne sont très petites et je dois utiliser le rembourrage. Puis-je simplement supprimer les grandes valeurs et les traiter séparément pour économiser de l'espace ?

Nous vous déconseillons de supprimer des valeurs importantes et de les traiter séparément. Cela modifie les garanties de confidentialité fournies par le client de chiffrement C3R. En tant que modèle de menace, supposons qu'un observateur puisse voir les deux ensembles de données chiffrés. Si l'observateur constate qu'une colonne d'un sous-ensemble de données est plus ou moins remplie qu'un autre sous-ensemble, il peut tirer des conclusions sur la taille des données de chaque sous-ensemble. Supposons, par exemple, qu'une `fullName` colonne soit complétée à un total de 40 octets dans un fichier et à 800 octets dans un autre fichier. Un observateur peut supposer qu'un ensemble de données contient le nom le plus long du monde (747 octets).

Dois-je fournir un rembourrage supplémentaire lorsque j'utilise ce type de **`max`** rembourrage ?

Non. Lorsque vous utilisez le `max` rembourrage, nous recommandons que le`pad_length`, également connu sous le nom de rembourrage supplémentaire au-delà de la plus grande valeur de la colonne, soit défini sur 0.

Puis-je simplement en choisir une grande **`pad_length`** lorsque j'utilise un **`fixed`** rembourrage pour ne pas me demander si la plus grande valeur convient ?

Oui, mais la grande longueur du pad est inefficace et utilise plus d'espace de stockage que nécessaire. Nous vous recommandons de vérifier la taille de la plus grande valeur et de la `pad_length` définir sur cette valeur.

Comment savoir si j'ai besoin des garanties cryptographiques fournies par **`preserveNulls`** ?

Malheureusement, la réponse est que cela dépend. Au minimum, Informatique cryptographique pour Clean Rooms il convient de vérifier la manière dont le `preserveNulls` paramètre protège vos données. Cependant, nous vous recommandons de faire référence aux exigences de traitement des données de votre organisation et à tout contrat applicable à la collaboration correspondante.

Pourquoi dois-je supporter la surcharge de base64 ?

Pour garantir la compatibilité avec les formats de fichiers tabulaires tels que CSV, le codage base64 est nécessaire. Bien que certains formats de fichier Parquet puissent prendre en charge les représentations binaires des données, il est important que tous les participants à une collaboration représentent les données de la même manière afin de garantir des résultats de requête corrects.

Résolution des problèmes liés aux augmentations imprévues de la taille du texte chiffré

Supposons que vous ayez chiffré vos données et que la taille des données obtenues soit étonnamment importante. Les étapes suivantes peuvent vous aider à identifier l'endroit où l'augmentation de taille s'est produite et les mesures que vous pouvez prendre, le cas échéant.

Identification de l'endroit où l'augmentation de taille s'est produite

Avant de pouvoir déterminer pourquoi vos données chiffrées sont nettement plus volumineuses que vos cleartext données, vous devez d'abord identifier l'origine de l'augmentation de taille. Cleartextles colonnes peuvent être ignorées en toute sécurité car elles sont inchangées. Examinez le reste fingerprint des sealed colonnes et choisissez-en une qui semble significative.

Identifier la raison pour laquelle l'augmentation de taille s'est produite

Une fingerprint colonne ou une sealed colonne peut contribuer à l'augmentation de la taille.

Rubriques

L'augmentation de taille provient-elle d'une fingerprint colonne ?

Si la colonne qui contribue le plus à l'augmentation du stockage est une fingerprint colonne, cela est probablement dû au fait que les cleartext données sont petites (par exemple, l'âge du client). Chaque fingerprint texte chiffré obtenu a une longueur de 52 octets. Malheureusement, rien ne peut être fait à ce sujet sur une column-by-column base solide. Pour plus d'informations, voir Frais généraux de base pour les fingerprint colonnes les détails de cette colonne, notamment son impact sur les exigences de stockage.

L'autre cause possible de l'augmentation de la taille d'une fingerprint colonne est le paramètre de collaboration,`preserveNulls`. Si le paramètre de collaboration pour `preserveNulls` est désactivé (paramètre par défaut), toutes les `null` valeurs des fingerprint colonnes seront devenues 52 octets de texte chiffré. Rien ne peut être fait pour cela dans le cadre de la collaboration actuelle. Le `preserveNulls` paramètre est défini au moment de la création d'une collaboration et tous les collaborateurs doivent utiliser le même paramètre pour garantir des résultats de requête corrects. Pour plus d'informations sur ce `preserveNulls` paramètre et sur l'impact de son activation sur les garanties de confidentialité de vos données, consultezInformatique cryptographique.

L'augmentation de taille provient-elle d'une sealed colonne ?

Si la colonne qui contribue le plus à l'augmentation du stockage est une sealed colonne, certains détails peuvent contribuer à l'augmentation de la taille.

Si les cleartext données sont petites (par exemple, l'âge du client), chaque sealed texte chiffré obtenu a une longueur d'au moins 91 octets. Malheureusement, rien ne peut être fait à ce sujet. Pour plus d'informations, voir Frais généraux de base pour les sealed colonnes les détails de cette colonne, notamment son impact sur les exigences de stockage.

La deuxième cause principale de l'augmentation du stockage dans les sealed colonnes est le rembourrage. Le remplissage ajoute des octets supplémentaires cleartext avant le chiffrement afin de masquer la taille des valeurs individuelles d'un ensemble de données. Nous vous recommandons de

définir le rembourrage à la valeur minimale possible pour votre ensemble de données. Au minimum, le `pad_length` `fixed` remplissage doit être défini de manière à inclure la plus grande valeur possible dans la colonne. Tout paramètre supérieur n'ajoute aucune garantie de confidentialité supplémentaire. Par exemple, si vous savez que la plus grande valeur possible d'une colonne peut être de 50 octets, nous vous recommandons de la `pad_length` définir sur 50 octets. Toutefois, si la sealed colonne utilise un `max` remplissage, nous vous recommandons de définir la `pad_length` valeur sur 0 octet. Cela est dû au fait que le `max` rembourrage fait référence au rembourrage supplémentaire au-delà de la plus grande valeur de la colonne.

La dernière cause possible de l'augmentation de la taille d'une sealed colonne est le paramètre de collaboration,`preserveNulls`. Si le paramètre de collaboration pour `preserveNulls` est désactivé (paramètre par défaut), toutes les `null` valeurs des sealed colonnes seront devenues 91 octets de texte chiffré. Rien ne peut être fait pour cela dans le cadre de la collaboration actuelle. Le `preserveNulls` paramètre est défini au moment de la création d'une collaboration, et tous les collaborateurs doivent utiliser le même paramètre pour garantir des résultats de requête corrects. Pour plus d'informations sur ce paramètre et sur l'impact de son activation sur les garanties de confidentialité de vos données, consultezInformatique cryptographique.

Connexion à une requête AWS Clean Rooms

La journalisation des requêtes est une fonctionnalité de AWS Clean Rooms. Lorsque vous créez une collaboration et que vous activez la journalisation des requêtes, les membres peuvent stocker les journaux de requêtes les concernant dans Amazon CloudWatch Logs.

Grâce aux journaux de requêtes, les membres peuvent déterminer si les requêtes sont conformes aux règles d'analyse et à l'accord de collaboration. En outre, les journaux de requêtes facilitent les audits.

Lorsque l'option d'enregistrement des requêtes est activée dans la AWS Clean Rooms console, les journaux des requêtes incluent les éléments suivants :

- `analysisRule`— Règle d'analyse pour la table configurée.
- `analysisTemplateArn`— Le modèle d'analyse qui a été exécuté (apparaît en fonction de la règle d'analyse).
- `collaborationId`— Identifiant unique pour la collaboration dans laquelle la requête a été exécutée.
- `configuredTableID`— Identifiant unique de la table configurée référencée dans la requête.
- `directQueryAnalysisRulePolicy.custom.allowedAnalysis`— Le modèle d'analyse autorisé à s'exécuter sur une table configurée (apparaît en fonction de la règle d'analyse).
- `directQueryAnalysisRulePolicy.v1.custom.allowedAnalysisProviders`— Les fournisseurs de requêtes autorisés à créer des requêtes (apparaissent en fonction de la règle d'analyse).
- `errorCode`— Code d'erreur lorsqu'une requête ne s'exécute pas correctement.
- `errorMessage`— Le message d'erreur lorsqu'une requête ne s'est pas exécutée correctement.
- `eventID`— Identifiant unique de la requête exécutée. Après le 31 août 2023, l'identifiant unique est le même que le`protectedQueryID`.
- `eventTimestamp`— Durée d'exécution de la requête.
- `parameters.parametervalue`— Les valeurs des paramètres (apparaissent en fonction du texte de la requête).
- `queryText`— SQL Définition de la requête exécutée. S'il existe des paramètres, ils sont étiquetés comme`:parametervalue`.
- `queryValidationErrors`— Les erreurs de requête lors de la validation de la requête.

- `schemaName`— Nom de l'association de tables configurée référencée dans la requête.
- `status`— État d'exécution de la requête.

Réception des journaux de requêtes

Vous n'avez pas besoin d'effectuer d'actions en dehors AWS Clean Rooms de la configuration des journaux de requêtes. AWS Clean Rooms crée des groupes de journaux pour les collaborations une fois que chaque membre de la collaboration a créé une adhésion.

Les membres autorisés à effectuer des requêtes, les membres autorisés à recevoir des résultats et les membres dont les tables de configuration sont référencées dans la requête recevront un journal des requêtes.

Le membre autorisé à effectuer une requête et le membre autorisé à recevoir des résultats recevront des journaux de requêtes pour chaque table configurée référencée dans la requête. S'ils ne possèdent pas la table configurée, ils ne pourront pas voir l'ID de table configuré (`configuredTableID`).

Si un membre possède plusieurs associations de tables configurées référencées dans la requête, il recevra un journal des requêtes pour chaque table configurée.

Des journaux sont créés pour les requêtes contenant des informations non prises en charge et prises en charge SQL dans AWS Clean Rooms. Pour plus de détails, consultez la AWS Clean Rooms SQLréférence.

Des journaux sont également créés lorsque les requêtes font référence à des tables configurées qui ne sont pas associées à la collaboration.

Aucun journal n'est créé SQL en cas d'entrée incorrecte AWS Clean Rooms.

Les journaux de requêtes indiquent le statut d'une requête mais n'indiquent pas si le résultat de la requête a été livré. Ils confirment qu'une requête a été soumise par le membre habilité à effectuer la demande. Les journaux de requêtes confirment également que la requête contient des tables configurées associées à la collaboration AWS Clean Rooms et y fait référence. SQL

Example

Par exemple, aucun journal n'est produit si la requête a été annulée après avoir AWS Clean Rooms validé sa conformité aux règles d'analyse et pendant le traitement de la requête.

Si vous supprimez le groupe de journaux, vous devez le recréer manuellement avec le même nom de groupe de journaux (ID de collaboration de la collaboration). Vous pouvez également désactiver et activer la déconnexion dans votre abonnement.

Pour plus d'informations sur la façon d'activer la journalisation des requêtes, consultezCréation d'une collaboration.

Pour plus d'informations sur Amazon CloudWatch Logs, consultez le guide de l'utilisateur Amazon CloudWatch Logs.

Utilisation des journaux de requêtes

Nous recommandons aux membres de prendre régulièrement les mesures suivantes :

- Pour vérifier que les requêtes correspondent aux cas d'utilisation ou aux requêtes convenus pour la collaboration, passez en revue les requêtes exécutées dans le cadre de la collaboration.

  Pour plus d'informations sur la façon d'afficher les requêtes récentes, consultez la section Affichage des requêtes récentes.
- Pour vérifier que les colonnes de table configurées correspondent à ce qui a été convenu pour la collaboration, passez en revue les colonnes de table configurées qui sont utilisées dans les règles d'analyse des membres de la collaboration et dans les requêtes.

  Pour plus d'informations sur la façon d'afficher les colonnes configurées, consultez la section Affichage des tables et des règles d'analyse.

Con AWS Clean Rooms figuration

Les rubriques suivantes expliquent comment procéder à la configuration AWS Clean Rooms.

Rubriques

Inscrivez-vous pour AWS

Avant de pouvoir en utiliser AWS service, y compris AWS Clean Rooms, vous devez vous inscrire à AWS.

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

Configurer les rôles de service pour AWS Clean Rooms

Rubriques

- Créez un rôle de service pour recevoir des résultats

Création d'un utilisateur administrateur

Pour l'utiliser AWS Clean Rooms, vous devez créer un utilisateur administrateur pour vous-même et l'ajouter à un groupe d'administrateurs.

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	Utiliser des identifiants à long terme pour accéder à AWS.	Suivez les instructions de la section Création de votre premier utilisateur IAM administrateur et de votre premier groupe d'utilisa	Configurez l'accès par programmation en gérant les clés d'accès pour IAM les utilisateurs dans le guide de IAM l'utilisateur.

Choisissez un moyen de gérer votre administrateur	Pour	Par	Vous pouvez également
(Non recommandé)		teurs dans le guide de IAM l'utilisateur.	

Création d'un IAM rôle pour un membre de la collaboration

Un membre est un AWS client participant à une collaboration.

Pour créer un IAM rôle pour un membre de la collaboration

1. Suivez la procédure Création d'un rôle pour déléguer des autorisations à un IAM utilisateur dans le Guide de AWS Identity and Access Management l'utilisateur.
2. Pour l'étape Créer une politique, sélectionnez l'JSONonglet dans l'éditeur de politiques, puis ajoutez des politiques en fonction des capacités accordées au membre de la collaboration.

   AWS Clean Rooms propose les politiques gérées suivantes basées sur des cas d'utilisation courants :

Si vous voulez...	Ensuite, utilisez...
Afficher les ressources et les métadonnées	AWS politique gérée : `AWSCleanRoomsReadOnlyAccess`
Requête	AWS politique gérée : `AWSCleanRoomsFullAccess`
Interrogez et recevez des résultats	AWS politique gérée : `AWSCleanRoomsFullAccess`

Si vous voulez...	Ensuite, utilisez...
Gérez les ressources de collaboration, mais n'interrogez pas	AWS politique gérée : `AWSCleanRoomsFullAccessNoQuerying`

Pour plus d'informations sur les différentes politiques gérées proposées par AWS Clean Rooms, voir AWS politiques gérées pour AWS Clean Rooms

Création d'un rôle de service pour lire les données

AWS Clean Rooms utilise un rôle de service pour lire les données.

Il existe deux manières de créer ce rôle de service :

Si...	Alors
Vous disposez des IAM autorisations nécessaires pour créer un rôle de service	Utilisez la AWS Clean Rooms console pour créer un rôle de service.
Vous n'en avez pas `iam:CreateRole`, `iam:CreatePolicy` et `iam:AttachRolePolicy` les autorisations or Vous souhaitez créer les IAM rôles manuellement	Effectuez l'une des actions suivantes : • Utilisez la procédure suivante pour créer un rôle de service. • Demandez à votre administrateur de créer le rôle de service en suivant la procédure suivante.

Pour créer un rôle de service permettant de lire des données

> **Note**
>
> Vous ou votre IAM administrateur ne devez suivre cette procédure que si vous ne disposez pas des autorisations nécessaires pour créer un rôle de service à l'aide de la AWS Clean Rooms console.

1. Suivez la procédure de création d'un rôle à l'aide de politiques de confiance personnalisées (console) du Guide de AWS Identity and Access Management l'utilisateur.
2. Utilisez la politique de confiance personnalisée suivante conformément à la procédure de création d'un rôle à l'aide de politiques de confiance personnalisées (console).

   > **Note**
   >
   > Si vous souhaitez vous assurer que le rôle ne peut être utilisé que dans le cadre d'une certaine adhésion à une collaboration, vous pouvez affiner davantage la politique de confiance. Pour de plus amples informations, veuillez consulter Prévention du problème de l'adjoint confus entre services.

   ```
   {

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

3. Utilisez la politique d'autorisation suivante conformément à la procédure de création d'un rôle à l'aide de politiques de confiance personnalisées (console).

> **Note**
>
> L'exemple de politique suivant prend en charge les autorisations nécessaires pour lire AWS Glue les métadonnées et les données Amazon S3 correspondantes. Toutefois, il se peut que vous deviez modifier cette politique en fonction de la façon dont vous avez configuré vos données S3. Par exemple, si vous avez configuré une KMS clé personnalisée pour vos données S3, vous devrez peut-être modifier cette politique avec des AWS KMS autorisations supplémentaires.
> Vos AWS Glue ressources et les ressources Amazon S3 sous-jacentes doivent être identiques à Région AWS celles de la AWS Clean Rooms collaboration.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "NecessaryGluePermissions",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:BatchGetPartition"
            ],
            "Resource": [
                "arn:aws:glue:aws-region:accountId:database/database",
                "arn:aws:glue:aws-region:accountId:table/table",
                "arn:aws:glue:aws-region:accountId:catalog"
            ]
        },
  {
            "Effect": "Allow",
            "Action": [
                "glue:GetSchema",
                "glue:GetSchemaVersion"
            ],
```

```
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "NecessaryS3BucketPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "s3BucketOwnerAccountId"
                    ]
                }
            }
        },
        {
            "Sid": "NecessaryS3ObjectPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3::bucket/prefix/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "s3BucketOwnerAccountId"
                    ]
                }
            }
        }

    ]
}
```

4. Remplacez chacun *placeholder* avec vos propres informations.

5. Continuez à suivre la procédure de création d'un rôle à l'aide de politiques de confiance personnalisées (console) pour créer le rôle.

Créez un rôle de service pour recevoir des résultats

> **Note**
>
> Si vous êtes le membre qui ne peut recevoir que des résultats (dans la console, les capacités de votre membre sont uniquement de recevoir des résultats), suivez cette procédure.
> Si vous êtes un membre capable à la fois d'interroger et de recevoir des résultats (dans la console, vos capacités de membre sont à la fois Query et Receive des résultats), vous pouvez ignorer cette procédure.

Pour les membres de la collaboration qui ne peuvent recevoir que des résultats, AWS Clean Rooms utilise un rôle de service pour écrire les résultats des données demandées dans la collaboration dans le compartiment Amazon S3 spécifié.

Il existe deux manières de créer ce rôle de service :

Si...	Alors
Vous disposez des IAM autorisations nécessaires pour créer un rôle de service	Utilisez la AWS Clean Rooms console pour créer un rôle de service.
Vous n'en avez pas `iam:CreateRole` , `iam:CreatePolicy` et `iam:AttachRolePolicy` les autorisations or Vous souhaitez créer les IAM rôles manuellement	Effectuez l'une des actions suivantes : • Utilisez la procédure suivante pour créer un rôle de service. • Demandez à votre administrateur de créer le rôle de service en suivant la procédure suivante.

Pour créer un rôle de service afin de recevoir des résultats

> **Note**
>
> Vous ou votre IAM administrateur ne devez suivre cette procédure que si vous ne disposez pas des autorisations nécessaires pour créer un rôle de service à l'aide de la AWS Clean Rooms console.

1. Suivez la procédure de création d'un rôle à l'aide de politiques de confiance personnalisées (console) du Guide de AWS Identity and Access Management l'utilisateur.
2. Utilisez la politique de confiance personnalisée suivante conformément à la procédure de création d'un rôle à l'aide de politiques de confiance personnalisées (console).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowIfExternalIdMatches",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "sts:ExternalId":
 "arn:aws:*:region:*:dbuser:*/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa*"
                }
            }
        },
        {
            "Sid": "AllowIfSourceArnMatches",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ForAnyValue:ArnEquals": {
                    "aws:SourceArn": [
```

```
                        "arn:aws:cleanrooms:us-east-1:555555555555:membership/
a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
                    ]

                }
            }
        }
    ]
}
```

3. Utilisez la politique d'autorisation suivante conformément à la procédure de création d'un rôle à l'aide de politiques de confiance personnalisées (console).

> **Note**
>
> L'exemple de politique suivant prend en charge les autorisations nécessaires pour lire AWS Glue les métadonnées et les données Amazon S3 correspondantes. Toutefois, il se peut que vous deviez modifier cette politique en fonction de la façon dont vous avez configuré vos données S3.
>
> Vos AWS Glue ressources et les ressources Amazon S3 sous-jacentes doivent être identiques à Région AWS celles de la AWS Clean Rooms collaboration.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount":"accountId"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name/optional_key_prefix/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount":"accountId"
                }
            }
        }
    ]
}
```

4. Remplacez chacun *placeholder* avec vos propres informations :

   - *region* — Le nom du Région AWS. Par exemple, **us-east-1**.
   - *a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa* — L'ID de membre du membre qui peut effectuer la demande. L'identifiant de membre se trouve dans l'onglet Détails de la collaboration. Cela garantit qu'il AWS Clean Rooms n'assume le rôle que lorsque ce membre exécute l'analyse dans le cadre de cette collaboration.
   - *arn:aws:cleanrooms:us-east-1:555555555555:membership/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa* — L'adhésion unique ARN du membre qui peut effectuer une requête. L'adhésion ARN se trouve dans l'onglet Détails de la collaboration. Cela garantit qu' AWS Clean Rooms il n'assume le rôle que lorsque ce membre exécute l'analyse dans le cadre de cette collaboration.
   - *bucket_name* — Le nom de ressource Amazon (ARN) du compartiment S3. Le nom de la ressource Amazon (ARN) se trouve dans l'onglet Propriétés du compartiment dans Amazon S3.
   - *accountId* — L' Compte AWS ID dans lequel se trouve le compartiment S3.

     bucket_name/optional_key_prefix — Le nom de ressource Amazon (ARN) de la destination des résultats dans S3. Le nom de la ressource Amazon (ARN) se trouve dans l'onglet Propriétés du compartiment dans Amazon S3.

5. Continuez à suivre la procédure de création d'un rôle à l'aide de politiques de confiance personnalisées (console) pour créer le rôle.

Configuration des rôles de service pour le AWS Clean Rooms ML

Rubriques

- Création d'un rôle de service pour lire les données d'entraînement
- Création d'un rôle de service pour écrire un segment similaire
- Création d'un rôle de service pour lire les données de départ

Création d'un rôle de service pour lire les données d'entraînement

AWS Clean Rooms utilise un rôle de service pour lire les données d'entraînement. Vous pouvez créer ce rôle à l'aide de la console si vous disposez des IAM autorisations nécessaires. Si vous ne disposez pas des `CreateRole` autorisations nécessaires, demandez à votre administrateur de créer le rôle de service.

Pour créer un rôle de service afin d'entraîner un ensemble de données

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 Policies (politiques).
3. Choisissez Create Policy (Créer une politique).
4. Dans l'éditeur de stratégie, sélectionnez l'JSONonglet, puis copiez et collez la politique suivante.

> **Note**
>
> L'exemple de politique suivant prend en charge les autorisations nécessaires pour lire AWS Glue les métadonnées et les données Amazon S3 correspondantes. Toutefois, il se peut que vous deviez modifier cette politique en fonction de la façon dont vous avez configuré vos données S3. Cette politique n'inclut pas de KMS clé permettant de déchiffrer les données.
> Vos AWS Glue ressources et les ressources Amazon S3 sous-jacentes doivent être identiques à Région AWS celles de la AWS Clean Rooms collaboration.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetPartitions",
                "glue:GetPartition",
                "glue:BatchGetPartition",
                "glue:GetUserDefinedFunctions"
            ],
            "Resource": [
                "arn:aws:glue:region:accountId:database/databases",
                "arn:aws:glue:region:accountId:table/databases/tables",
                "arn:aws:glue:region:accountId:catalog",
                "arn:aws:glue:region:accountId:database/default"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase"
            ],
            "Resource": [
                "arn:aws:glue:region:accountId:database/default"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::bucket"
            ],
            "Condition":{
                "StringEquals":{
```

```
                    "s3:ResourceAccount":[
                        "accountId"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucketFolders/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "accountId"
                    ]
                }
            }
        }
    ]
}
```

Si vous devez utiliser une KMS clé pour déchiffrer des données, ajoutez cette AWS KMS instruction au modèle précédent :

```
{
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
            ],
            "Resource": [
                "arn:aws:kms:region:accountId:key/keyId"
            ],
            "Condition": {
                "ArnLike": {
                        "kms:EncryptionContext:aws:s3:arn":
 "arn:aws:s3:::bucketFolders*"
                }
            }
        }
```

```
    ]
}
```

5. Choisissez Suivant.
6. Pour Révision et création, entrez le nom et la description de la politique, puis consultez le résumé.
7. Choisissez Create Policy (Créer une politique).

   Vous avez créé une politique pour AWS Clean Rooms.
8. Sous Access Management (Gestion des accès), choisissez Roles (Rôles).

   Avec les rôles, vous pouvez 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.
9. Sélectionnez Créer un rôle.
10. Dans l'assistant de création de rôle, pour Type d'entité fiable, choisissez Politique de confiance personnalisée.
11. Copiez et collez la politique de confiance personnalisée suivante dans l'JSONéditeur.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms-ml.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEqualsIfExists": {
                    "aws:SourceAccount": ["accountId"]
                },
                "StringLikeIfExists": {
                    "aws:SourceArn": "arn:aws:cleanrooms-
ml:region:account:training-dataset/*"
                }
            }
        }
```

```
    ]
}
```

`SourceAccount`C'est toujours votre AWS compte. Ils `SourceArn` peuvent être limités à un ensemble de données d'entraînement spécifique, mais uniquement après la création de cet ensemble de données. Comme vous ne pouvez pas connaître à l'avance le jeu de données d'entraînementARN, le caractère générique est spécifié ici.

12. Choisissez Suivant et sous Ajouter des autorisations, entrez le nom de la politique que vous venez de créer. (Vous devrez peut-être recharger la page.)
13. Cochez la case à côté du nom de la politique que vous avez créée, puis choisissez Next.
14. 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 interroger et recevoir des résultats et des rôles de membre.

    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.
15. Le rôle de service pour AWS Clean Rooms a été créé.

Création d'un rôle de service pour écrire un segment similaire

AWS Clean Rooms utilise un rôle de service pour écrire des segments similaires dans un compartiment. Vous pouvez créer ce rôle à l'aide de la console si vous disposez des IAM autorisations nécessaires. Si vous ne disposez pas des `CreateRole` autorisations nécessaires, demandez à votre administrateur de créer le rôle de service.

Pour créer un rôle de service, pour écrire un segment similaire

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 Policies (politiques).
3. Choisissez Create Policy (Créer une politique).
4. Dans l'éditeur de stratégie, sélectionnez l'JSONonglet, puis copiez et collez la politique suivante.

> **Note**
>
> L'exemple de politique suivant prend en charge les autorisations nécessaires pour lire AWS Glue les métadonnées et les données Amazon S3 correspondantes. Toutefois, il se peut que vous deviez modifier cette politique en fonction de la façon dont vous avez configuré vos données S3. Cette politique n'inclut pas de KMS clé permettant de déchiffrer les données.
> Vos AWS Glue ressources et les ressources Amazon S3 sous-jacentes doivent être identiques à Région AWS celles de la AWS Clean Rooms collaboration.

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

```
            "Resource": [
                "arn:aws:s3:::bucketFolders/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "accountId"
                    ]
                }
            }
        }
  ]
}
```

Si vous devez utiliser une KMS clé pour chiffrer des données, ajoutez cette AWS KMS instruction au modèle :

```
{
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:GenerateDataKey*",
                "kms:ReEncrypt*",
            ],
            "Resource": [
                "arn:aws:kms:region:accountId:key/keyId"
            ],
            "Condition": {
                "ArnLike": {
                        "kms:EncryptionContext:aws:s3:arn":
 "arn:aws:s3:::bucketFolders*"
                }
            }
        }
  ]
}
```

Si vous devez utiliser une KMS clé pour déchiffrer des données, ajoutez cette AWS KMS instruction au modèle :

```
{
            "Effect": "Allow",
```

```
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:region:accountId:key/keyId"
            ],
            "Condition": {
                "ArnLike": {
                        "kms:EncryptionContext:aws:s3:arn":
 "arn:aws:s3:::bucketFolders*"
                }
            }
        }
  ]
}
```

5. Choisissez Suivant.
6. Pour Révision et création, entrez le nom et la description de la politique, puis consultez le résumé.
7. Choisissez Create Policy (Créer une politique).

   Vous avez créé une politique pour AWS Clean Rooms.
8. Sous Access Management (Gestion des accès), choisissez Roles (Rôles).

   Avec les rôles, vous pouvez 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.
9. Sélectionnez Créer un rôle.
10. Dans l'assistant de création de rôle, pour Type d'entité fiable, choisissez Politique de confiance personnalisée.
11. Copiez et collez la politique de confiance personnalisée suivante dans l'JSONéditeur.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAssumeRole",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "cleanrooms-ml.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEqualsIfExists": {
                    "aws:SourceAccount": ["accountId"]

                },
                "StringLikeIfExists": {
                    "aws:SourceArn": "arn:aws:cleanrooms-
ml:region:account:configured-audience-model/*"
                }
            }
        }
    ]
}
```

`SourceAccount`C'est toujours votre AWS compte. Ils `SourceArn` peuvent être limités à un ensemble de données d'entraînement spécifique, mais uniquement après la création de cet ensemble de données. Comme vous ne pouvez pas connaître à l'avance le jeu de données d'entraînementARN, le caractère générique est spécifié ici.

12. Choisissez Suivant.
13. Cochez la case à côté du nom de la politique que vous avez créée, puis choisissez Next.
14. 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 interroger et recevoir des résultats et des rôles de membre.

    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.
15. Le rôle de service pour AWS Clean Rooms a été créé.

Création d'un rôle de service pour lire les données de départ

AWS Clean Rooms utilise un rôle de service pour lire les données de départ. Vous pouvez créer ce rôle à l'aide de la console si vous disposez des IAM autorisations nécessaires. Si vous ne disposez pas des `CreateRole` autorisations nécessaires, demandez à votre administrateur de créer le rôle de service.

Créer un rôle de service pour lire les données de départ stockées dans un compartiment Amazon S3.

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 Policies (politiques).
3. Choisissez Create Policy (Créer une politique).
4. Dans l'éditeur de stratégies, sélectionnez l'JSONonglet, puis copiez et collez l'une des politiques suivantes.

> **Note**
>
> L'exemple de politique suivant prend en charge les autorisations nécessaires pour lire AWS Glue les métadonnées et les données Amazon S3 correspondantes. Toutefois, il se peut que vous deviez modifier cette politique en fonction de la façon dont vous avez configuré vos données S3. Cette politique n'inclut pas de KMS clé permettant de déchiffrer les données.
> Vos AWS Glue ressources et les ressources Amazon S3 sous-jacentes doivent être identiques à Région AWS celles de la AWS Clean Rooms collaboration.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
            ],
            "Resource": [
                "arn:aws:s3:::buckets"
            ],
            "Condition":{
```

```
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "accountId"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucketFolders/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "accountId"
                    ]
                }
            }
        }
  ]
}
```

> **Note**
>
> L'exemple de politique suivant prend en charge les autorisations nécessaires pour lire les résultats d'une SQL requête et les utiliser comme données d'entrée. Toutefois, il se peut que vous deviez modifier cette politique en fonction de la structure de votre requête. Cette politique n'inclut pas de KMS clé permettant de déchiffrer les données.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCleanRoomsStartQuery",
            "Effect": "Allow",
            "Action": [
```

```
                "cleanrooms:GetCollaborationAnalysisTemplate",
                "cleanrooms:GetSchema",
                "cleanrooms:StartProtectedQuery"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowCleanRoomsGetAndUpdateQuery",
            "Effect": "Allow",
            "Action": [
                "cleanrooms:GetProtectedQuery",
                "cleanrooms:UpdateProtectedQuery"
            ],
            "Resource": [
                "arn:aws:cleanrooms:{{region}}:{{queryRunnerAccountId}}:membership/
{{queryRunnerMembershipId}}"
            ]
        }
    ]
}
```

Si vous devez utiliser une KMS clé pour déchiffrer des données, ajoutez cette AWS KMS instruction au modèle :

```
{
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:region:accountId:key/keyId"
            ],
            "Condition": {
                "ArnLike": {
                        "kms:EncryptionContext:aws:s3:arn":
 "arn:aws:s3:::bucketFolders*"
                }
            }
        }
  ]
}
```

5. Choisissez Suivant.
6. Pour Révision et création, entrez le nom et la description de la politique, puis consultez le résumé.
7. Choisissez Create Policy (Créer une politique).

   Vous avez créé une politique pour AWS Clean Rooms.
8. Sous Access Management (Gestion des accès), choisissez Roles (Rôles).

   Avec les rôles, vous pouvez 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.
9. Sélectionnez Créer un rôle.
10. Dans l'assistant de création de rôle, pour Type d'entité fiable, choisissez Politique de confiance personnalisée.
11. Copiez et collez la politique de confiance personnalisée suivante dans l'JSONéditeur.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms-ml.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEqualsIfExists": {
                    "aws:SourceAccount": ["accountId"]

                },
                "StringLikeIfExists": {
                    "aws:SourceArn": "arn:aws:cleanrooms-
ml:region:account:audience-generation-job/*"
                }
            }
        }
    ]
}
```

`SourceAccount`C'est toujours votre AWS compte. Ils `SourceArn` peuvent être limités à un ensemble de données d'entraînement spécifique, mais uniquement après la création de cet ensemble de données. Comme vous ne pouvez pas connaître à l'avance le jeu de données d'entraînementARN, le caractère générique est spécifié ici.

12. Choisissez Suivant.
13. Cochez la case à côté du nom de la politique que vous avez créée, puis choisissez Next.
14. 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 interroger et recevoir des résultats et des rôles de membre.

    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.
15. Le rôle de service pour AWS Clean Rooms a été créé.

Travailler avec des collaborations dans AWS Clean Rooms

Une collaboration est une limite logique sécurisée AWS Clean Rooms dans laquelle les membres peuvent effectuer des SQL requêtes sur des tables configurées.

Tout membre AWS Clean Rooms peut créer une collaboration.

Le créateur de la collaboration peut désigner un seul membre pour interroger et recevoir les résultats. Toutefois, le créateur de la collaboration souhaitera peut-être empêcher le membre autorisé à effectuer une requête d'accéder aux résultats de la requête. Dans ce cas, le créateur de la collaboration peut désigner un membre qui peut effectuer des requêtes et un autre membre qui peut recevoir les résultats.

Dans la plupart des cas, le membre qui peut interroger est également le membre qui paie les coûts de calcul des requêtes. Cependant, le créateur de la collaboration peut configurer un autre membre pour qu'il soit responsable du paiement des coûts de calcul des requêtes.

Pour plus d'informations sur la création d'une collaboration à l'aide du AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Rubriques

- Création d'une collaboration
- Création d'un abonnement et adhésion à une collaboration
- Gérer les collaborations dans AWS Clean Rooms

Création d'une collaboration

Dans cette procédure, le créateur de la collaboration effectue les tâches suivantes :

- Crée une collaboration.
- Invite un ou plusieurs membres à la collaboration.
- Attribue des capacités aux membres, telles que le membre qui peut effectuer des requêtes et le membre qui peut recevoir des résultats.

  Si le créateur de la collaboration est également le membre habilité à recevoir les résultats, il spécifie la destination et le format des résultats de la requête. Ils fournissent également un rôle de

service Amazon Resource Name (ARN) pour écrire les résultats dans la destination des résultats de la requête.

- Configure quel membre est responsable du paiement des coûts de calcul des requêtes dans le cadre de la collaboration.

Avant de commencer, assurez-vous d'avoir rempli les conditions préalables suivantes :

- Vous avez le nom et l' Compte AWS identifiant de chaque membre que vous souhaitez inviter à rejoindre la collaboration.
- Vous êtes autorisé à partager le nom et l' Compte AWS identifiant de chaque membre avec tous les membres de la collaboration.

> **Note**
>
> Vous ne pouvez pas ajouter d'autres membres une fois la collaboration créée.

Pour plus d'informations sur la création d'une collaboration à l'aide du AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Pour créer une collaboration à l'aide de la AWS Clean Rooms console

1. Connectez-vous à la console AWS Management Console et ouvrez-la avec la AWS Clean Rooms console Compte AWS qui fonctionnera en tant que créateur de collaboration.
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Dans le coin supérieur droit, choisissez Créer une collaboration.
4. Pour l'étape 1 : définir la collaboration, procédez comme suit :

    a. Pour plus de détails, entrez le nom et la description de la collaboration.

    Ces informations seront visibles par les membres de la collaboration invités à participer à la collaboration. Le nom et la description les aident à comprendre à quoi fait référence la collaboration.

    b. Pour les membres :

    i. Pour le membre 1 : vous devez saisir le nom d'affichage de votre membre tel que vous souhaitez qu'il apparaisse pour la collaboration.

> **Note**
>
> Votre Compte AWS identifiant est automatiquement inclus comme Compte AWS identifiant de membre.

ii. Pour Membre 2, entrez le nom d'affichage du membre et l' Compte AWS ID du membre que vous souhaitez inviter à rejoindre la collaboration.

Le nom d'affichage et l' Compte AWS identifiant du membre seront visibles par toutes les personnes invitées à la collaboration. Une fois que vous avez saisi et enregistré les valeurs de ces champs, vous ne pouvez pas les modifier.

> **Note**
>
> Vous devez informer le membre de la collaboration que son Compte AWS identifiant de membre et son nom d'affichage seront visibles par tous les collaborateurs invités et actifs de la collaboration.

iii. Si vous souhaitez ajouter un autre membre, choisissez Ajouter un autre membre. Entrez ensuite le nom d'affichage du membre et l' Compte AWS identifiant de membre pour chaque membre susceptible de fournir les données que vous souhaitez inviter à la collaboration.

c. En ce qui concerne les capacités des membres, effectuez l'une des actions suivantes en fonction de votre objectif.

Votre objectif	Action recommandée
Interrogez les données de la collaboration et recevez les résultats	1. Choisissez-vous comme membre autorisé à exécuter des requêtes. 2. Laissez le paramètre par défaut du membre autorisé à recevoir des résultats identique à celui du membre qui exécute les requêtes.

Votre objectif	Action recommandée
Interrogez les données de la collaboration et désignez un autre membre pour recevoir les résultats	1. Choisissez-vous comme membre autorisé à exécuter des requêtes. 2. Sélectionnez le membre qui peut recevoir les résultats dans la liste déroulante.
Recevez les résultats de la requête dans la collaboration et désignez un autre membre pour interroger les données	1. Sélectionnez le membre autorisé à exécuter des requêtes dans la liste déroulante. 2. Choisissez vous-même en tant que membre qui peut recevoir les résultats dans la liste déroulante.
Créez et gérez la collaboration, assignez un autre membre pour interroger les données et affectez un autre membre pour recevoir les résultats	1. Sélectionnez le membre autorisé à exécuter des requêtes dans la liste déroulante. 2. Sélectionnez le membre qui peut recevoir les résultats dans la liste déroulante.

d. Pour la configuration des paiements, effectuez l'une des actions suivantes en fonction de votre objectif.

Votre objectif	Action recommandée
Désignez le membre qui peut exécuter des requêtes comme étant le membre qui paie les coûts de calcul de la requête	Laissez le paramètre par défaut du membre qui paiera pour les requêtes identique à celui du membre qui exécute les requêtes.
Désignez un membre différent pour payer les coûts de calcul de la requête	Sélectionnez le membre qui paiera pour les requêtes dans la liste déroulante.

e. Si vous souhaitez activer la journalisation des requêtes, cochez la case Support de la journalisation des requêtes pour cette collaboration.

f. Si vous souhaitez activer la fonctionnalité de calcul cryptographique, cochez la case Soutenir le calcul cryptographique dans cette collaboration et choisissez les paramètres de calcul cryptographique suivants :

- Autoriser cleartext les colonnes

  Choisissez Non si vous ne souhaitez pas que cleartext les colonnes soient autorisées dans la table cryptée.

  Choisissez Oui si vous souhaitez que cleartext les colonnes soient autorisées dans la table cryptée.

  Pour fonctionner SUM ou AVG sur certaines colonnes, les colonnes doivent être insérées cleartext.

- Autoriser les doublons

  Choisissez Non si vous ne souhaitez pas que les doublons soient autorisés dans une fingerprint colonne.

  Choisissez Oui si vous souhaitez que les entrées dupliquées soient autorisées dans une fingerprint colonne.

- JOINAutorisation de colonnes portant des noms différents

  Choisissez Non si vous ne souhaitez pas joindre des fingerprint colonnes portant des noms différents.

  Choisissez Oui si vous souhaitez joindre des fingerprint colonnes portant des noms différents.

- Préservez NULL les valeurs

  Choisissez Non si vous ne souhaitez pas conserver NULL les valeurs. NULLles valeurs n'apparaîtront pas comme NULL dans une table cryptée.

  Choisissez Oui si vous souhaitez conserver NULL les valeurs. NULLles valeurs apparaîtront comme NULL dans une table cryptée.

Pour plus d'informations sur les paramètres informatiques cryptographiques, consultezParamètres de calcul cryptographique.

Pour plus d'informations sur le chiffrement de vos données pour les utiliser dans AWS Clean Rooms, consultezPréparation de tables de données chiffrées à l'aide de l'informatique cryptographique pour Clean Rooms.

> **Note**
>
> Vérifiez soigneusement ces configurations avant de passer à l'étape suivante. Après avoir créé la collaboration, vous pouvez uniquement modifier le nom et la description de la collaboration et indiquer si les journaux de requêtes sont stockés dans Amazon CloudWatch Logs.

g. Si vous souhaitez activer les balises pour la ressource de collaboration, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

h. Choisissez Suivant.

5. Pour l'étape 2 : configurer l'adhésion, procédez comme suit :

a. Choisissez une option :

Option	Résultat
Oui, inscrivez-vous en créant un abonnement dès maintenant	La collaboration et votre adhésion sont créées. Votre statut dans la collaboration est actif.
Non, je créerai un abonnement plus tard	Seule la collaboration est créée. Votre statut dans la collaboration est inactif.

b. Si vous êtes le membre habilité à recevoir les résultats, sous Paramètres des résultats de requête par défaut, choisissez l'une des options suivantes :

Option	Action recommandée
Conservez la case à cocher Définir les paramètres par défaut maintenant cochée. (Il est sélectionné par défaut.)	1. Pour la destination des résultats dans Amazon S3, entrez la destination Amazon S3. 2. Pour le format du résultat de la requête, choisissez CSVsoit PARQUET.
Désactivez la case à cocher Définir les paramètres par défaut maintenant	Seule la collaboration est créée. Votre statut dans la collaboration est inactif.

c. Si vous avez choisi d'activer la journalisation des requêtes à l'étape 4.e, choisissez l'une des options suivantes pour le stockage des CloudWatch journaux dans Amazon Logs :

Option	Résultat
Allumez	Les journaux de requêtes qui vous concernent sont stockés dans Amazon CloudWatch Logs. Chaque membre ne peut recevoir que les journaux des requêtes qu'il a initiées ou qui contiennent ses données. Le membre qui peut recevoir les résultats reçoit également des journaux pour toutes les requêtes exécutées dans le cadre d'une collaboration, même si ses données ne sont pas accessibles dans le cadre d'une requête.
Éteindre	Les journaux de requêtes qui vous concernent ne sont pas stockés dans votre compte Amazon CloudWatch Logs.

> **Note**
>
> Après avoir activé la journalisation des requêtes, la configuration du stockage des journaux et le début de la réception des journaux dans Amazon CloudWatch Logs peuvent prendre quelques minutes. Pendant cette brève période, le membre autorisé à effectuer des requêtes peut exécuter des requêtes qui n'envoient pas réellement de journaux.

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

e. Si vous êtes le membre qui paie pour les requêtes, indiquez votre acceptation en cochant la case J'accepte de payer les frais de calcul des requêtes dans le cadre de cette collaboration.

> **Note**
>
> Vous devez cocher cette case pour continuer.
> Pour plus d'informations sur le mode de calcul des prix, consultezTarification pour AWS Clean Rooms.

Si vous êtes le membre qui paie les frais de calcul des requêtes, mais que vous n'êtes pas le membre habilité AWS Budgets à effectuer des requêtes, il est recommandé de configurer un budget AWS Clean Rooms et de recevoir des notifications une fois le budget maximum atteint. Pour plus d'informations sur la configuration d'un budget, consultez la section Gérer vos coûts AWS Budgets dans le Guide de AWS Cost Management l'utilisateur. Pour plus d'informations sur la configuration des notifications, consultez la section Création d'une SNS rubrique Amazon pour les notifications budgétaires dans le guide de AWS Cost Management l'utilisateur. Si le budget maximum est atteint, vous pouvez contacter le membre qui pourra lancer des requêtes ou quitter la collaboration. Si vous quittez la collaboration, aucune autre requête ne sera autorisée à être exécutée et, par conséquent, les frais de calcul des requêtes ne vous seront plus facturés.

f. Choisissez Suivant.

6. Pour l'étape 3 : 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 l'une des options.

Si vous avez choisi de...	Ensuite, choisissez...
Créez un abonnement avec la collaboration (Oui, inscrivez-vous en créant un abonnement maintenant)	Créez des liens de collaboration et d'adhésion
Créez la collaboration et ne créez pas d'adhésion pour le moment (Non, je créerai un abonnement plus tard)	Créez une collaboration

Une fois que votre collaboration a été créée avec succès, vous pouvez voir la page des détails de la collaboration sous Collaborations.

Vous êtes maintenant prêt à :

- Préparez votre table de données pour y être interrogée. AWS Clean Rooms (Facultatif si vous souhaitez interroger vos propres données d'événement ou si vous souhaitez interroger des données d'identité.)
- Associez le tableau configuré à votre collaboration. (Facultatif si vous souhaitez interroger vos propres données d'événement.)
- Ajoutez une règle d'analyse pour la table configurée. (Facultatif si vous souhaitez interroger vos propres données d'événement.)
- Créez un abonnement et rejoignez une collaboration. (Facultatif si vous avez déjà créé un abonnement.)
- Gérez votre collaboration.

Création d'un abonnement et adhésion à une collaboration

Un abonnement est une ressource créée lorsqu'un membre rejoint une collaboration dans AWS Clean Rooms.

Vous pouvez rejoindre une collaboration en tant que membre habilité à interroger des données, en tant que membre autorisé à recevoir les résultats d'une requête, ou les deux. Vous pouvez également rejoindre une collaboration en tant que membre en payant les frais de calcul des requêtes. Tous les membres peuvent fournir des données.

Pour plus d'informations sur la façon de créer un abonnement et de rejoindre une collaboration à l'aide du AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Dans cette procédure, le membre invité rejoint la collaboration en créant une ressource d'adhésion.

Si le membre invité est celui qui peut recevoir les résultats, il spécifie la destination et le format des résultats de la requête. Ils fournissent également un rôle de service permettant ARN d'écrire dans la destination des résultats de la requête.

Si le membre invité est le membre chargé de payer les frais de calcul des requêtes, il accepte ses responsabilités de paiement avant de rejoindre la collaboration.

Pour créer un abonnement et rejoindre une collaboration

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre membre Compte AWS.
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Dans l'onglet Disponible pour rejoindre, pour les collaborations disponibles, choisissez le nom de la collaboration.
4. Sur la page des détails de la collaboration, consultez les détails de la collaboration, y compris les détails de vos membres et la liste des autres membres.

   Vérifiez que Compte AWS IDs les membres de chaque membre de la collaboration sont ceux avec lesquels vous avez l'intention de participer à la collaboration.
5. Choisissez Créer un abonnement.
6. Sur la page Créer un abonnement, dans l'aperçu, consultez le nom de la collaboration, la description de la collaboration, l' Compte AWS identifiant du créateur de la collaboration, vos capacités de membre et l' Compte AWS identifiant du membre qui paiera pour les requêtes.
7. Si le créateur de la collaboration a choisi d'activer la journalisation des requêtes, choisissez l'une des options suivantes pour le stockage des CloudWatch journaux dans Amazon Logs :

Si vous choisissez…	Alors...
Allumez	Les journaux de requêtes qui vous concernent sont stockés dans Amazon CloudWatch Logs. Chaque membre ne peut recevoir que les journaux des requêtes qu'il a initiées ou qui contiennent ses données. Le membre qui peut recevoir les résultats reçoit également des journaux pour toutes les requêtes exécutées dans le cadre d'une collaboration, même si ses données ne sont pas accessibles dans le cadre d'une requête.
Éteindre	Les journaux de requêtes qui vous concernent ne sont pas stockés dans votre compte Amazon CloudWatch Logs.

> **Note**
>
> Après avoir activé la journalisation des requêtes, la configuration du stockage des journaux et le début de la réception des journaux dans Amazon CloudWatch Logs peuvent prendre quelques minutes. Pendant cette brève période, le membre autorisé à effectuer des requêtes peut exécuter des requêtes qui n'envoient pas réellement de journaux.

8. Si les capacités de votre membre incluent Recevoir des résultats :

   a. Pour les paramètres des résultats de requête,

      i. Spécifiez la destination des résultats dans Amazon S3 en saisissant la destination S3 ou choisissez Parcourir S3 pour effectuer une sélection dans la liste des compartiments S3 disponibles.

Example

Par exemple : **`s3://bucket/prefix`**

ii. Choisissez le format du résultat (CSVou PARQUET).

b. Pour accéder au service, choisissez de créer et d'utiliser un nouveau rôle de service ou d'utiliser un rôle de service existant.

> **Note**
>
> Vous devez sélectionner un rôle de service existant ou être autorisé à en créer un nouveau. Pour de plus amples informations, veuillez consulter Créez un rôle de service pour recevoir des résultats.

9. Si vous souhaitez activer les balises pour la ressource d'adhésion, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
10. Si le créateur de la collaboration vous a désigné comme membre chargé de payer pour les requêtes, indiquez votre acceptation en cochant la case J'accepte de payer les frais de calcul des requêtes dans le cadre de cette collaboration.

> **Note**
>
> Vous devez cocher cette case pour continuer.
> Pour plus d'informations sur le mode de calcul des prix, consultezTarification pour AWS Clean Rooms.

Si vous êtes le membre qui paie les frais de calcul des requêtes, mais que vous n'êtes pas le membre habilité AWS Budgets à effectuer des requêtes, il est recommandé de configurer un budget AWS Clean Rooms et de recevoir des notifications une fois le budget maximum atteint. Pour plus d'informations sur la configuration d'un budget, consultez la section Gérer vos coûts AWS Budgets dans le Guide de AWS Cost Management l'utilisateur. Pour plus d'informations sur la configuration des notifications, consultez la section Création d'une SNS rubrique Amazon pour les notifications budgétaires dans le guide de AWS Cost Management l'utilisateur. Si le budget maximum est atteint, vous pouvez contacter le membre qui pourra lancer des requêtes ou quitter la collaboration. Si vous quittez la collaboration, aucune autre requête ne sera autorisée à être exécutée et, par conséquent, les frais de calcul des requêtes ne vous seront plus facturés.

11. Si vous êtes sûr de vouloir créer un abonnement et rejoindre la collaboration, choisissez Créer un abonnement.

Vous disposez d'un accès en lecture aux métadonnées de collaboration. Cela inclut des informations telles que le nom d'affichage et la description de la collaboration, en plus de tous les noms et Compte AWS IDs des autres membres.

Vous êtes maintenant prêt à :

- Préparez votre table de données pour y être interrogée. AWS Clean Rooms (Facultatif si vous souhaitez interroger vos propres données d'événement ou si vous souhaitez interroger des données d'identité.)
- Associez la table configurée à votre collaboration, si vous souhaitez interroger les données d'un événement.
- Ajoutez une règle d'analyse pour la table configurée, si vous souhaitez interroger les données d'événements.
- Créez et associez un nouvel espace de noms d'identification : si vous souhaitez créer une table de mappage d'identifiants pour interroger les données d'identité,

Pour plus d'informations sur la façon de quitter une collaboration, consultezQuitter une collaboration.

Gérer les collaborations dans AWS Clean Rooms

Les rubriques suivantes décrivent comment le créateur de la collaboration peut gérer une collaboration à AWS Clean Rooms l'aide de la AWS Clean Rooms console.

Pour plus d'informations sur la gestion d'une collaboration à l'aide du AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Rubriques

- Collaborations d'édition
- Supprimer des collaborations
- Afficher les collaborations
- Surveillance des membres
- Supprimer un membre d'une collaboration

- Quitter une collaboration

Collaborations d'édition

Découvrez comment modifier les différentes parties d'une collaboration.

Rubriques

- Modifier le nom et la description de la collaboration
- Modifier les balises de collaboration
- Modifier les tags d'adhésion
- Modifier les balises de table associées
- Modifier les balises du modèle d'analyse
- Modifier les balises de politique de confidentialité différentielles

Modifier le nom et la description de la collaboration

Après avoir créé la collaboration, vous ne pouvez modifier que le nom et la description de la collaboration.

> **Note**
>
> Si vous avez activé la journalisation des requêtes, vous pouvez modifier si les journaux des requêtes sont stockés dans votre compte Amazon CloudWatch Logs.

Pour modifier le nom et la description de la collaboration

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration que vous avez créée.
4. Sur la page détaillée de la collaboration, choisissez Actions, puis Modifier la collaboration.
5. Pour plus de détails, modifiez le nom et la description de la collaboration.
6. Sélectionnez Enregistrer les modifications.

Modifier les balises de collaboration

En tant que créateur de collaboration, après avoir créé une collaboration, vous pouvez gérer les balises de la ressource de collaboration.

Pour modifier les balises de collaboration

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration que vous avez créée.
4. Sélectionnez l'une des méthodes suivantes :

Si...	Alors...
Membre de la collaboration	Cliquez sur l'onglet Détails.
Le créateur de la collaboration mais non membre de la collaboration	Faites défiler la page vers le bas jusqu'à la section Tags.

5. Pour plus de détails sur la collaboration, choisissez Gérer les balises.
6. Sur la page de gestion des étiquettes, vous pouvez effectuer les opérations suivantes :
   - Pour supprimer une identification, choisissez Supprimer.
   - Pour ajouter une balise, sélectionnez Add new tag (Ajouter une nouvelle balise).
   - Pour enregistrer vos modifications, choisissez Enregistrer les modifications

Modifier les tags d'adhésion

En tant que créateur de collaboration, après avoir créé une collaboration, vous pouvez gérer les balises de la ressource d'adhésion.

Pour modifier les tags d'adhésion

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.

3. Choisissez la collaboration que vous avez créée.
4. Cliquez sur l'onglet Détails.
5. Pour les détails de l'adhésion, choisissez Gérer les tags.
6. Sur la page Gérer les tags d'adhésion, vous pouvez effectuer les opérations suivantes :

   - Pour supprimer une identification, choisissez Supprimer.
   - Pour ajouter une balise, sélectionnez Add new tag (Ajouter une nouvelle balise).
   - Choisissez Enregistrer pour enregistrer les modifications.

Modifier les balises de table associées

En tant que créateur de collaboration, après avoir associé des tables à une collaboration, vous pouvez gérer les balises de la ressource de table associée.

Pour modifier les balises de table associées

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration que vous avez créée.
4. Choisissez l'onglet Tables.
5. Pour les tables que vous avez associées, choisissez une table.
6. Sur la page détaillée du tableau configuré, pour Balises, choisissez Gérer les balises.

   Sur la page de gestion des étiquettes, vous pouvez effectuer les opérations suivantes :

   - Pour supprimer une identification, choisissez Supprimer.
   - Pour ajouter une balise, sélectionnez Add new tag (Ajouter une nouvelle balise).
   - Choisissez Enregistrer pour enregistrer les modifications.

Modifier les balises du modèle d'analyse

En tant que créateur de collaboration, après avoir créé une collaboration, vous pouvez gérer les balises de la ressource du modèle d'analyse.

Pour modifier les tags d'adhésion

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration que vous avez créée.
4. Sélectionnez l'onglet Templates (Modèles) .
5. Dans la section Modèles d'analyse que vous avez créés, choisissez le modèle d'analyse.
6. Sur la page détaillée du tableau du modèle d'analyse, faites défiler la page vers le bas jusqu'à la section Tags.
7. Choisissez Gérer les balises.
8. Sur la page de gestion des étiquettes, vous pouvez effectuer les opérations suivantes :
   - Pour supprimer une identification, choisissez Supprimer.
   - Pour ajouter une balise, sélectionnez Add new tag (Ajouter une nouvelle balise).
   - Choisissez Enregistrer pour enregistrer les modifications.

Modifier les balises de politique de confidentialité différentielles

En tant que créateur de collaboration, après avoir créé une collaboration, vous pouvez gérer les balises de la ressource du modèle d'analyse.

Pour modifier les tags d'adhésion

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration contenant la politique de confidentialité différentielle que vous souhaitez modifier.
4. Choisissez l'onglet Tables.
5. Dans l'onglet Tables, sélectionnez Gérer les balises.
6. Sur la page de gestion des étiquettes, vous pouvez effectuer les opérations suivantes :
   - Pour supprimer une identification, choisissez Supprimer.
   - Pour ajouter une balise, sélectionnez Add new tag (Ajouter une nouvelle balise).

- Choisissez Enregistrer pour enregistrer les modifications.

Supprimer des collaborations

En tant que créateur de collaboration, vous pouvez supprimer une collaboration que vous avez créée.

> **Note**
>
> Lorsque vous supprimez une collaboration, vous et tous les membres ne pouvez pas exécuter de requêtes, recevoir de résultats ou apporter des données. Chaque membre de la collaboration continue d'avoir accès à ses propres données dans le cadre de son adhésion.

Pour supprimer une collaboration

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration que vous souhaitez supprimer.
4. Sous Actions, choisissez Supprimer la collaboration.
5. Confirmez la suppression, puis choisissez Supprimer.

Afficher les collaborations

En tant que créateur de collaboration, vous pouvez consulter toutes les collaborations que vous avez créées.

Pour consulter les collaborations

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Sur la page Collaborations, sous Dernière utilisation, consultez les 5 dernières collaborations utilisées.
4. Dans l'onglet Avec adhésion active, consultez la liste des collaborations avec adhésion active.

Vous pouvez trier par nom, date de création de l'adhésion et informations relatives à votre membre.

Vous pouvez utiliser la barre de recherche pour rechercher une collaboration.

5. Dans l'onglet Disponible pour participer, consultez la liste des collaborations disponibles.
6. Dans l'onglet Plus disponible, consultez la liste des collaborations supprimées et des adhésions pour les collaborations qui ne sont plus disponibles (adhésions supprimées).

Surveillance des membres

En tant que créateur de collaboration, après avoir créé une collaboration, vous pouvez suivre le statut de tous les membres dans l'onglet Membres.

Pour vérifier le statut d'un membre

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration que vous avez créée.
4. Choisissez l'onglet Membres.
5. Dans le tableau Membres, passez en revue le statut de chaque membre.
6. Dans le tableau des capacités des membres, déterminez quels membres peuvent effectuer des requêtes, recevoir des résultats, fournir des données et effectuer d'autres tâches.
7. Dans le tableau de configuration des paiements, vérifiez quels membres paient pour les requêtes, les tables de mappage d'identifiants et la modélisation du machine learning.

Supprimer un membre d'une collaboration

> **Note**
>
> La suppression d'un membre entraîne également la suppression de tous ses ensembles de données associés de la collaboration.

Pour supprimer un membre d'une collaboration

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration que vous avez créée.
4. Choisissez l'onglet Membres.
5. Sélectionnez le bouton d'option situé à côté du membre à supprimer.

> **Note**
>
> Un créateur de collaboration ne peut pas choisir son propre identifiant de compte.

6. Sélectionnez Remove (Supprimer).
7. Dans la boîte de dialogue, confirmez la décision de supprimer le membre **`confirm`** en saisissant du texte dans le champ de saisie.

> **Note**
>
> Si vous supprimez le membre payant les frais de calcul des requêtes, aucune autre requête n'est autorisée à être exécutée dans le cadre de la collaboration.

Quitter une collaboration

En tant que membre d'une collaboration, vous pouvez quitter une collaboration en supprimant votre adhésion. Si vous êtes le créateur de la collaboration, vous ne pouvez quitter une collaboration qu'en la supprimant.

> **Note**
>
> Lorsque vous supprimez votre adhésion, vous quittez la collaboration et vous ne pouvez pas la rejoindre à nouveau. Si vous êtes membre et que vous payez les frais de calcul des requêtes et que vous supprimez votre adhésion, aucune autre requête n'est autorisée à être exécutée.

Pour quitter une collaboration

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Pour Avec adhésion active, choisissez la collaboration dont vous êtes membre.
4. Choisissez Actions.
5. Choisissez Supprimer l'adhésion.
6. Dans la boîte de dialogue, confirmez la décision de quitter la collaboration **`confirm`** en saisissant du texte dans le champ de saisie, puis en choisissant Vide et supprimer l'adhésion.

   Un message s'affiche sur la console indiquant que l'adhésion a été supprimée.

   Le créateur de la collaboration considère que le statut de membre est Gauche.

Utilisation de tables de données dans AWS Clean Rooms

Les tables de données que vous utilisez pour les requêtes AWS Clean Rooms sont généralement du même type que celles que vous utilisez pour d'autres applications. Par exemple, les mêmes types de jeux de données sont utilisés avec Amazon Athena, Amazon, EMR Amazon Redshift Spectrum et Amazon. QuickSight Vous pouvez interroger les données dans leur format d'origine directement depuis Amazon Simple Storage Service (Amazon S3).

Rubriques

Formats de données pour AWS Clean Rooms

Pour interroger des données, les ensembles de données doivent être dans un format AWS Clean Rooms compatible. Le compartiment Amazon S3 contenant les ensembles de données et le AWS Clean Rooms cluster doivent se trouver dans le même Région AWS compartiment.

Formats de données pris en charge

AWS Clean Rooms prend en charge les formats structurés suivants :

- Tables Apache Iceberg
- Parquet
- RCFile
- TextFile
- SequenceFile
- RegexSerde
- OpenCSV

- AVRO
- JSON

> **Note**
>
> `timestamp`La valeur d'un fichier texte doit être au format`yyyy-MM-dd HH:mm:ss.SSSSSS`. Par exemple :`2017-05-01 11:30:59.000000`.

Nous vous recommandons d'utiliser un format de fichier de stockage en colonnes, tel queApache Parquet. Avec un format de fichier de stockage en colonnes, vous pouvez minimiser le transfert de données hors d'Amazon S3 en ne sélectionnant que les colonnes dont vous avez besoin. Pour des performances optimales, les objets volumineux doivent être divisés en objets de 100 Mo à 1 Go.

Types de données pris en charge

Pour une expérience optimale AWS Clean Rooms, toutes vos données doivent être cataloguées. AWS Glue Pour plus d'informations, consultez la section intitulée Getting started with the AWS Glue Data Catalog dans le manuel du AWS Glue développeur.

AWS Clean Rooms prend en charge les types AWS Glue Data Catalog de données suivants :

- bigint
- boolean
- char
- date
- decimal
- double
- float
- int
- Types de données imbriqués tels que :
  - array
  - map
  - struct

- smallint
- string
- timestamp
- varchar

AWS Clean Rooms ne prend pas en charge :

- binary
- interval

Types de compression de fichiers pour AWS Clean Rooms

Pour réduire l'espace de stockage, améliorer les performances et minimiser les coûts, nous vous recommandons vivement de compresser vos ensembles de données.

AWS Clean Rooms reconnaît les types de compression de fichiers en fonction de leur extension et prend en charge les types de compression et les extensions indiqués dans le tableau suivant.

Algorithme de compression	Extension de fichier
GZIP	.gz
Bzip2	.bz2
Snappy	.snappy

Vous pouvez appliquer la compression à différents niveaux. Le plus souvent, vous compressez un fichier entier ou des blocs individuels dans un fichier. La compression des formats en colonnes au niveau du fichier n'apporte aucun avantage en termes de performances.

Chiffrement côté serveur pour AWS Clean Rooms

> **Note**
>
> Le chiffrement côté serveur ne remplace pas le calcul cryptographique dans les cas d'utilisation qui l'exigent.

AWS Clean Rooms déchiffre de manière transparente les ensembles de données chiffrés à l'aide des options de chiffrement suivantes :

- SSE-S3 — Chiffrement côté serveur à l'aide d'une clé de chiffrement AES -256 gérée par Amazon S3
- SSE- KMS — Chiffrement côté serveur avec des clés gérées par AWS Key Management Service

Pour utiliser SSE -S3, le rôle de AWS Clean Rooms service utilisé pour associer la table configurée à la collaboration doit disposer des autorisations KMS -decrypt. Pour utiliser SSE -KMS, la politique de KMS clé doit également autoriser le rôle AWS Clean Rooms de service à déchiffrer.

AWS Clean Rooms ne prend pas en charge le chiffrement côté client Amazon S3. Pour plus d'informations sur le chiffrement côté serveur, consultez la section Protection des données à l'aide du chiffrement côté serveur dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Utilisation de Apache Iceberg tableaux dans AWS Clean Rooms

Apache Icebergest un format de table open source pour les lacs de données. AWS Clean Rooms peut utiliser les statistiques stockées dans les Apache Iceberg métadonnées pour optimiser les plans de requêtes et réduire le nombre de scans de fichiers lors du traitement des requêtes en salle blanche. Pour plus d'informations, consultez la documentation d'Apache Iceberg.

Lorsque vous utilisez des tables Iceberg, tenez compte AWS Clean Rooms des points suivants :

- Tables incluses dans le AWS Glue Data Catalog seul — Apache Iceberg les tables doivent être définies dans le sur la AWS Glue Data Catalog base de l'implémentation du catalogue Glue Open Source.
- Format de fichier Parquet : prend AWS Clean Rooms uniquement en charge les tables Iceberg au format de fichier de données Parquet.
- Compression GZIP et Snappy : AWS Clean Rooms supporte Parquet avec GZIP et compression. Snappy
- Versions Iceberg : AWS Clean Rooms permet d'exécuter des requêtes sur les tables Iceberg des versions 1 et 2.
- Partitions : vous n'avez pas besoin d'ajouter manuellement des partitions pour vos Apache Iceberg tables dans AWS Glue. AWS Clean Rooms détecte automatiquement les nouvelles partitions dans Apache Iceberg les tables et aucune opération manuelle n'est nécessaire pour mettre à jour les

partitions dans la définition de table. Les partitions Iceberg apparaissent sous forme de colonnes normales dans le schéma de AWS Clean Rooms table et non séparément sous forme de clé de partition dans le schéma de table configuré.

- Limites
  - Nouvelles tables Iceberg uniquement

    Apache Icebergles tables converties à partir de Apache Parquet tables ne sont pas prises en charge.
  - Requêtes Time Travel

    AWS Clean Rooms ne prend pas en charge les requêtes de voyage dans le temps avec Apache Iceberg des tableaux.
  - Moteur Athena version 2

    Icebergles tables créées avec la version 2 du moteur Athena ne sont pas prises en charge.
  - Formats de fichiers

    Avroet les formats de fichier ORC (Optimized Row Columnar) ne sont pas pris en charge.
  - Compression

    ZstandardLa compression (Zstd) pour n'Parquetest pas prise en charge.

Types de données pris en charge pour les tables Iceberg

AWS Clean Rooms peut interroger Iceberg des tables contenant les types de données suivants :

- boolean
- date
- decimal
- double
- float
- int
- list
- long
- map

- string
- struct
- timestamp without time zone

Pour en savoir plus sur les types de données Iceberg, consultez Schemas for Iceberg dans la documentation Apache Iceberg.

Préparation des tables de données pour les requêtes dans AWS Clean Rooms

> **Note**
>
> La préparation des tableaux de données peut avoir lieu avant ou après avoir rejoint une collaboration. Une fois qu'un tableau est préparé, vous pouvez le réutiliser dans plusieurs collaborations, à condition que vos besoins en matière de confidentialité soient les mêmes pour ce tableau.

En tant que membre de la collaboration, vous devez préparer vos tables de données avant que le membre AWS Clean Rooms de la collaboration puisse les interroger.

Si votre cas d'utilisation ne vous oblige pas à apporter vos propres données, vous pouvez ignorer cette procédure.

Si votre cas d'utilisation implique de demander des données d'identité, consultezTravailler avec Résolution des entités AWS in AWS Clean Rooms.

Si vos tables de données sont déjà cataloguées AWS Glue, passez àCréation d'une table configurée dans AWS Clean Rooms.

La préparation de vos tables de données implique les étapes suivantes :

- Étape 1 : Exécuter les prérequis
- Étape 2 : (Facultatif) Préparez vos données pour le calcul cryptographique
- Étape 3 : Chargez votre tableau de données sur Amazon S3
- Étape 4 : Création d'une AWS Glue table

Pour plus d'informations sur les formats de données que vous pouvez utiliser pour les requêtes, consultezFormats de données pour AWS Clean Rooms.

Étape 1 : Exécuter les prérequis

Pour préparer vos tables de données à utiliser avec AWS Clean Rooms, vous devez remplir les conditions préalables suivantes :

- Vos tables de données doivent être enregistrées dans l'un des formats de données pris en charge pour AWS Clean Rooms.
- Vos tables de données doivent être cataloguées AWS Glue et utiliser les types de données pris en charge pour AWS Clean Rooms.
- Toutes vos tables de données doivent être stockées dans Amazon Simple Storage Service (Amazon S3), là où la Région AWS collaboration a été créée.
- Ils AWS Glue Data Catalog doivent se trouver dans la même région que celle dans laquelle la collaboration a été créée.
- Ils AWS Glue Data Catalog doivent être identiques à ceux Compte AWS de l'adhésion.
- Le compartiment Amazon S3 ne peut pas être enregistré auprès de celui-ci AWS Lake Formation.
- Le créateur de la collaboration a configuré une collaboration dans AWS Clean Rooms. Pour de plus amples informations, veuillez consulter Création d'une collaboration.
- Le créateur de la collaboration vous a envoyé l'identifiant de collaboration en tant que participant à la collaboration.

Étape 2 : (Facultatif) Préparez vos données pour le calcul cryptographique

(Facultatif) Si vous utilisez l'informatique cryptographique et que votre table de données contient des informations sensibles que vous souhaitez chiffrer, vous devez chiffrer la table de données à l'aide du client de chiffrement C3R.

Pour préparer vos données pour le calcul cryptographique, suivez les procédures décrites dansPréparation de tables de données chiffrées à l'aide de l'informatique cryptographique pour Clean Rooms.

Étape 3 : Chargez votre tableau de données sur Amazon S3

> **Note**
>
> Si vous avez l'intention d'utiliser des tables de données chiffrées dans le cadre de la collaboration, vous devez d'abord chiffrer les données pour le calcul cryptographique avant de télécharger votre table de données sur Amazon S3. Pour de plus amples informations, veuillez consulter Préparation de tables de données chiffrées à l'aide de l'informatique cryptographique pour Clean Rooms.

Pour télécharger votre tableau de données sur Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Buckets, puis choisissez un bucket dans lequel vous souhaitez 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 les données.

Étape 4 : Création d'une AWS Glue table

Si vous disposez déjà d'une table de AWS Glue données, vous pouvez ignorer cette étape.

Au cours de cette étape, vous configurez un robot d'exploration AWS Glue qui analyse tous les fichiers de votre compartiment S3 et crée une AWS Glue table. Pour plus d'informations, consultez la section Définition des robots d'exploration AWS Glue dans le guide de l'AWS Glue utilisateur.

Pour plus d'informations sur les types de AWS Glue Data Catalog données pris en charge, consultezTypes de données pris en charge.

> **Note**
>
> AWS Clean Rooms ne prend actuellement pas en charge les compartiments S3 enregistrés auprès AWS Lake Formation de.

La procédure suivante décrit comment créer une AWS Glue table. Si vous souhaitez utiliser un AWS Glue Data Catalog objet chiffré avec une clé AWS Key Management Service (AWS KMS), vous devez configurer la politique d'autorisation des KMS clés pour autoriser l'accès à cette table chiffrée. Pour plus d'informations, consultez la section Configuration du chiffrement dans AWS Glue dans le manuel du AWS Glue développeur.

Pour créer une AWS Glue table

1. Suivez la procédure relative à l'utilisation des robots d'exploration sur la AWS Glue console du guide de l'AWS Glue utilisateur.
2. Notez le nom de la AWS Glue base de données et le nom de AWS Glue la table.

Maintenant que vous avez préparé vos tableaux de données, vous êtes prêt à :

- Création d'une table configurée
- Création d'un modèle ML

Préparation de tables de données chiffrées à l'aide de l'informatique cryptographique pour Clean Rooms

L'informatique cryptographique pour Clean Rooms (C3R) est une fonctionnalité de. AWS Clean Rooms Vous pouvez utiliser C3R pour limiter cryptographiquement ce qui peut être appris par n'importe quelle partie et AWS dans le cadre d'une AWS Clean Rooms collaboration.

Vous pouvez chiffrer la table de données à l'aide du client de chiffrement C3R, un outil de chiffrement côté client, avant de télécharger la table de données sur Amazon Simple Storage Service (Amazon S3).

Pour de plus amples informations, veuillez consulter Informatique cryptographique pour Clean Rooms.

La préparation de tables de données chiffrées avec C3R implique les étapes suivantes :

Étapes

Étape 1 : Exécuter les prérequis

Pour préparer vos tables de données en vue de leur utilisation avec C3R, vous devez remplir les conditions préalables suivantes :

- Vous pouvez accéder au Clean Rooms référentiel Cryptographic Computing for sur GitHub :

  https://github.com/aws/c3r
- Vous avez configuré les AWS informations d'identification pour utiliser le client de chiffrement C3R. Ces informations d'identification sont utilisées par le client de chiffrement C3R pour les API appels en lecture seule afin de récupérer les métadonnées AWS Clean Rooms de collaboration. Pour plus d'informations, consultez la section Configuration du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur de la version 2.
- Vous avez installé Java Runtime Environment (JRE) 11 ou une version ultérieure sur votre machine.
  - La version recommandéeJava Runtime Environment, Amazon Corretto 11 ou version ultérieure, peut être téléchargée sur https://aws.amazon.com/corretto.
  - Le Java Development Kit (JDK) inclut un correspondant JRE de la même version. Toutefois, les fonctionnalités supplémentaires du ne JDK sont pas nécessaires pour exécuter le client de chiffrement Cryptographic Computing for Clean Rooms (C3R).

- Vos fichiers de données tabulaires (.csv) ou vos Parquet fichiers (. parquet) sont enregistrés localement.
- Vous ou un autre membre de la collaboration avez la possibilité de créer une clé secrète partagée. Pour de plus amples informations, veuillez consulter Étape 5 : Création d'une clé secrète partagée.
- Le créateur de la collaboration a créé une collaboration AWS Clean Rooms avec l'informatique cryptographique activée pour la collaboration. Pour de plus amples informations, veuillez consulter Création d'une collaboration.
- Le créateur de la collaboration vous a envoyé l'identifiant de collaboration en tant que participant à la collaboration. Le nom de ressource Amazon de la collaboration (ARN) est inclus dans l'invitation envoyée, qui contient l'identifiant de collaboration.

Étape 2 : Téléchargez le client de chiffrement C3R

Pour télécharger le client de chiffrement C3R depuis GitHub

1. Accédez au Clean RoomsAWSGitHub référentiel Cryptographic Computing for : c3r https://github.com/aws/
2. Sélectionnez et téléchargez les fichiers.

   Le code source, les licences et le matériel connexe peuvent être clonés ou téléchargés sous forme de fichier. zipfichier depuis la page d'accueil du GitHub dépôt. (Voir le bouton Code en haut à droite de la liste du contenu du référentiel).

   Le dernier client de chiffrement C3R signé Java Executable File (c'est-à-dire l'application d'interface de ligne de commande) se trouve sur la page Versions du GitHub référentiel.

   Le package client de chiffrement C3R pour Apache Spark (`c3r-cli-spark`) est une version du c3r-cli qui doit être soumise en tant que tâche à un serveur Apache Spark en cours d'exécution. Pour plus d'informations, consultez Exécuter C3R sur Apache Spark.

Étape 3 : (Facultatif) Afficher les commandes disponibles dans le client de chiffrement C3R

Utilisez cette procédure pour vous familiariser avec les commandes disponibles dans le client de chiffrement C3R.

Pour afficher toutes les commandes disponibles dans le client de chiffrement C3R

1. À partir d'une interface de ligne de commande (CLI), accédez au dossier contenant le c3r-cli.jar fichier téléchargé.
2. Exécutez la commande suivante: `java -jar c3r-cli.jar`
3. Consultez la liste des commandes et options disponibles.

Étape 4 : générer un schéma de chiffrement pour un fichier tabulaire

Pour chiffrer des données, un schéma de chiffrement décrivant la manière dont les données seront utilisées est requis. Cette section décrit comment le client de chiffrement C3R aide à générer un schéma de chiffrement pour un CSV fichier avec une ligne d'en-tête ou un Parquet fichier.

Vous ne devez effectuer cette opération qu'une seule fois par fichier. Une fois que le schéma existe, il peut être réutilisé pour chiffrer le même fichier (ou tout autre fichier dont le nom de colonne est identique). Si les noms des colonnes ou le schéma de chiffrement souhaité changent, vous devez mettre à jour le fichier de schéma. Pour de plus amples informations, veuillez consulter (Facultatif) Créez un schéma (utilisateurs avancés).

> **Important**
>
> Il est essentiel que toutes les parties collaboratrices utilisent la même clé secrète partagée. Les parties collaboratrices doivent également coordonner les noms des colonnes afin de déterminer s'ils doivent être JOIN édités ou comparés d'une autre manière pour garantir l'égalité dans les requêtes. Dans le cas contraire, les SQL requêtes risquent de produire des résultats inattendus ou incorrects. Toutefois, cela n'est pas nécessaire si le créateur de la collaboration a activé le paramètre de `allowJoinsOnColumnsWithDifferentNames` chiffrement lors de la création de la collaboration. Pour plus d'informations sur les paramètres relatifs au chiffrement, consultez. Paramètres de calcul cryptographique

Lorsqu'il est exécuté en mode schéma, le client de chiffrement C3R parcourt le fichier d'entrée colonne par colonne pour vous demander si et comment cette colonne doit être traitée. Si le fichier contient de nombreuses colonnes qui ne sont pas souhaitées pour la sortie cryptée, la génération de schéma interactif peut devenir fastidieuse car vous devez ignorer chaque colonne indésirable. Pour éviter cela, vous pouvez écrire manuellement un schéma ou créer une version simplifiée du fichier d'entrée contenant uniquement les colonnes souhaitées. Ensuite, le générateur de schéma interactif

pourrait être exécuté sur ce fichier réduit. Le client de chiffrement C3R produit des informations sur le fichier de schéma et vous demande comment les colonnes source doivent être incluses ou cryptées (le cas échéant) dans la sortie cible.

Pour chaque colonne source du fichier d'entrée, vous êtes invité à saisir :

1. Combien de colonnes cibles doivent être générées
2. Comment chaque colonne cible doit être cryptée (le cas échéant)
3. Le nom de chaque colonne cible
4. Comment les données doivent être remplies avant le chiffrement si la colonne est chiffrée en tant que sealed colonne

> **Note**
>
> Lorsque vous chiffrez les données d'une colonne chiffrée en tant que sealed colonne, vous devez déterminer quelles données doivent être rembourrées. Le client de chiffrement C3R suggère un rembourrage par défaut lors de la génération du schéma, afin que toutes les entrées d'une colonne aient la même longueur.
> Lorsque vous déterminez la longueur de`fixed`, notez que le remplissage est exprimé en octets et non en bits.

Vous trouverez ci-dessous une table de décision pour créer le schéma.

Tableau de décision relatif au schéma

Décision	Nombre de colonnes cibles depuis la colonne source <' name-of-column '> ?	Type de colonne cible : [c]cleartext, [f] fingerprint ou [s] sealed ?	Nom de l'en-tête de la colonne cible <default 'name-of-column'>	Ajouter un suffixe <suffix>à l'en-tête pour indiquer comment il a été crypté, [y] oui ou [n] non <default 'yes'>	<' name-of-column _sealed'> type de rembourrage : [n] un, [f] fixe ou [m] max <default 'max'>
Laissez la colonne non chiffrée.	1	c	Ne s'applique pas	Ne s'applique pas	Ne s'applique pas
Chiffrez la colonne en tant que fingerprint colonne.	1	f	Choisissez le nom par défaut ou entrez un nouveau nom d'en-tête.	Entrez y pour choisir par défaut (`_fingerprint`) ou entrezn.	Ne s'applique pas
Chiffrez la colonne en tant que sealed colonne.	1	s	Choisissez le nom par défaut ou entrez un nouveau nom d'en-tête.	Entrez y pour choisir par défaut (`_sealed`) ou entrezn.	Choisissez le type de rembourrage. Pour de plus amples informations, veuillez consulter (Facultatif) Créez un schéma (utilisateurs avancés).

Décision	Nombre de colonnes cibles depuis la colonne source <' name-of-column '> ?	Type de colonne cible : [c]cleartext, [f] fingerprint ou [s] sealed ?	Nom de l'en-tête de la colonne cible <default 'name-of-column'>	Ajouter un suffixe <suffix>à l'en-tête pour indiquer comment il a été crypté, [y] oui ou [n] non <default 'yes'>	<' name-of-column _sealed'> type de rembourrage : [n] un, [f] fixe ou [m] max <default 'max'>
Chiffrez la colonne sous la forme à la fois fingerprint et. sealed	2	Entrez la première colonne cible : f. Entrez la deuxième colonne cible : s.	Choisissez les en-têtes cibles pour chaque colonne cible.	Entrez y pour choisir la valeur par défaut ou entrez n.	Choisissez le type de rembourrage (pour les sealed colonnes uniquement). Pour de plus amples informations, veuillez consulter (Facultatif) Créez un schéma (utilisateurs avancés).

Voici deux exemples de création de schémas de chiffrement. Le contenu exact de votre interaction dépend du fichier d'entrée et des réponses que vous fournissez.

Exemples

- Exemple : génération d'un schéma de chiffrement pour une fingerprint colonne et une cleartext colonne

- Exemple : génération d'un schéma de chiffrement avec des cleartext colonnes sealedfingerprint, et

Exemple : génération d'un schéma de chiffrement pour une fingerprint colonne et une cleartext colonne

Dans cet exemple, pourads.csv, il n'y a que deux colonnes : username etad_variant. Pour ces colonnes, nous voulons ce qui suit :

- Pour que la username colonne soit cryptée en tant que fingerprint colonne
- Pour que la ad_variant colonne soit une cleartext colonne

Pour générer un schéma de chiffrement pour une fingerprint colonne et une cleartext colonne

1. (Facultatif) Pour vous assurer que le c3r-cli.jar fichier et le fichier à chiffrer sont présents :

   a. Naviguez jusqu'au répertoire souhaité et exécutez ls (si vous utilisez a Mac ouUnix/Linux) ou dir si vous utilisezWindows).

   b. Consultez la liste des fichiers de données tabulaires (par exemple, .csv) et choisissez un fichier à chiffrer.

      Dans cet exemple, ads.csv c'est le fichier que nous voulons chiffrer.

2. À partir deCLI, exécutez la commande suivante pour créer un schéma de manière interactive.

```
java -jar c3r-cli.jar schema ads.csv --interactive --output=ads.json
```

> **Note**
>
> - Tu peux courirjava --jar PATH/TO/c3r-cli.jar. Ou, si vous avez ajouté PATH/TO/c3r-cli.jar à votre variable d'CLASSPATHenvironnement, vous pouvez également exécuter le nom de classe. Le client de chiffrement C3R va regarder dans le CLASSPATH pour le trouver (par exemple,java com.amazon.psion.cli.Main).
> - L'--interactiveindicateur sélectionne le mode interactif pour développer le schéma. Cela guide l'utilisateur à travers un assistant de création du schéma. Les utilisateurs dotés de compétences avancées peuvent créer leur propre schéma JSON sans utiliser l'assistant. Pour de plus amples informations, veuillez consulter (Facultatif) Créez un schéma (utilisateurs avancés).

- L'`--output`indicateur définit un nom de sortie. Si vous n'incluez pas l'`--output`indicateur, le client de chiffrement C3R essaie de choisir un nom de sortie par défaut (tel que `<input>.out.csv` ou pour le schéma`<input>.json`).

3. Pour`Number of target columns from source column 'username'?`, entrez, **1** puis appuyez sur Entrée.
4. Pour`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, entrez, **f** puis appuyez sur Entrée.
5. Pour`Target column headername <default 'username'>`, appuyez sur Entrée.

   Le nom par défaut « `username` » est utilisé.
6. Pour`Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, entrez, **y** puis appuyez sur Entrée.

> **Note**
>
> Le mode interactif suggère des suffixes à ajouter aux en-têtes de colonnes chiffrés (`_fingerprint`pour les fingerprint colonnes et `_sealed` pour sealed les colonnes). Les suffixes peuvent être utiles lorsque vous effectuez des tâches telles que le téléchargement de données AWS services ou la création de collaborations. AWS Clean Rooms Ces suffixes peuvent aider à indiquer ce qui peut être fait avec les données chiffrées de chaque colonne. Par exemple, les choses ne fonctionneront pas si vous chiffrez une colonne sous forme de sealed colonne (`_sealed`) et que vous essayez d'y JOIN accéder ou que vous essayez l'inverse.

7. Pour`Number of target columns from source column 'ad_variant'?`, entrez, **1** puis appuyez sur Entrée.
8. Pour`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, entrez, **c** puis appuyez sur Entrée.
9. Pour`Target column headername <default 'username'>`, appuyez sur Entrée.

   Le nom par défaut « `ad_variant` » est utilisé.

   Le schéma est écrit dans un nouveau fichier appelé`ads.json`.

> **Note**
>
> Vous pouvez afficher le schéma en l'ouvrant dans n'importe quel éditeur de texte, tel que Notepad on Windows ou TextEdit onmacOS.

10. Vous êtes maintenant prêt à chiffrer les données.

Exemple : génération d'un schéma de chiffrement avec des cleartext colonnes sealedfingerprint, et

Dans cet exemple, poursales.csv, il y a trois colonnes : usernamepurchased, etproduct. Pour ces colonnes, nous voulons ce qui suit :

- Pour que la product colonne soit une sealed colonne
- Pour que la username colonne soit cryptée en tant que fingerprint colonne
- Pour que la purchased colonne soit une cleartext colonne

Pour générer un schéma de chiffrement avec des cleartext colonnes sealedfingerprint, et

1. (Facultatif) Pour vous assurer que le c3r-cli.jar fichier et le fichier à chiffrer sont présents :
   a. Naviguez jusqu'au répertoire souhaité et exécutez ls (si vous utilisez a Mac ouUnix/Linux) ou dir si vous utilisezWindows).
   b. Consultez la liste des fichiers de données tabulaires (.csv) et choisissez un fichier à chiffrer.

      Dans cet exemple, sales.csv c'est le fichier que nous voulons chiffrer.
2. À partir deCLI, exécutez la commande suivante pour créer un schéma de manière interactive.

```
java -jar c3r-cli.jar schema sales.csv --interactive --
output=sales.json
```

> **Note**
>
> - L'--interactiveindicateur sélectionne le mode interactif pour développer le schéma. Cela guide l'utilisateur à travers un flux de travail guidé pour créer le schéma.

- Si vous êtes un utilisateur avancé, vous pouvez créer votre propre schéma JSON sans utiliser le flux de travail guidé. Pour de plus amples informations, veuillez consulter (Facultatif) Créez un schéma (utilisateurs avancés).
- Pour les fichiers .csv sans en-tête de colonne, consultez l'`--noHeaders`indicateur de la commande de schéma disponible dans le. CLI
- L'`--output`indicateur définit un nom de sortie. Si vous n'incluez pas l'`--output`indicateur, le client de chiffrement C3R essaie de choisir un nom de sortie par défaut (tel que `<input>.out` ou pour le schéma`<input>.json`).

3. Pour`Number of target columns from source column 'username'?`, entrez, **1** puis appuyez sur Entrée.
4. Pour`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, entrez, **f** puis appuyez sur Entrée.
5. Pour`Target column headername <default 'username'>`, appuyez sur Entrée.

   Le nom par défaut « `username` » est utilisé.
6. Pour`Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, entrez, **y** puis appuyez sur Entrée.
7. Pour`Number of target columns from source column 'purchased'?`, entrez, **1** puis appuyez sur Entrée.
8. Pour`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, entrez, **c** puis appuyez sur Entrée.
9. Pour`Target column headername <default 'purchased'>`, appuyez sur Entrée.

   Le nom par défaut « `purchased` » est utilisé.
10. Pour`Number of target columns from source column 'product'?`, entrez, **1** puis appuyez sur Entrée.
11. Pour`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, entrez, **s** puis appuyez sur Entrée.
12. Pour`Target column headername <default 'product'>`, appuyez sur Entrée.

    Le nom par défaut « `product` » est utilisé.
13. Pour`'product_sealed' padding type: [n]one, [f]ixed, or [m]ax <default 'max'?>`, appuyez sur Entrée pour choisir la valeur par défaut.

14. Pour sélectionner la valeur par défaut, `Byte-length beyond max length to pad cleartext to in 'product_sealed' <default '0'>?` appuyez sur Entrée.

    Le schéma est écrit dans un nouveau fichier appelé`sales.json`.

15. Vous êtes maintenant prêt à chiffrer les données.

Étape 5 : Création d'une clé secrète partagée

Pour chiffrer les tables de données, les participants à la collaboration doivent s'entendre sur une clé secrète partagée et la partager en toute sécurité.

La clé secrète partagée doit être d'au moins 256 bits (32 octets). Vous pouvez spécifier une clé plus grande, mais cela ne vous apportera aucune sécurité supplémentaire.

> **Important**
>
> N'oubliez pas que la clé et l'identifiant de collaboration utilisés pour le chiffrement et le déchiffrement doivent être identiques pour tous les participants à la collaboration.

Les sections suivantes fournissent des exemples de commandes de console permettant de générer une clé secrète partagée enregistrée `secret.key` dans le répertoire de travail actuel du terminal concerné.

Rubriques

- Exemple : génération de clés à l'aide de OpenSSL
- Exemple : génération de clés lors de l'Windowsutilisation PowerShell

Exemple : génération de clés à l'aide de OpenSSL

Pour une bibliothèque de cryptographie à usage général, exécutez la commande suivante pour créer une clé secrète partagée.

```
openssl rand 32 > secret.key
```

Si vous utilisez Windows et n'en avez pas OpenSSL installé, vous pouvez générer des clés à l'aide de l'exemple décrit dans Exemple : génération de clés lors de Windows l'utilisation PowerShell.

Exemple : génération de clés lors de l'Windowsutilisation PowerShell

Pour PowerShell une application de terminal disponible surWindows, exécutez la commande suivante pour créer une clé secrète partagée.

```
$bs = New-Object Byte[](32);
[Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($bs); Set-
Content 'secret.key' -Encoding Byte -Value $bs
```

Étape 6 : Stocker la clé secrète partagée dans une variable d'environnement

Une variable d'environnement est un moyen pratique et extensible pour les utilisateurs de fournir une clé secrète provenant de différents magasins de clés, par exemple, AWS Secrets Manager et de la transmettre au client de chiffrement C3R.

Le client de chiffrement C3R peut utiliser des clés stockées dans AWS services si vous utilisez le AWS CLI pour stocker ces clés dans la variable d'environnement correspondante. Par exemple, le client de chiffrement C3R peut utiliser une clé provenant de AWS Secrets Manager. Pour plus d'informations, voir Création et gestion de secrets AWS Secrets Manager dans le Guide de AWS Secrets Manager l'utilisateur.

> **Note**
>
> Cependant, avant d'utiliser un AWS service tel AWS Secrets Manager pour maintenir vos clés C3R, vérifiez que votre cas d'utilisation le permet. Certains cas d'utilisation peuvent nécessiter que la clé ne soit pas divulguée. AWS Cela permet de garantir que les données cryptées et la clé ne sont jamais détenues par le même tiers.

Les seules conditions requises pour une clé secrète partagée sont que la clé secrète partagée soit base64 codée et stockée dans la variable `C3R_SHARED_SECRET` d'environnement.

Les sections suivantes décrivent les commandes de console permettant de convertir un `secret.key` fichier en variable d'environnement base64 et de le stocker en tant que variable d'environnement. Le `secret.key` fichier peut avoir été généré à partir de l'une des commandes répertoriées dans Étape 5 : Création d'une clé secrète partagée et n'est qu'un exemple de source.

Stocker la clé dans une variable d'environnement lors de Windows l'utilisation PowerShell

Pour convertir base64 et définir la variable d'environnement lors de Windows l'utilisationPowerShell, exécutez la commande suivante.

```
$Bytes=[IO.File]::ReadAllBytes((Get-Location).ToString()+'\secret.key');
 $env:C3R_SHARED_SECRET=[Convert]::ToBase64String($Bytes)
```

Stocker la clé dans une variable d'environnement sur Linux ou macOS

Pour convertir base64 et définir la variable d'environnement sur Linux oumacOS, exécutez la commande suivante.

```
export C3R_SHARED_SECRET="$(cat secret.key | base64)"
```

Étape 7 : Chiffrer les données

Pour effectuer cette étape, vous devez acquérir l'ID de AWS Clean Rooms collaboration et la clé secrète partagée. Pour de plus amples informations, veuillez consulter les Prérequis.

Dans l'exemple suivant, nous exécutons le `ads.csv` chiffrement en utilisant le schéma que nous avons créé appelé`ads.json`.

Pour chiffrer des données

1. Stockez la clé secrète partagée pour la collaboration dansÉtape 6 : Stocker la clé secrète partagée dans une variable d'environnement.
2. Sur la ligne de commande, entrez la commande suivante.

   ```
   java -jar c3r-cli.jar encrypt <name of input .csv file> --schema=<name of schema .json file> --id=<collaboration id> --output=<name of output.csv file> <optional flags>
   ```
3. Dans *<name of input .csv file>*, entrez le nom du fichier .csv d'entrée.
4. Pour`schema=`, entrez le nom du fichier de schéma de chiffrement .json.
5. Pour`id=`, entrez l'ID de collaboration.
6. Pour`output=`, entrez le nom du fichier de sortie (par exemple,`ads-output.csv`).

7. Incluez l'un des indicateurs de ligne de commande décrits dans Paramètres de calcul cryptographique etDrapeaux facultatifs dans le calcul cryptographique pour Clean Rooms.
8. Exécutez la commande .

Dans l'exemple deads.csv, nous exécutons la commande suivante.

java -jar c3r-cli.jar encrypt ***ads.csv*** --schema=***ads.json*** --id=***123e4567-e89b-42d3-a456-556642440000*** --output=***ads-output.csv***

Dans l'exemple desales.csv, nous exécutons la commande suivante.

java -jar c3r-cli.jar encrypt ***sales.csv*** --schema=***sales.json*** --id=***123e4567-e89b-42d3-a456-556642440000***

> **Note**
>
> Dans cet exemple, nous ne spécifiez pas de nom de fichier de sortie (`--output=`*`sales-output.csv`*). Par conséquent, le nom du fichier de sortie par défaut `name-of-file.out.csv` a été généré.

Vous êtes maintenant prêt à vérifier les données cryptées.

Étape 8 : vérifier le chiffrement des données

Pour vérifier que les données ont été cryptées

1. Affichez le fichier de données crypté (par exemple,`sales-output.csv`).
2. Vérifiez les colonnes suivantes :

   a. Colonne 1 — Chiffré (par exemple,`username_fingerprint`).

      Pour les fingerprint colonnes (HMAC), après le préfixe de version et de type (par exemple,`01:hmac:`), il y a 44 caractères de données codées en base64.

   b. Colonne 2 — Non chiffré (par exemple,`purchased`).

   c. Colonne 3 — Chiffré (par exemple,`product_sealed`).

      Pour les colonnes cryptées (SELECT), la longueur du cleartext plus tout remplissage après le préfixe de version et de type (par exemple,`01:enc:`) est directement proportionnelle à

la longueur de la cleartext colonne cryptée. En d'autres termes, la longueur correspond à la taille de l'entrée plus environ 33 % de surcharge due au codage.

Vous êtes maintenant prêt à :

1. Téléchargez les données cryptées sur S3.
2. Créez une AWS Glue table.
3. Créez une table configurée dans AWS Clean Rooms.

Le client de chiffrement C3R créera des fichiers temporaires qui ne contiennent pas de données non chiffrées (à moins que ces données ne soient également déchiffrées dans la sortie finale). Cependant, certaines valeurs cryptées peuvent ne pas être correctement renseignées. Les colonnes d'empreintes digitales peuvent contenir des valeurs dupliquées, même si le paramètre de collaboration l'`allowRepeatedFingerprintValueestfalse`. Ce problème se produit parce que le fichier temporaire est écrit avant que les longueurs de remplissage appropriées et les propriétés de suppression des doublons ne soient vérifiées.

Si le client de chiffrement C3R échoue ou est interrompu pendant le chiffrement, il peut s'arrêter après l'écriture du fichier temporaire, mais avant de vérifier ces propriétés et de supprimer les fichiers temporaires. Il se peut donc que ces fichiers temporaires soient toujours sur le disque. Dans ce cas, le contenu de ces fichiers ne protège pas les données en texte brut au même niveau que la sortie. En particulier, ces fichiers temporaires peuvent révéler des données en texte brut pour des analyses statistiques qui ne nuiraient pas au résultat final. L'utilisateur doit supprimer ces fichiers (en particulier une SQLite base de données) pour éviter qu'ils ne tombent entre des mains non autorisées.

(Facultatif) Créez un schéma (utilisateurs avancés)

La création manuelle d'un schéma est réservée aux utilisateurs expérimentés.

Vous trouverez ci-dessous une description du format de fichier de JSON schéma pour les fichiers d'entrée avec ou sans en-têtes de colonne. Les utilisateurs avancés peuvent directement écrire ou modifier le schéma s'ils le souhaitent.

> **Note**
>
> Le client de chiffrement C3R peut vous aider à créer un schéma par le biais du processus interactif décrit dans Exemple : génération d'un schéma de chiffrement avec des cleartext colonnes sealedfingerprint, et ou par la création d'un modèle de stub.

Schémas de tables cartographiées et positionnelles

La section suivante décrit deux types de schémas de table :

- Schéma de table mappé — Ce schéma est utilisé pour chiffrer les fichiers .csv avec une ligne d'en-tête et des fichiers. Apache Parquet
- Schéma de table positionnelle — Ce schéma est utilisé pour chiffrer des fichiers .csv sans ligne d'en-tête.

Le client de chiffrement C3R peut chiffrer un fichier tabulaire pour une collaboration. Pour ce faire, il doit disposer d'un fichier de schéma correspondant qui indique comment la sortie cryptée doit être dérivée de l'entrée.

Le client de chiffrement C3R peut aider à générer un schéma pour un `INPUT` fichier en exécutant la commande C3R encryption client schema sur la ligne de commande. Voici un exemple de commande`java -jar c3r-cli.jar schema --interactive INPUT`.

Le schéma indique les informations suivantes :

1. Quelles colonnes source correspondent à quelles colonnes transformées dans le fichier de sortie par le biais de leur nom d'en-tête (schémas mappés) ou de leur position (schémas positionnels)
2. Quelles colonnes cibles doivent rester cleartext
3. Quelles colonnes cibles doivent être cryptées pour les SELECT requêtes
4. Quelles colonnes cibles doivent être cryptées pour les JOIN requêtes

Ces informations sont codées dans un fichier de JSON schéma spécifique à une table, composé d'un seul objet dont `headerRow` le champ est une valeur booléenne. La valeur doit être `true` pour Parquet les fichiers et les fichiers .csv avec une ligne d'en-tête, et `false` sinon.

Schéma de table mappé

Le schéma mappé a la forme suivante.

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": STRING,
      "targetHeader": STRING,
      "type": TYPE,
      "pad": PAD
    },
    ...
  ]
}
```

Si tel `headerRow` est le cas`true`, le champ suivant de l'objet contient un tableau de schémas de colonnes qui mappent les en-têtes source aux en-têtes cibles (c'est-à-dire des JSON objets décrivant ce que les colonnes de sortie doivent contenir). `columns`

- `sourceHeader`— Le nom d'`STRING`en-tête de la colonne source dont les données sont dérivées.

> **Note**
>
> La même colonne source peut être utilisée pour plusieurs colonnes cibles.
> Une colonne du fichier d'entrée qui n'est répertoriée `sourceHeader` nulle part dans le schéma n'apparaît pas dans le fichier de sortie.

- `targetHeader`— Le nom d'`STRING`en-tête de la colonne correspondante dans le fichier de sortie.

> **Note**
>
> Ce champ est facultatif pour les schémas mappés. Si ce champ est omis, il `sourceHeader` est réutilisé comme nom d'en-tête dans la sortie. L'`_fingerprint`un ou l'autre `_sealed` est ajouté si la colonne de sortie est une fingerprint colonne ou une sealed colonne respectivement.

- `type`— Celui TYPE de la colonne cible dans le fichier de sortie. C'est-à-dire l'une des options `cleartext` ou `fingerprint` selon la manière dont la colonne sera utilisée dans le cadre de la collaboration. `sealed`
- `pad`— Champ d'un objet de schéma de colonne qui n'est présent que lorsque TYPE c'est le cas`sealed`. La valeur correspondante de PAD est un objet qui décrit la manière dont les données doivent être remplies avant d'être cryptées.

  ```
  {
    "type": PAD_TYPE,
    "length": INT
  }
  ```

  Pour spécifier le rembourrage avant le chiffrement, `type` `length` ils sont utilisés comme suit :

  - PAD_TYPEas `none` — Aucun remplissage ne sera appliqué aux données de la colonne et le `length` champ n'est pas applicable (c'est-à-dire omis).
  - PAD_TYPEas `fixed` — Les données de la colonne sont complétées au nombre `length` d'octets spécifié.
  - PAD_TYPEas `max` — Les données de la colonne sont complétées à la taille de l'octet de la valeur la plus longue plus un `length` octet supplémentaire.

Voici un exemple de schéma mappé, avec une colonne de chaque type.

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": "FullName",
      "targetHeader": "name",
      "type": "cleartext"
    },
    {
      "sourceHeader": "City",
      "targetHeader": "city_sealed",
      "type": "sealed",
      "pad": {
        "type": "max",
        "length": 16
      }
    },
```

```
    {
      "sourceHeader": "PhoneNumber",
      "targetHeader": "phone_number_fingerprint",
      "type": "fingerprint"
    },
    {
      "sourceHeader": "PhoneNumber",
      "targetHeader": "phone_number_sealed",
      "type": "sealed",
      "pad": {
        "type": "fixed",
        "length": 20
      }
    }
  ]
}
```

À titre d'exemple plus complexe, voici un exemple de fichier .csv avec des en-têtes.

```
FirstName,LastName,Address,City,State,PhoneNumber,Title,Level,Notes
Jorge,Souza,12345 Mills Rd,Anytown,SC,703-555-1234,CEO,10,
Paulo,Santos,0 Street,Anytown,MD,404-555-111,CIO,9,This is a really long note that
 could really be a paragraph
Mateo,Jackson,1 Two St,Anytown,NY,304-555-1324,COO,9,""
Terry,Whitlock4 N St,Anytown,VA,407-555-8888,EA,7,Secret notes
Diego,Ramirez,9 Hollows Rd,Anytown,VA,407-555-1222,SDE I,4,null
John,Doe,8 Hollows Rd,Anytown,VA,407-555-4321,SDE I,4,Jane's younger brother
Jane,Doe,8 Hollows Rd,Anytown,VA,407-555-4322,SDE II,5,John's older sister
```

Dans l'exemple de schéma mappé suivant, les colonnes `FirstName` et `LastName` sont des `cleartext` colonnes. La `State` colonne est cryptée en tant que `fingerprint` colonne et en tant que `sealed` colonne avec un rembourrage denone. Les autres colonnes sont omises.

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": "FirstName",
      "targetHeader": "GivenName",
      "type": "cleartext"
    },
    {
```

```
      "sourceHeader": "LastName",
      "targetHeader": "Surname",
      "type": "cleartext"
    },
    {
      "sourceHeader": "State",
      "targetHeader": "State_Join",
      "type": "fingerprint"
    },
    {
      "sourceHeader": "State",
      "targetHeader": "State",
      "type": "sealed",
      "pad": {
        "type": "none"
      }
    }
  ]
}
```

Le fichier .csv qui résulte du schéma mappé est le suivant.

```
givenname,surname,state_fingerprint,state
John,Doe,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv
+1Mk=,01:enc:FQ3n3Ahv9BQQNWQGcugeHzHYzEZE1vapHa2Uu4SRgSAtZ3qObjPA4TcsHt
+BOkMKBcnHWI13BeGG/SBqmj7vKpI=
Paulo,Santos,01:hmac:CHF4eIrtTNgAooU9v4h9Qjc
+txBnMidQTjdjWuaDTTA=,01:enc:KZ5n5GtaXACco65AXk48BQO2durDNR2ULc4YxmMC8NaZZKKJiksU1IwFadAvV4iBQ1
Mateo,Jackson,01:hmac:iIRnjfNBzryusIJ1w35lgNzeY1RQ1bSfq6PDHW8Xrbk=,01:enc:mLKpS5HIOSgphdEsrzhEd
eN9nBO2gAbIygt4OFn4LalYn9Xyj/XUWXlmn8zFe2T4kyDTD8kGOvpQEUGxAUFk=
Diego,Ramirez,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:rmZhT98Zm
+IIGw1UTjMIJP4IrW/AAltBLMXcHvnYfRgmWP623VFQ6aUnhsb2MDqEw4G5Uwg5rKKZepUxx5uKbfk=
Jorge,Souza,01:hmac:3BxJdXiFFyZ8HBbYNqqEhBVqhNOd7s2ZiKUe7QiTyo8=,01:enc:vVaqWC1VRbhvkf8gnuR7q0z
Terry,Whitlock01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:3c9VEWbODO/
xbQjdGuccLvI7oZTBdPU+SyrJIyr2kudfAxbuMQ2uRdU/q7rbgyJjxZS8M2U35ILJf/lDgTyg7cM=
Jane,Doe,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:9RWv46YLveykeNZ/
G0NdlYFg+AVdOnu05hHyAYTQkPLHnyX+0/jbzD/g9ZT8GCgVE9aB5bV4ooJIXHGBVMXcjrQ=
```

Schéma de tableau positionnel

Le schéma positionnel a la forme suivante.

```
{
```

```
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      },
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      }
    ],
    [],
    ...
  ]
}
```

Si `headerRow` tel est le cas`false`, le champ suivant de l'objet est`columns`, qui contient un tableau d'entrées. Chaque entrée est elle-même un tableau de zéro ou plusieurs schémas de colonnes positionnels (aucun `sourceHeader` champ), qui sont JSON des objets décrivant ce que la sortie doit contenir.

- `sourceHeader`— Le nom d'`STRING`en-tête de la colonne source dont les données sont dérivées.

  > **Note**
  >
  > Ce champ doit être omis dans les schémas de position. Dans les schémas positionnels, la colonne source est déduite par l'index correspondant de la colonne dans le fichier de schéma.

- `targetHeader`— Le nom d'`STRING`en-tête de la colonne correspondante dans le fichier de sortie.

  > **Note**
  >
  > Ce champ est obligatoire pour les schémas de position.

- `type`— Celui `TYPE` de la colonne cible dans le fichier de sortie. C'est-à-dire l'une des options `cleartext` ou `fingerprint` selon la manière dont la colonne sera utilisée dans le cadre de la collaboration. `sealed`

- `pad`— Champ d'un objet de schéma de colonne qui n'est présent que lorsque `TYPE` c'est le cas`sealed`. La valeur correspondante de `PAD` est un objet qui décrit la manière dont les données doivent être remplies avant d'être cryptées.

```
{
  "type": PAD_TYPE,
  "length": INT
}
```

  Pour spécifier le rembourrage avant le chiffrement, `type` `length` ils sont utilisés comme suit :

  - `PAD_TYPE`as `none` — Aucun remplissage ne sera appliqué aux données de la colonne et le `length` champ n'est pas applicable (c'est-à-dire omis).
  - `PAD_TYPE`as `fixed` — Les données de la colonne sont complétées au nombre `length` d'octets spécifié.
  - `PAD_TYPE`as `max` — Les données de la colonne sont complétées à la taille de l'octet de la valeur la plus longue plus un `length` octet supplémentaire.

    > **Note**
    >
    > `fixed`est utile si vous connaissez à l'avance la limite supérieure de la taille en octets des données de la colonne. Une erreur est générée si les données de cette colonne sont plus longues que celles spécifiées`length`.
    > `max`est pratique lorsque la taille exacte des données d'entrée est inconnue, car elle fonctionne quelle que soit la taille des données. Cependant, `max` cela nécessite un temps de traitement supplémentaire car il chiffre les données deux fois. `max`chiffre les données une fois lorsqu'elles sont lues dans le fichier temporaire et une fois que l'entrée de données la plus longue dans la colonne est connue.
    > De plus, la longueur de la valeur la plus longue n'est pas enregistrée entre les appels du client. Si vous prévoyez de chiffrer vos données par lots, ou de chiffrer régulièrement de nouvelles données, sachez que la longueur du texte chiffré peut varier d'un lot à l'autre.

Voici un exemple de schéma positionnel.

```
{
  "headerRow": false,
  "columns": [
```

```
    [
      {
        "targetHeader": "name",
        "type": "cleartext"
      }
    ],
    [
      {
        "targetHeader": "city_sealed",
        "type": "sealed",
        "pad": {
          "type": "max",
          "length": 16
        }
      }
    ],
    [
      {
        "targetHeader": "phone_number_fingerprint",
        "type": "fingerprint"
      },
      {
        "targetHeader": "phone_number_sealed",
        "type": "sealed",
        "pad": {
          "type": "fixed",
          "length": 20
        }
      }
    ]
  ]
}
```

À titre d'exemple complexe, voici un exemple de fichier .csv s'il ne contient pas la première ligne avec les en-têtes.

```
Jorge,Souza,12345 Mills Rd,Anytown,SC, 703 -555 -1234,CEO, 10,
Paulo,Santos, 0 Street,Anytown,MD, 404-555-111,CIO, 9,This is a really long note that
 could really be a paragraph
Mateo,Jackson, 1 Two St,Anytown,NY, 304-555-1324,COO, 9, ""
Terry,Whitlock, 4 N St,Anytown,VA, 407-555-8888,EA, 7,Secret notes
Diego,Ramirez, 9 Hollows Rd,Anytown,VA, 407-555-1222,SDE I, 4,null
John,Doe, 8 Hollows Rd,Anytown,VA, 407-555-4321,SDE I, 4,Jane's younger brother
```

```
Jane,Doe, 8 Hollows Rd,Anytown,VA, 407-555-4322,SDE II, 5,John's older sister
```

Le schéma positionnel se présente sous la forme suivante.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": "GivenName",
        "type": "cleartext"
      }
    ],
    [
      {
        "targetHeader": "Surname",
        "type": "cleartext"
      }
    ],
    [],
    [],
    [
      {
        "targetHeader": "State_Join",
        "type": "fingerprint"
      },
      {
        "targetHeader": "State",
        "type": "sealed",
        "pad": {
          "type": "none"
        }
      }
    ],
    [],
    [],
    [],
    []
  ]
}
```

Le schéma précédent produit le fichier de sortie suivant avec une ligne d'en-tête contenant les en-têtes cibles spécifiés.

```
givenname,surname,state_fingerprint,state
Mateo,Jackson,01:hmac:iIRnjfNBzryusIJ1w35lgNzeY1RQ1bSfq6PDHW8Xrbk=,01:enc:ENS6QD3cMVl9vQEGfe9MN
Q8m/Y5SA89dJwKpT5rGPp8e36h6klwDoslpFzGvU0=
Jorge,Souza,01:hmac:3BxJdXiFFyZ8HBbYNqqEhBVqhNOd7s2ZiKUe7QiTyo8=,01:enc:LKo0zirq2+
+XEIIIMNRjAsGMdyWUDwYaum0B+IFP+rUf1BNeZDJjtFe1Z+zbZfXQWwJy52Rt7HqvAb2WIK1oMmk=
Paulo,Santos,01:hmac:CHF4eIrtTNgAooU9v4h9Qjc
+txBnMidQTjdjWuaDTTA=,01:enc:MyQKyWxJ9kvK1xDQQtXlUNwv3F+yrBRr0xrUY/1BGg5KFgOn9pK+MZ7g
+ZNqZEPcPz4lht1u0t/wbTaqzOCLXFQ=
Jane,Doe,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:Pd8sbITBfb0/
ttUB4svVsgoYkDfnDvgkvxzeci0Yxq54rLSwccy1o3/B50C3cpkkn56dovCwzgmmPNwrmCmYtb4=
Terry,Whitlock01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv
+1Mk=,01:enc:Qmtzu3B3GAXKh2KkRYTiEAaMopYedsSdF2e/
ADUiBQ9kv2CxKPzWyYTD3ztmKPMka19dHre5VhUHNpO3O+j1AQ8=
Diego,Ramirez,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:ysdg
+GHKdeZrS/geBIooOEPLHG68MsWpx1dh3xjb+fG5rmFmqUcJLNuuYBHhHAlxchM2WVeV1fmHkBX3mvZNvkc=
John,Doe,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:9uX0wZuO7kAPAx
+Hf6uvQownkWqFSKtWS7gQIJSe5aXFquKWCK6yZN0X5Ea2N3bn03Uj1kh0agDWoiP9FRZGJA4=
```

Déchiffrer des tables de données avec le client de chiffrement C3R

Suivez cette procédure pour les collaborations qui utilisent l'informatique cryptographique pour Clean Rooms et le client de chiffrement C3R pour chiffrer des tables de données. Utilisez cette procédure après avoir demandé des données dans le cadre de la collaboration.

La clé secrète partagée et l'identifiant de collaboration sont requis pour cette procédure.

Le membre qui peut recevoir les résultats déchiffre les données à l'aide de la même clé secrète partagée et du même identifiant de collaboration que ceux utilisés pour chiffrer les données de la collaboration.

> **Note**
>
> AWS Clean Rooms les collaborations limitent déjà les personnes autorisées à exécuter et à consulter les résultats des requêtes. Pour effectuer le déchiffrement, toute personne ayant accès à ces résultats a besoin de la même clé secrète partagée et du même identifiant de collaboration que ceux utilisés pour chiffrer les données.

Pour déchiffrer une table de données cryptée

1. (Facultatif) Affichez les commandes disponibles dans le client de chiffrement C3R.
2. (Facultatif) Accédez au répertoire souhaité et exécutez `ls` (macOS) ou `dir` (Windows).

   - Vérifiez que le c3r-cli.jar fichier et le fichier de données des résultats de requête chiffrés se trouvent dans le répertoire souhaité.

   > **Note**
   >
   > Si les résultats de la requête sont téléchargés depuis l'interface de la AWS Clean Rooms console, ils se trouvent probablement dans le dossier Téléchargements de votre compte utilisateur. (Par exemple, le dossier Téléchargements de votre répertoire utilisateur sur Windows etmacOS.) Nous vous recommandons de déplacer le fichier des résultats de la requête dans le même dossier que lec3r-cli.jar.

3. Stockez la clé secrète partagée dans la variable d'`C3R_SHARED_SECRET`environnement. Pour de plus amples informations, veuillez consulter Étape 6 : Stocker la clé secrète partagée dans une variable d'environnement.
4. À partir du AWS Command Line Interface (AWS CLI), exécutez la commande suivante.

   java -jar c3r-cli.jar decrypt ***<name of input .csv file>*** --id=***<collaboration id>*** --output=***<output file name>***
5. Remplacez chacun *`user input placeholder`* avec vos propres informations :

   a. Pour`id=`, entrez l'ID de collaboration.

   b. Pour`output=`, entrez le nom du fichier de sortie (par exemple,`results-decrypted.csv`).

      Si vous ne spécifiez pas de nom de sortie, un nom par défaut est affiché dans le terminal.

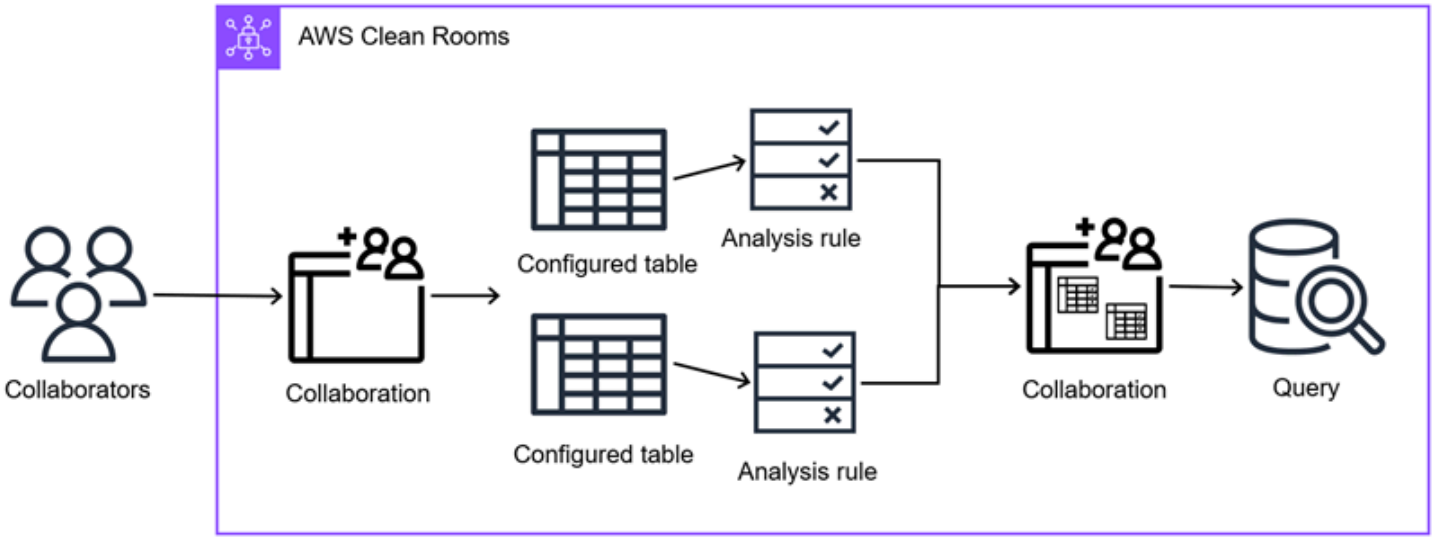
   c. Affichez les données déchiffrées dans le fichier de sortie spécifié à l'aide de votre application préférée CSV ou de Parquet visualisation (éditeur de texte ou autre application, par exemple). Microsoft Excel

Utilisation des données d'événements dans AWS Clean Rooms

Avec AWS Clean Rooms, vous pouvez effectuer une analyse d'agrégation sur les données d'événements, telles que le nombre d'achats par rapport au nombre d'achats. Vous pouvez également effectuer une analyse de liste sur les données d'événements, par exemple en enrichissant les données clients qui se chevauchent des données de segment en CRM données. Vous pouvez également effectuer des requêtes personnalisées et définir une confidentialité différentielle sur les données d'événements, telles que les données d'audience et les attributs de segment.

Tout d'abord, vous créez une collaboration AWS Clean Rooms et vous y ajoutez celle que Comptes AWS vous souhaitez inviter, ou vous rejoignez une collaboration à laquelle vous êtes invité en créant un abonnement. Ensuite, vous et l'autre membre de la collaboration créez des tables configurées. Vous ajoutez à la fois une règle d'analyse aux tables configurées (agrégation, liste ou personnalisée) et associez les tables configurées à la collaboration. Enfin, le membre qui peut effectuer une requête exécute une requête dans les deux tables de données.

Le schéma suivant récapitule comment utiliser les données d'événements dans AWS Clean Rooms.



Rubriques

- Création d'une table configurée dans AWS Clean Rooms
- Ajouter une règle d'analyse à une table configurée
- Associer une table configurée à une collaboration
- Ajouter une règle d'analyse de collaboration à une table configurée

- Configuration d'une politique de confidentialité différentielle (facultatif)
- Gestion des tables configurées dans AWS Clean Rooms

Création d'une table configurée dans AWS Clean Rooms

Une table configurée est une référence à une table existante dans le AWS Glue Data Catalog. Il contient une règle d'analyse qui détermine la manière dont les données peuvent être consultées. AWS Clean Rooms Les tables configurées peuvent être associées à une ou plusieurs collaborations.

Utilisez la génération de statistiques fournie par AWS Glue pour calculer les statistiques au niveau des colonnes pour les tables. AWS Glue Data Catalog Après avoir AWS Glue généré des statistiques pour les tables du catalogue de données, Amazon Redshift Spectrum utilise automatiquement ces statistiques pour optimiser le plan de requête. Pour plus d'informations sur le calcul des statistiques au niveau des colonnes à l'aide de statistiques AWS Glue, consultez la section Optimisation des performances des requêtes à l'aide des statistiques des colonnes dans le Guide de l'AWS Glue utilisateur. Pour plus d'informations à ce sujet AWS Glue, consultez le guide du développeur de AWS Glue.

Dans cette procédure, le membre effectue les tâches suivantes :

- Configure une AWS Glue table existante à utiliser dans. AWS Clean Rooms (Cette étape peut être effectuée avant ou après avoir rejoint une collaboration, sauf si vous utilisez l'informatique cryptographique pourClean Rooms.)

> **Note**
>
> AWS Clean Rooms supporte AWS Glue les tables. Pour plus d'informations sur l'introduction de vos données AWS Glue, consultezÉtape 3 : Chargez votre tableau de données sur Amazon S3.

- Nomme la table configurée et choisit les colonnes à utiliser dans la collaboration.

La procédure suivante part du principe que :

- Le membre de la collaboration a déjà chargé ses tables de données sur Amazon S3 et en a créé une AWS Glue.

- (Facultatif) Pour les tables de données chiffrées uniquement, le membre de la collaboration a déjà préparé des tables de données chiffrées à l'aide du client de chiffrement C3R.

Pour créer une table configurée dans AWS Clean Rooms

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Tables configurées.
3. Dans le coin supérieur droit, choisissez Configurer une nouvelle table.
4. Pour Configurer une nouvelle table, pour Choisir AWS Glue une table :

   a. Choisissez la base de données que vous souhaitez configurer dans la liste déroulante.

   b. Choisissez la table que vous souhaitez configurer dans la liste déroulante.

> **Note**
>
> Pour vérifier que ce tableau est correct, effectuez l'une des opérations suivantes :
>
> - Choisissez Afficher dans AWS Glue.
> - Activez Afficher le schéma pour afficher le schéma.

5. Pour les colonnes autorisées dans les collaborations, sélectionnez Toutes les colonnes ou Liste personnalisée.

Si vous choisissez…	Alors...
Toutes les colonnes	Toutes les colonnes peuvent être utilisées dans AWS Clean Rooms (sous réserve des règles d'analyse).
Liste personnalisée	Choisissez une ou plusieurs colonnes que vous souhaitez autoriser dans la liste déroulante Spécifier les colonnes autorisées.

6. Pour les détails de la table configurée,

   a. Entrez un nom pour la table configurée.

Vous pouvez utiliser le nom par défaut ou renommer cette table.

b. Entrez une description de la table.

La description permet de différencier les autres tables configurées portant des noms similaires.

c. Si vous souhaitez activer les balises pour la ressource de table configurée, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

7. Choisissez Configurer une nouvelle table.

Maintenant que vous avez créé une table configurée, vous êtes prêt à :

- Ajouter une règle d'analyse à la table configurée
- Associer la table configurée à une collaboration

Ajouter une règle d'analyse à une table configurée

Les sections suivantes décrivent comment ajouter une règle d'analyse à votre table configurée. En définissant les règles d'analyse, vous pouvez autoriser le membre autorisé à exécuter des requêtes correspondant à une règle d'analyse spécifique prise en charge par. AWS Clean Rooms

AWS Clean Rooms prend en charge les types de règles d'analyse suivants :

- Règle d'analyse d'agrégation
- Règle d'analyse des listes
- Règle d'analyse personnalisée dans AWS Clean Rooms

Il ne peut y avoir qu'une seule règle d'analyse par table configurée. Vous pouvez configurer la règle d'analyse à tout moment avant d'associer les tables configurées à la collaboration.

> **Important**
>
> Si vous utilisez l'informatique cryptographique pour la collaboration Clean Rooms et que vous avez chiffré des tables de données, la règle d'analyse que vous ajoutez à la table configurée cryptée doit être cohérente avec la manière dont les données ont été cryptées. Par exemple,

si vous avez chiffré les données pour SELECT (règle d'analyse d'agrégation), vous ne devez pas ajouter la règle d'analyse pour JOIN (règle d'analyse de liste).

Rubriques

Ajouter une règle d'analyse d'agrégation à une table (flux guidé)

La règle d'analyse d'agrégation autorise les requêtes qui regroupent les statistiques sans révéler d'informations au niveau des lignes en utilisant COUNT et en utilisant des AVG dimensions facultatives. SUM

Cette procédure décrit le processus d'ajout d'une règle d'analyse d'agrégation à votre table configurée à l'aide de l'option Flux guidé de la AWS Clean Rooms console.

Pour ajouter la règle d'analyse d'agrégation à une table (flux guidé)

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Tables configurées.
3. Choisissez le tableau configuré.
4. Sur la page détaillée de la table configurée, choisissez Configurer la règle d'analyse.
5. À l'étape 1 : Choisissez le type, sous Type, laissez l'option d'agrégation sélectionnée par défaut.
6. Sous Méthode de création, sélectionnez Flux guidé, puis Suivant.
7. Dans Étape 2 : Spécifier les contrôles de requête, pour les fonctions d'agrégation :

    a. Choisissez une fonction d'agrégation dans le menu déroulant :

    - COUNT
    - COUNT DISTINCT

- SUM
- SUM DISTINCT
- AVG

b. Choisissez les colonnes qui peuvent être utilisées dans la fonction d'agrégation dans le menu déroulant Colonnes.

c. (Facultatif) Choisissez Ajouter une autre fonction pour ajouter une autre fonction d'agrégation et associer une ou plusieurs colonnes à cette fonction.

> **Note**
>
> Au moins une fonction d'agrégation est requise.

d. (Facultatif) Choisissez Supprimer pour supprimer une fonction d'agrégation.

8. Pour les commandes Join,

a. Choisissez une option pour Autoriser la table elle-même à être interrogée :

Si vous choisissez…	Alors...
Non, seul le chevauchement peut être interrogé	La table ne peut être interrogée que lorsqu'elle est jointe à une table appartenant au membre qui peut effectuer la requête.
Oui	La table peut être interrogée seule ou lorsqu'elle est jointe à d'autres tables.

b. Sous Spécifier les colonnes de jointure, choisissez les colonnes que vous souhaitez autoriser à utiliser dans l'INNERJOINinstruction.

Cette option est facultative si vous avez sélectionné Oui à l'étape précédente.

c. Sous Spécifier les opérateurs autorisés pour la mise en correspondance, choisissez quels opérateurs, le cas échéant, peuvent être utilisés pour faire correspondre plusieurs colonnes de jointure. Si vous sélectionnez deux JOIN colonnes ou plus, l'un de ces opérateurs est requis.

Si vous choisissez…	Alors...
AND	Vous pouvez inclure `AND` dans le `INNER JOIN` match des conditions permettant de joindre une colonne à une autre entre les tables.
OU	Vous pouvez inclure `OR` dans les condition s de `INNER JOIN` correspondance pour combiner plusieurs correspondances de colonnes entre les tables. Cet opérateur logique est utile pour obtenir un taux de correspondance plus élevé.

9. (Facultatif) Pour les contrôles de dimension, dans la liste déroulante Spécifier les colonnes de dimension, choisissez les colonnes que vous souhaitez autoriser à utiliser dans l'SELECTinstruction, ainsi que dans les ORDER BY parties WHERE GROUPBY, et de la requête.

> **Note**
>
> La fonction d'agrégation ou les colonnes de jointure ne peuvent pas être utilisées comme colonnes de dimension.

10. Pour les fonctions scalaires, choisissez une option pour Quelles fonctions scalaires souhaitez-vous autoriser ?

Si vous choisissez…	Alors...
Tous sont actuellement pris en charge par AWS Clean Rooms	Vous autorisez toutes les fonctions scalaires actuellement prises en charge par AWS Clean Rooms. • Vous pouvez choisir Afficher la liste pour voir la liste complète des fonctions

Si vous choisissez…	Alors...
	scalaires prises en charge dans AWS Clean Rooms.
Une liste personnalisée	Vous pouvez personnaliser les fonctions scalaires à autoriser. • Choisissez une ou plusieurs options dans la liste déroulante Spécifier les fonctions scalaires autorisées.
Aucun	Vous ne souhaitez autoriser aucune fonction scalaire.

Pour de plus amples informations, veuillez consulter Fonctions scalaires.

11. Choisissez Suivant.
12. Dans Étape 3 : Spécifier les contrôles des résultats de requête, pour les contraintes d'agrégation :
    a. Sélectionnez la liste déroulante pour chaque nom de colonne.
    b. Sélectionnez la liste déroulante pour chaque nombre minimum de valeurs distinctes qui doivent être respectées pour que chaque ligne de sortie soit renvoyée, une fois la COUNT DISTINCT fonction appliquée à celle-ci.
    c. Choisissez Ajouter une contrainte pour ajouter d'autres contraintes d'agrégation.
    d. (Facultatif) Choisissez Supprimer pour supprimer une contrainte d'agrégation.
13. Pour les analyses supplémentaires appliquées aux résultats, sélectionnez une option en fonction de votre objectif.

Votre objectif	Option recommandée
Autoriser uniquement les requêtes directes sur cette table. Empêchez l'exécution d'analyses supplémentaires sur les résultats des requêtes. La table ne peut être utilisée que pour des requêtes directes.	Non autorisé

Votre objectif	Option recommandée
Autorisez mais n'exigez pas à la fois des requêtes directes et des analyses supplémentaires sur cette table.	Autorisé
Exiger que la table ne puisse être utilisée que dans des requêtes directes traitées avec l'une des analyses supplémentaires requises. Les requêtes directes sur cette table doivent être traitées ultérieurement avant de pouvoir être renvoyées.	Obligatoire

14. Choisissez Suivant.
15. Dans Étape 4 : révision et configuration, passez en revue les sélections que vous avez effectuées lors des étapes précédentes, modifiez-les si nécessaire, puis choisissez Configurer la règle d'analyse.

Un message de confirmation s'affiche indiquant que vous avez correctement configuré une règle d'analyse d'agrégation pour la table.

Ajouter une règle d'analyse de liste à un tableau (flux guidé)

La règle d'analyse de liste autorise les requêtes qui produisent des listes au niveau des lignes indiquant le chevauchement entre la table associée et une table du membre autorisé à effectuer la requête.

Cette procédure décrit le processus d'ajout de la règle d'analyse de liste à votre table configurée à l'aide de l'option Flux guidé de la AWS Clean Rooms console.

Pour ajouter une règle d'analyse de liste à un tableau (flux guidé)

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Tables configurées.
3. Choisissez le tableau configuré.
4. Sur la page détaillée de la table configurée, choisissez Configurer la règle d'analyse.
5. À l'étape 1 : Choisissez le type, sous Type, choisissez l'option Liste.

6. Sous Méthode de création, sélectionnez Flux guidé, puis Suivant.
7. Dans Étape 2 : Spécifier les contrôles de requête, pour les contrôles de jointure :

   a. Sous Spécifier les colonnes de jointure, choisissez les colonnes que vous souhaitez autoriser à utiliser dans l'INNERJOINinstruction.

   b. Sous Spécifier les opérateurs autorisés pour la mise en correspondance, choisissez quels opérateurs, le cas échéant, peuvent être utilisés pour faire correspondre plusieurs colonnes de jointure. Si vous sélectionnez deux JOIN colonnes ou plus, l'un de ces opérateurs est requis.

Si vous choisissez…	Alors...
AND	Vous pouvez inclure `AND` dans le `INNER JOIN` match des conditions permettant de joindre une colonne à une autre entre les tables.
OU	Vous pouvez inclure `OR` dans les condition s de `INNER JOIN` correspondance pour combiner plusieurs correspondances de colonnes entre les tables. Cet opérateur logique est utile pour obtenir un taux de correspondance plus élevé.

8. (Facultatif) Pour les contrôles de liste, dans la liste déroulante Spécifier les colonnes de liste, choisissez les colonnes que vous souhaitez autoriser à utiliser dans le résultat de la requête (c'est-à-dire utilisées dans l'SELECTinstruction) ou utilisées pour filtrer les résultats (c'est-à-dire l'WHEREinstruction).
9. Choisissez Suivant.
10. Dans Étape 3 : Spécifier les contrôles des résultats de requête, pour Analyses supplémentaires appliquées à la sortie, sélectionnez une option en fonction de votre objectif.

Votre objectif	Option recommandée
Autoriser uniquement les requêtes directes sur cette table. Empêchez l'exécution d'analyses supplémentaires sur les résultats	Non autorisé

Votre objectif	Option recommandée
des requêtes. La table ne peut être utilisée que pour des requêtes directes.	
Autorisez mais n'exigez pas à la fois des requêtes directes et des analyses supplémen taires sur cette table.	Autorisé
Exiger que la table ne puisse être utilisée que dans des requêtes directes traitées avec l'une des analyses supplémentaires requises. Les requêtes directes sur cette table doivent être traitées ultérieurement avant de pouvoir être renvoyées.	Obligatoire

11. Dans Étape 4 : révision et configuration, passez en revue les sélections que vous avez effectuées lors des étapes précédentes, modifiez-les si nécessaire, puis choisissez Configurer la règle d'analyse.

Un message de confirmation s'affiche indiquant que vous avez correctement configuré une règle d'analyse de liste pour la table.

Ajouter une règle d'analyse personnalisée à un tableau (flux guidé)

La règle d'analyse personnalisée permet d'effectuer SQL des requêtes personnalisées sur une table configurée. La règle d'analyse personnalisée est requise si vous utilisez :

- modèles d'analyse : pour autoriser un ensemble spécifique de SQL requêtes préapprouvées ou un ensemble spécifique de comptes pouvant fournir des requêtes utilisant vos données
- confidentialité différentielle — pour protéger contre les tentatives d'identification des utilisateurs

Cette procédure décrit le processus d'ajout de la règle d'analyse personnalisée à votre table configurée à l'aide de l'option Flux guidé de la AWS Clean Rooms console.

Pour ajouter une règle d'analyse personnalisée à un tableau (flux guidé)

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Tables configurées.
3. Choisissez le tableau configuré.
4. Sur la page détaillée de la table configurée, choisissez Configurer la règle d'analyse.
5. À l'étape 1 : Choisissez le type, sous Type, choisissez l'option Personnalisée.
6. Sous Méthode de création, sélectionnez Flux guidé, puis Suivant.
7. À l'étape 2 : définir la confidentialité différentielle, déterminez si vous souhaitez activer ou désactiver la confidentialité différentielle. La confidentialité différentielle est une technique mathématiquement éprouvée pour protéger vos données contre les attaques de réidentification.

   a. Pour une confidentialité différentielle :

Si tu...	Ensuite, choisissez...
Disposez de données de niveau utilisateur et vous souhaitez être protégé contre les tentatives de réidentification	Allumez
Vous ne disposez pas de données de niveau utilisateur ou n'avez pas besoin de protection contre les tentatives de réidentif ication	Éteindre

   b. Si vous avez choisi d'activer la confidentialité différentielle, sélectionnez la colonne Identifiant utilisateur qui contient l'identifiant unique de vos utilisateurs, par exemple la `user_id` colonne dont vous souhaitez protéger la confidentialité.

      Pour activer la confidentialité différentielle pour deux tables ou plus dans le cadre d'une collaboration, vous devez configurer la même colonne que la colonne Identifiant utilisateur dans les deux règles d'analyse afin de conserver une définition cohérente des utilisateurs entre les tables. En cas de mauvaise configuration, le membre autorisé à effectuer une requête reçoit un message d'erreur indiquant qu'il a le choix entre deux colonnes afin de calculer le nombre de contributions des utilisateurs (par exemple, le nombre d'impressions publicitaires effectuées par un utilisateur) lors de l'exécution de la requête.

   c. Choisissez Suivant.
8. Dans Étape 3 : Spécifier les contrôles de requête,

   a. Pour Type de contrôle, choisissez une option en fonction de votre objectif.

Votre objectif	Option
Passez en revue chaque nouveau modèle d'analyse avant de l'exécuter sur votre table configurée	Passez en revue chaque nouvelle analyse avant de l'autoriser à être exécutée sur cette table
Permettez d'exécuter n'importe quel modèle d'analyse ou requête directe sur votre table configurée	Autoriser toutes les requêtes créées par des collaborateurs spécifiques à s'exécuter sans révision sur ce tableau

b. Sélectionnez l'une des méthodes suivantes :

Si tu as choisi...	Alors...
Passez en revue chaque nouvelle analyse avant de l'autoriser à être exécutée sur cette table	Sous Modèles d'analyse autorisés à être exécutés, choisissez Ajouter un modèle d'analyse, puis choisissez le modèle de collaboration et d'analyse appropriés dans les listes déroulantes.
Autoriser toutes les requêtes créées par des collaborateurs spécifiques à s'exécuter sans révision sur ce tableau	Sous Comptes AWS Autorisé à créer une requête, choisissez Ajouter Compte AWS, puis choisissez l'Compte AWS ID approprié.

9. Choisissez Suivant.
10. Dans Étape 4 : Spécifier les contrôles des résultats de requête,

a. Pour les colonnes non autorisées en sortie, choisissez-en une en fonction de votre objectif.

Votre objectif	Option recommandée
Autoriser le renvoi de toutes les colonnes dans les sorties de requête	Aucun
Interdire le renvoi de certaines colonnes dans les résultats des requêtes	Liste personnalisée

b. Sélectionnez l'une des méthodes suivantes :

Si tu as choisi...	Alors...
Aucun	Passez à Analyses supplémentaires appliquées à la sortie
Liste personnalisée	Sous Spécifier les colonnes interdites, choisissez les colonnes que vous souhaitez supprimer des résultats de requête.

c. Pour les analyses supplémentaires appliquées à la sortie, sélectionnez une option en fonction de votre objectif.

Votre objectif	Option recommandée
Autoriser uniquement les requêtes directes sur cette table. Empêchez l'exécution d'analyses supplémentaires sur les résultats des requêtes. La table ne peut être utilisée que pour des requêtes directes.	Non autorisé
Autorisez mais n'exigez pas à la fois des requêtes directes et des analyses supplémentaires sur cette table.	Autorisation
Exiger que la table ne puisse être utilisée que dans des requêtes directes traitées avec l'une des analyses supplémentaires requises. Les requêtes directes sur cette table doivent être traitées ultérieurement avant de pouvoir être renvoyées.	Obligatoire

11. Choisissez Suivant.

12. Dans Étape 5 : révision et configuration, passez en revue les sélections que vous avez effectuées lors des étapes précédentes, modifiez-les si nécessaire, puis choisissez Configurer la règle d'analyse.

Un message de confirmation s'affiche indiquant que vous avez correctement configuré une règle d'analyse personnalisée pour la table.

Ajouter une règle d'analyse à une table (JSONéditeur)

La procédure suivante montre comment ajouter une règle d'analyse à une table à l'aide de l'option d'JSONéditeur de la AWS Clean Rooms console.

Pour ajouter une agrégation, une liste ou une règle d'analyse personnalisée à une table (JSONéditeur)

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Tables configurées.
3. Choisissez le tableau configuré.
4. Sur la page détaillée de la table configurée, choisissez Configurer la règle d'analyse.
5. À l'étape 1 : Choisissez le type, sous Type, choisissez l'option Agrégation, Liste ou Personnalisation.
6. Sous Méthode de création, sélectionnez JSONéditeur, puis cliquez sur Suivant.
7. À l'étape 2 : Spécifier les contrôles, vous pouvez choisir d'insérer une structure de requête (Insérer un modèle) ou d'insérer un fichier (Importer depuis un fichier).

Si vous choisissez…	Alors...
Insérer un modèle	1. Spécifiez les paramètres de la règle d'analyse sélectionnée dans la définition de la règle d'analyse. 2. Vous pouvez appuyer sur Ctrl + barre d'espace pour activer la saisie automatiq ue.

Si vous choisissez…	Alors...
	Pour plus d'informations sur les paramètres des règles d'analyse d'agrégation, consultez Règle d'analyse d'agrégation : contrôles des requêtes. Pour plus d'informations sur les paramètres des règles d'analyse de liste, consultezRègle d'analyse des listes : contrôles des requêtes.
Importer depuis un fichier	1. Sélectionnez votre JSON fichier sur votre disque local. 2. Choisissez Ouvrir. La définition de la règle d'analyse affiche la règle d'analyse du fichier chargé.

8. Choisissez Suivant.
9. Dans Étape 3 : révision et configuration, passez en revue les sélections que vous avez effectuées lors des étapes précédentes, modifiez-les si nécessaire, puis choisissez Configurer la règle d'analyse.

Vous recevez un message de confirmation indiquant que vous avez correctement configuré une règle d'analyse pour la table.

Étapes suivantes

Maintenant que vous avez configuré une règle d'analyse pour votre table configurée, vous êtes prêt à :

- Associer une table configurée à une collaboration
- Interroger les tables de données (en tant que membre pouvant effectuer des requêtes)

Associer une table configurée à une collaboration

Après avoir créé une table configurée et y avoir ajouté une règle d'analyse, vous pouvez l'associer à une collaboration et attribuer AWS Clean Rooms un rôle de service pour accéder à vos AWS Glue tables.

> **Note**
>
> Ce rôle de service dispose d'autorisations d'accès aux tables. Le rôle de service ne peut être assumé que AWS Clean Rooms pour exécuter les requêtes autorisées au nom du membre autorisé à effectuer des requêtes. Aucun membre de la collaboration (autre que le propriétaire des données) n'a accès aux tables sous-jacentes de la collaboration. Le propriétaire des données peut activer la confidentialité différentielle pour que ses tables puissent être consultées par d'autres membres.

> **Important**
>
> Avant d'associer les AWS Glue tables configurées à la collaboration, l'emplacement des AWS Glue tables doit pointer vers un dossier Amazon Simple Storage Service (Amazon S3) et non vers un seul fichier. Vous pouvez vérifier cet emplacement en consultant le tableau dans la AWS Glue console à l'adresse https://console.aws.amazon.com/glue/.

> **Note**
>
> Si vous avez configuré le chiffrement AWS Glue et créé un rôle de service, vous devez autoriser ce rôle à accéder AWS KMS keys pour déchiffrer AWS Glue les tables.
> Si vous avez associé une table configurée soutenue par un ensemble de données Amazon S3 AWS KMS chiffré, vous devez autoriser le rôle à utiliser la KMS clé pour déchiffrer les données Amazon S3.
> Pour plus d'informations, consultez la section Configuration du chiffrement AWS Glue dans le Guide du AWS Glue développeur.

Les rubriques suivantes décrivent comment associer une table configurée à une collaboration à l'aide de la AWS Clean Rooms console :

Rubriques

Pour plus d'informations sur la façon d'associer vos tables configurées à la collaboration à l'aide du AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Associer une table configurée depuis la page détaillée de la table configurée

Pour associer AWS Glue des tables à la collaboration depuis la page détaillée des tables configurée

1. Connectez-vous à la AWS Clean Rooms 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, choisissez Tables configurées.
3. Choisissez le tableau configuré.
4. Sur la page détaillée du tableau configuré, choisissez Associer à la collaboration.
5. Dans la boîte de dialogue Associer la table à la collaboration, choisissez la collaboration dans la liste déroulante.
6. Choisissez Choisir une collaboration.

   Sur la page Associer une table, le nom de la table configurée que vous avez choisie apparaît dans la section Choisir une table configurée.
7. Pour Choisir une table configurée, procédez comme suit :

Si vous souhaitez...	Alors...
Configuration d'une nouvelle table	Choisissez Configurer le tableau et suivez les instructions de la page Configurer le tableau.
Afficher le schéma et la règle d'analyse pour la table configurée	Activez Afficher le schéma et la règle d'analyse.

8. Spécifiez les autorisations d'accès au service en sélectionnant Créer et utiliser un nouveau rôle de service ou Utiliser un rôle de service existant.

Si vous choisissez…	Alors...
Création et utilisation d'un nouveau rôle de service	• AWS Clean Rooms crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut est `cleanrooms-<timestamp>` • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, vous pouvez sélectionner Ces données sont cryptées avec une KMS clé, puis saisir une clé AWS KMS key qui sera utilisée pour déchiffrer vos données saisies.

Si vous choisissez…	Alors...
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. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. Par défaut, AWS Clean Rooms ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires. 3. (Facultatif) Cochez la case Ajouter une politique préconfigurée avec les autorisat ions nécessaires à ce rôle pour ajouter attacher les autorisations nécessaires au rôle. Vous devez disposer des autorisat ions nécessaires pour modifier les rôles et créer des politiques.

> **Note**
>
> - AWS Clean Rooms nécessite des autorisations pour effectuer des requêtes conformément aux règles d'analyse. Pour plus d'informations sur les autorisations pour AWS Clean Rooms, voirAWS politiques gérées pour AWS Clean Rooms.

- Si le rôle ne dispose pas d'autorisations suffisantes pour AWS Clean Rooms, vous recevez un message d'erreur indiquant que le rôle ne dispose pas d'autorisations suffisantes pour AWS Clean Rooms. La politique de rôle doit être ajoutée avant de continuer.
- Si vous ne pouvez pas modifier la politique de rôle, vous recevez un message d'erreur indiquant que AWS Clean Rooms la politique pour le rôle de service est introuvable.

9. Si vous souhaitez activer les balises pour la ressource d'association de tables configurée, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
10. Choisissez Associer une table.

Associer une table configurée depuis la page détaillée de la collaboration

Pour associer AWS Glue des tables à la collaboration depuis la page détaillée de la collaboration

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Tables, choisissez Associer une table.
5. Pour Choisir une table configurée, procédez comme suit :

Si vous souhaitez...	Alors...
Choisissez une table configurée existante	Choisissez le nom de la table configurée que vous souhaitez associer à la collaboration dans la liste déroulante.
Configuration d'une nouvelle table	Choisissez Configurer le tableau et suivez les instructions de la page Configurer le tableau.
Afficher le schéma et la règle d'analyse pour la table configurée	Activez Afficher le schéma et la règle d'analyse.

6. Pour plus de détails sur l'association des tables,

a. Entrez un nom pour la table associée.

   Vous pouvez utiliser le nom par défaut ou renommer cette table.

b. (Facultatif) Entrez une description de la table.

   La description facilite la rédaction de requêtes.

7. Spécifiez les autorisations d'accès au service en sélectionnant Créer et utiliser un nouveau rôle de service ou Utiliser un rôle de service existant.

Si vous choisissez…	Alors...
Création et utilisation d'un nouveau rôle de service	• AWS Clean Rooms crée un rôle de service avec la politique requise pour cette table. • Le nom du rôle de service par défaut est`cleanrooms-<timestamp>` . • Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. • Si vos données d'entrée sont cryptées, vous pouvez sélectionner Ces données sont cryptées avec une KMS clé, puis saisir une clé AWS KMS key 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.

Si vous choisissez…	Alors...
	2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. Par défaut, AWS Clean Rooms ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires. 3. (Facultatif) Cochez la case Ajouter une politique préconfigurée avec les autorisat ions nécessaires à ce rôle pour ajouter attacher les autorisations nécessaires au rôle. Vous devez disposer des autorisat ions nécessaires pour modifier les rôles et créer des politiques.

> **Note**
>
> - AWS Clean Rooms nécessite des autorisations pour effectuer des requêtes conformément aux règles d'analyse. Pour plus d'informations sur les autorisations pour AWS Clean Rooms, voirAWS politiques gérées pour AWS Clean Rooms.
> - Si le rôle ne dispose pas d'autorisations suffisantes pour AWS Clean Rooms, vous recevez un message d'erreur indiquant que le rôle ne dispose pas d'autorisations suffisantes pour AWS Clean Rooms. La politique de rôle doit être ajoutée avant de continuer.
> - Si vous ne parvenez pas à modifier la politique de rôle, vous recevez un message d'erreur indiquant que AWS Clean Rooms la politique pour le rôle de service est introuvable.

8. Si vous souhaitez activer les balises pour la ressource d'association de tables configurée, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

9. Choisissez Associer une table.

Étapes suivantes

Maintenant que vous avez associé votre table de données configurée à la collaboration, vous êtes prêt à :

- Ajouter une règle d'analyse de collaboration au tableau configuré
- Modifiez la collaboration, si vous en êtes le créateur
- Interroger les tables de données (en tant que membre pouvant effectuer des requêtes)

Ajouter une règle d'analyse de collaboration à une table configurée

La règle d'analyse de collaboration vous permet de définir des contrôles spécifiques à cette collaboration. Ces contrôles fonctionnent conjointement avec la règle d'analyse de table configurée pour déterminer comment cette table peut être analysée dans le cadre de cette collaboration.

Vous ajoutez une règle d'analyse de collaboration à une table configurée après avoir créé une table configurée, ajouté une règle d'analyse et l'avoir associée à une collaboration. Vous devez ajouter une règle d'analyse de collaboration si la table est configurée pour prendre en charge l'analyse directe ou pour permettre une analyse supplémentaire.

- Analyse directe : la table peut être utilisée dans des requêtes qui l'analysent directement. Par exemple, dans une requête qui produit une analyse de mesure agrégée ou une liste d'identifiants à activer.
- Analyse supplémentaire — La table peut également être utilisée comme entrée dans des analyses supplémentaires, en plus des requêtes qui l'analysent directement. Par exemple, la table peut être utilisée dans une requête qui est le point de départ d'un modèle de machine learning similaire.

Pour ajouter la règle d'analyse de collaboration à un tableau

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration.

4. Dans l'onglet Tables, sous Tables associées par vous, consultez la table configurée que vous avez associée à la collaboration.

   Si le statut d'analyse directe ou le statut d'analyse supplémentaire a le statut Prêt, la table est prête à être interrogée.
5. Si le statut d'analyse directe ou le statut d'analyse supplémentaire a le statut Non prêt, sélectionnez le statut, puis choisissez Configurer dans la boîte de dialogue.
6. Sur la page Configurer la règle d'analyse de collaboration, développez Afficher la règle d'analyse de table configurée pour afficher les détails.
7. Pour les analyses supplémentaires autorisées, choisissez l'option en fonction de votre objectif.

Votre objectif	Option recommandée
Autorisez toute analyse supplémentaire sur la table.	Any
N'autorisez que des analyses supplémentaires sur la table par un membre spécifique.	N'importe lequel par des membres spécifiques
N'autorisez que des analyses spécifiques sur le tableau.	Liste personnalisée

8. Pour la livraison des résultats, spécifiez qui peut recevoir les résultats de la part des membres autorisés à recevoir des résultats pour la liste déroulante des résultats de requête.
9. Choisissez Configurer la règle d'analyse.

Configuration d'une politique de confidentialité différentielle (facultatif)

Cette procédure décrit le processus de configuration de la politique de confidentialité différentielle dans une collaboration à l'aide de l'option Flux guidé de la AWS Clean Rooms console. Il s'agit d'une étape unique pour toutes les tables dotées d'une protection de confidentialité différentielle.

Pour configurer les paramètres de confidentialité différentiels (flux guidé)

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Tables de la page de collaboration, choisissez Configurer la politique de confidentialité différentielle.
5. Sur la page Configurer une politique de confidentialité différentielle, choisissez des valeurs pour les propriétés suivantes :

   - Budget de confidentialité
   - Actualiser le budget de confidentialité tous les mois
   - Bruit ajouté par requête

   Vous pouvez utiliser les valeurs par défaut ou saisir des valeurs personnalisées adaptées à votre cas d'utilisation spécifique. Après avoir choisi des valeurs pour le budget de confidentialité et le bruit ajouté par requête, vous pouvez prévisualiser l'utilitaire obtenu en termes de nombre d'agrégations possibles pour toutes les requêtes portant sur vos données.
6. Choisissez Configurer.

Vous verrez un message de confirmation indiquant que vous avez correctement configuré la politique de confidentialité différentielle pour la collaboration.

Maintenant que vous avez configuré la confidentialité différentielle, vous êtes prêt à :

- Interroger les tables de données (en tant que membre pouvant effectuer des requêtes)
- Gérez la collaboration (si vous êtes le créateur de la collaboration)

Afficher les journaux d'utilisation différentiels de confidentialité

En tant que membre d'une collaboration qui protège les données avec une confidentialité différentielle, une fois que vous avez créé une collaboration avec une confidentialité différentielle, vous pouvez surveiller l'utilisation du budget de confidentialité.

Pour voir combien d'agrégations ont été effectuées et quelle part du budget de confidentialité a été utilisée

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Choisissez l'onglet Tables.
5. Choisissez Afficher les journaux d'utilisation (texte bleu).
6. Consultez les détails d'utilisation, y compris le budget de confidentialité et le niveau d'utilité fourni.

Modifier une politique de confidentialité différentielle

Après avoir configuré la politique de confidentialité différentielle, vous pouvez à tout moment la mettre à jour pour mieux refléter vos besoins en matière de confidentialité.

Pour modifier la politique de confidentialité différentielle

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Tables de la page de collaboration, sous Tables que vous avez associées, choisissez Modifier.
5. Sur la page Modifier la confidentialité différentielle, choisissez de nouvelles valeurs pour les propriétés suivantes :

   - Budget de confidentialité : déplacez le curseur pour augmenter ou diminuer le budget à tout moment au cours d'une collaboration. Vous ne pouvez pas réduire le budget une fois que le membre autorisé à interroger vos données a commencé à interroger vos données. Si le budget de confidentialité est augmenté, AWS Clean Rooms vous continuerez à utiliser le budget existant jusqu'à ce qu'il soit entièrement utilisé avant d'utiliser le budget de confidentialité nouvellement ajouté.
   - Bruit ajouté par requête : déplacez le curseur pour augmenter ou diminuer le bruit ajouté par requête à tout moment au cours d'une collaboration.

> **Note**
>
> Vous pouvez choisir des exemples interactifs pour découvrir comment les différentes valeurs du budget de confidentialité et du bruit ajouté par requête affectent le nombre de fonctions d'agrégation que vous pouvez exécuter.

Vous ne pouvez pas modifier la valeur de l'actualisation du budget de confidentialité. Pour modifier votre sélection, vous devez supprimer la politique de confidentialité différentielle et en créer une nouvelle.

6. Sélectionnez Enregistrer les modifications.

Un message de confirmation s'affiche indiquant que vous avez correctement modifié la politique de confidentialité différentielle.

Supprimer une politique de confidentialité différentielle

Vous pouvez supprimer la politique de confidentialité différentielle dans l'onglet Tables d'une collaboration.

Pour supprimer la politique de confidentialité différentielle

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Tables de la page de collaboration, à côté de Politique de confidentialité différentielle, sélectionnez Supprimer.
5. Si vous êtes certain de vouloir supprimer la politique de confidentialité différentielle, choisissez Supprimer.

Après avoir supprimé une politique de confidentialité différentielle, vous ne pouvez pas accéder aux journaux d'utilisation du budget de confidentialité contenus dans cette politique. Les tables dans lesquelles la confidentialité différentielle est activée ne peuvent pas être consultées si la politique de confidentialité différentielle est supprimée.

Affichage des paramètres de confidentialité différentiels calculés

Pour les utilisateurs expérimentés en matière de confidentialité différentielle, vous pouvez consulter les paramètres de confidentialité différentielle calculés dans l'onglet Requêtes d'une collaboration.

Pour afficher les paramètres de confidentialité différentiels calculés

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Requêtes, dans la section Résultats, sélectionnez Afficher les paramètres de confidentialité différentiels calculés.

Dans le tableau des paramètres de confidentialité différentiels calculés, vous pouvez voir les valeurs de sensibilité des fonctions d'agrégation, définies comme la valeur maximale selon laquelle le résultat d'une fonction peut changer si les enregistrements d'un seul utilisateur sont ajoutés, supprimés ou modifiés. La liste inclut les paramètres de confidentialité différentiels suivants :

- La limite de contribution utilisateur (UCL) est le nombre maximum de lignes ajoutées par un utilisateur dans une SQL requête. Par exemple, si vous souhaitez compter le nombre total d'impressions correspondantes dans une campagne spécifique où chaque utilisateur peut avoir plusieurs impressions, la confidentialité AWS Clean Rooms différentielle doit limiter le nombre d'impressions d'un seul utilisateur afin de garantir l'exactitude du calcul de la confidentialité différentielle. En d'autres termes, si un utilisateur a plus d'impressions que la limite, il prend AWS Clean Rooms automatiquement un échantillon aléatoire uniforme des impressions de cet utilisateur conformément à la UCL valeur calculée et exclut les impressions restantes de cet utilisateur lors de l'exécution de la requête. La UCL valeur est égale à 1 si vous comptez le nombre d'utilisateurs uniques. Cela est dû au fait que l'ajout, la suppression ou la modification d'un seul utilisateur peut modifier le nombre d'utilisateurs distincts d'au plus 1.
- La valeur minimale est la limite inférieure d'une expression utilisée dans une fonction d'agrégation telle que`sum()`. Par exemple, si l'expression est une colonne connue sous le nom de`purchase_value`, la valeur minimale est la limite inférieure de la colonne.
- La valeur maximale est la limite supérieure d'une expression utilisée dans une fonction d'agrégation telle que`sum()`. Par exemple, si l'expression est une colonne connue sous le nom de`purchase_value`, la valeur maximale est la limite supérieure de la colonne.

Dans le tableau des paramètres de confidentialité différentiels calculés, vous pouvez utiliser ces paramètres pour mieux comprendre la quantité totale de bruit dans les résultats des requêtes. Par exemple, lorsque le bruit configuré ajouté par requête est de 30 utilisateurs et qu'une `COUNT DISTINCT (user_id)` requête est exécutée, la confidentialité AWS Clean Rooms différentielle ajoute un bruit aléatoire compris entre -30 et 30 avec une probabilité élevée car la sensibilité de `COUNT DISTINCT` est de 1. Dans le cas d'une `COUNT` requête avec la même configuration, la confidentialité AWS Clean Rooms différentielle ajoute du bruit statistique qui est ajusté en fonction de la limite de contribution de l'utilisateur, car un seul utilisateur peut ajouter plusieurs lignes au résultat de la requête. Dans le cas d'une `SUM` requête `SUM (purchase_value)` où toutes les valeurs des colonnes sont positives, le bruit total est redimensionné en fonction de la limite de contribution de l'utilisateur multipliée par la valeur maximale. AWS Clean Rooms La confidentialité différentielle calcule automatiquement les paramètres de sensibilité pour effectuer l'ajout de bruit au moment de l'exécution de la requête et épuise le budget de confidentialité. L'épuisement du budget de confidentialité est nécessaire car les paramètres de sensibilité dépendent des données.

Gestion des tables configurées dans AWS Clean Rooms

Les rubriques suivantes décrivent comment gérer les tables configurées à AWS Clean Rooms l'aide de la AWS Clean Rooms console.

Pour plus d'informations sur la gestion des tables configurées à l'aide du AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Rubriques

Afficher les tables et les règles d'analyse

Pour afficher les tables associées à la collaboration et aux règles d'analyse

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Choisissez l'onglet Tables.
5. Sélectionnez l'une des méthodes suivantes :
    a. Pour afficher les tables associées à la collaboration, pour Tables associées par vous, choisissez une table (texte bleu).
    b. Pour afficher les autres tables associées à la collaboration, pour Tables associées par des collaborateurs, choisissez une table (texte bleu).
6. Consultez les détails de la table et les règles d'analyse sur la page des détails de la table.

Modification des détails d'une table configurée

En tant que membre de la collaboration, vous pouvez modifier les détails de la table configurée.

Pour modifier les détails d'une table configurée

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Tables configurées.
3. Choisissez la table configurée que vous avez créée.
4. Sur la page détaillée de la table configurée, faites défiler la page vers le bas jusqu'à Détails de la table configurée.
5. Choisissez Modifier.
6. Mettez à jour le nom ou la description de la table configurée.
7. Sélectionnez Enregistrer les modifications.

Modification des balises de tableau configurées

En tant que membre de la collaboration, après avoir créé une table configurée, vous pouvez gérer les balises de la ressource de table configurée dans l'onglet Tables configurées.

Pour modifier les balises de table configurées

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Tables configurées.
3. Choisissez la table configurée que vous avez créée.
4. Sur la page détaillée du tableau configuré, faites défiler la page vers le bas jusqu'à la section Tags.
5. Choisissez Gérer les balises.
6. Sur la page de gestion des étiquettes, vous pouvez effectuer les opérations suivantes :
   - Pour supprimer une identification, choisissez Supprimer.
   - Pour ajouter une balise, sélectionnez Add new tag (Ajouter une nouvelle balise).
   - Choisissez Enregistrer pour enregistrer les modifications.

Modification d'une règle d'analyse de table configurée

Pour modifier la règle d'analyse de table configurée

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Tables configurées.
3. Choisissez la table configurée que vous avez créée.
4. Sur la page détaillée de la table configurée, faites défiler la page vers le bas jusqu'à la section Règle d'analyse d'agrégation, Règle d'analyse de liste ou Règle d'analyse personnalisée. (Votre choix dépend du type de règle d'analyse que vous avez choisi pour la table configurée.)
5. Choisissez Modifier.
6. Sur la page Modifier la règle d'analyse, vous pouvez :
   - Modifiez la définition de la règle d'analyse en :

- Modification de l'JSONéditeur.
- Choisissez Importer depuis un fichier pour télécharger une nouvelle définition de règle d'analyse.

- Prévisualisez ce que les membres verront dans une collaboration en sélectionnant l'une des options suivantes :
  - Vue du tableau
  - JSON
  - Exemple de requête

7. Choisissez Enregistrer les Modifications pour enregistrer vos Modifications.

Suppression d'une règle d'analyse de table configurée

> **Warning**
>
> Cette action est irréversible et a un impact sur toutes les ressources associées.

Pour supprimer la règle d'analyse de table configurée

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Tables configurées.
3. Choisissez la table configurée que vous avez créée.
4. Sur la page détaillée de la table configurée, faites défiler la page vers le bas jusqu'à la section Règle d'analyse d'agrégation, Règle d'analyse de liste ou Règle d'analyse personnalisée. (Votre choix dépend du type de règle d'analyse que vous avez choisi pour la table configurée.)
5. Sélectionnez Delete (Supprimer).
6. Si vous êtes certain de vouloir supprimer la règle d'analyse, choisissez Supprimer.

Colonnes interdites dans le tableau configuré

La configuration des colonnes de sortie interdites est un contrôle de la règle d'analyse AWS Clean Rooms personnalisée qui vous permet de définir la liste des colonnes (le cas échéant) dont vous n'autorisez pas la projection dans le résultat de la requête. Les colonnes référencées dans cette

liste sont considérées comme des « colonnes de sortie interdites ». Cela signifie que toute référence à une telle colonne par transformation, aliasing ou autre moyen peut ne pas être présente dans la version finale SELECT (projection) de la requête.

Bien que cette fonctionnalité empêche les colonnes d'être directement projetées dans la sortie, elle n'empêche pas totalement les valeurs sous-jacentes d'être déduites indirectement par d'autres mécanismes. Ces colonnes peuvent toujours être utilisées dans une clause de projection (telle que dans une sous-requête ou une expression de table commune (CTE)), tant qu'elles ne sont pas référencées dans la toute dernière projection.

La configuration des colonnes de sortie interdites vous donne la flexibilité d'appliquer et de codifier le contrôle sur votre table en combinaison avec des révisions au niveau des modèles d'analyse basées sur des cas d'utilisation et des exigences de confidentialité correspondantes.

Pour plus d'informations sur la façon de définir cette configuration, consultezAjouter une règle d'analyse personnalisée à un tableau (flux guidé).

Exemples

Les exemples suivants montrent comment le contrôle des colonnes de sortie interdites est appliqué.

- Le membre A est en collaboration avec le membre B.
- Le membre B est le membre qui peut exécuter des requêtes.
- Le membre A définit les utilisateurs d'une table avec les colonnes âge, sexe, e-mail et nom. L'âge et le nom des colonnes sont des colonnes de sortie interdites.
- Le membre B définit un animal de table avec un ensemble similaire de colonnes age, sexe et nom_propriétaire. Cependant, ils ne définissent aucune contrainte sur les colonnes de sortie, ce qui signifie que toutes les colonnes de la table peuvent être projetées librement dans la requête.

Si le membre B exécute la requête suivante, elle est bloquée car les colonnes de sortie interdites ne peuvent pas être projetées directement :

```
SELECT
  age
FROM
  users
```

Si le membre B exécute la requête suivante, elle est bloquée car les colonnes de sortie interdites ne peuvent pas être implicitement projetées via project star :

```
SELECT
  *
FROM
  users
```

Si le membre B exécute la requête suivante, elle est bloquée car les transformations des colonnes de sortie interdites ne peuvent pas être projetées :

```
SELECT
  COUNT(age)
FROM
  users
```

Si le membre B exécute la requête suivante, elle est bloquée car les colonnes de sortie interdites ne peuvent pas être référencées dans la projection finale à l'aide d'un alias :

```
SELECT
  count_age
FROM
  (SELECT COUNT(age) AS count_age FROM users)
```

Si le membre B exécute la requête suivante, elle est bloquée car les colonnes restreintes transformées sont projetées dans la sortie :

```
SELECT
  CONCAT(name, email)
FROM
  users
```

Si le membre B exécute la requête suivante, elle est bloquée car les colonnes de sortie interdites définies dans ne CTE peuvent pas être référencées dans la projection finale :

```
WITH cte AS (
```

```
  SELECT
    age AS age_alias
  FROM
    users
)
SELECT age_alias FROM cte
```

Si le membre B exécute la requête suivante, elle est bloquée car les colonnes de sortie interdites ne peuvent pas être utilisées comme clés de tri ou de partition dans la projection finale :

```
SELECT
  LISTAGG(gender) WITHIN GROUP (ORDER BY age) OVER (PARTITION BY age)
FROM
  users
```

Si le membre B exécute la requête suivante, elle aboutit car les colonnes faisant partie des colonnes de sortie interdites peuvent toujours être utilisées dans d'autres constructions de la requête, par exemple dans les clauses de jointure ou de filtrage.

```
SELECT
  u.name,
  p.gender,
  p.age
FROM
  users AS u
JOIN
  pets AS p
ON
  u.name = p.owner_name
```

Dans le même scénario, le membre B peut également utiliser la colonne de nom dans les utilisateurs comme filtre ou clé de tri :

```
SELECT
  u.email,
  u.gender
FROM
  users AS u
```

```
WHERE
  u.name = 'Mike'
ORDER BY
  u.name
```

En outre, les colonnes de sortie interdites aux utilisateurs peuvent être utilisées dans des projections intermédiaires telles que des sous-requêtes etCTEs, par exemple :

```
WTIH cte AS (
 SELECT
   u.gender,
   u.id,
   u.first_name
 FROM
   users AS u
)
SELECT
  first_name
FROM
  (SELECT cte.gender, cte.id, cte.first_name FROM cte)
```

Modification des associations de tables configurées

En tant que membre de la collaboration, vous pouvez modifier les associations de tables configurées que vous avez créées.

Pour modifier les associations de tables configurées

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Choisissez l'onglet Tables.
5. Pour les tables que vous avez associées, choisissez une table.
6. Sur la page des détails de la table, faites défiler la page vers le bas pour afficher les détails de l'association de tables.

7. Choisissez Modifier.
8. Sur la page Modifier les associations de tables configurées, mettez à jour la description ou les informations d'accès au service.
9. Sélectionnez Enregistrer les modifications.

Dissociation des tables configurées

En tant que membre de la collaboration, vous pouvez dissocier une table configurée de la collaboration. Cette action empêche le membre autorisé à interroger la table.

Pour dissocier une table configurée

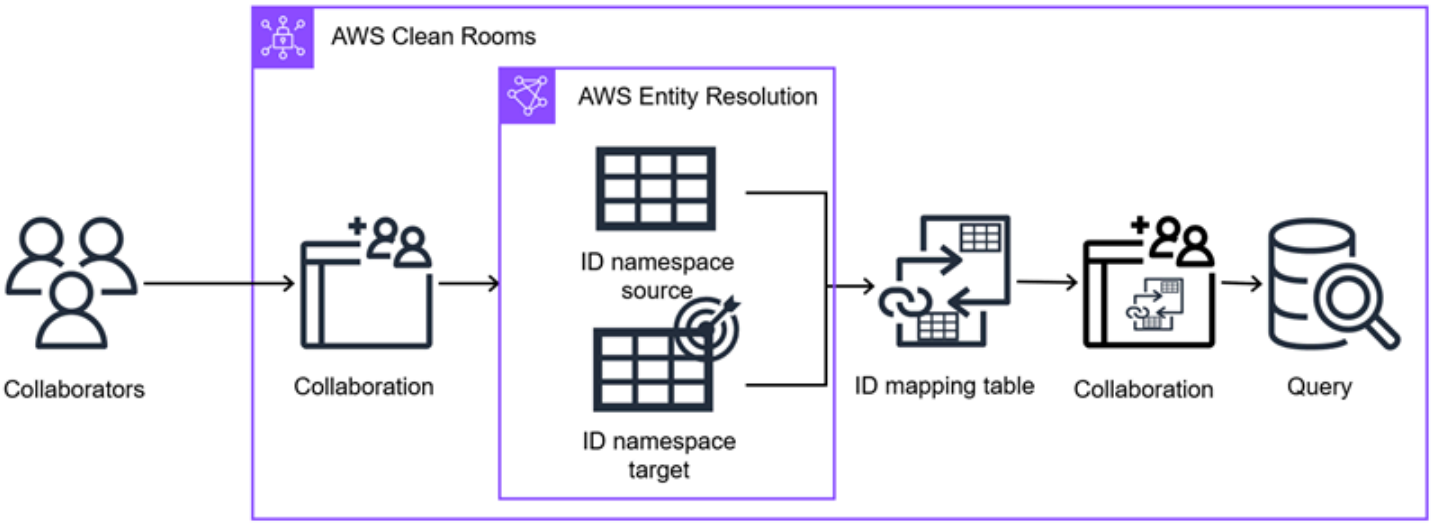
1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Choisissez l'onglet Tables.
5. Pour les tables que vous avez associées, sélectionnez le bouton d'option situé à côté de la table que vous souhaitez dissocier.
6. Choisissez Dissocier.
7. Dans la boîte de dialogue, confirmez la décision de dissocier la table configurée et empêchez le membre autorisé à interroger la table en choisissant Dissocier.

Travailler avec Résolution des entités AWS in AWS Clean Rooms

Grâce Résolution des entités AWS à in AWS Clean Rooms, vous pouvez traduire les données d'une source vers une cible, remplir une table de mappage d'identifiants avec les données traduites et interroger les données.

Tout d'abord, vous créez une collaboration AWS Clean Rooms et vous y ajoutez celle que Comptes AWS vous souhaitez inviter, ou vous rejoignez une collaboration à laquelle vous êtes invité en créant un abonnement. Ensuite, vous effectuez le mappage des identifiants sur deux tables de données. Pour ce faire, associez une source d'espace de noms d'ID existante ou créez-en une nouvelle dans Résolution des entités AWS. L'autre membre de la collaboration associe une cible d'espace de noms ID existante ou crée une nouvelle cible d'espace de noms d'ID. Ensuite, vous créez et remplissez une table de mappage d'ID à partir des deux espaces de noms d'ID associés. Enfin, le membre qui peut effectuer une requête exécute une requête dans les deux tables de données en se joignant à la table de mappage d'identifiants.

Le schéma suivant résume la manière d'utiliser Résolution des entités AWS in AWS Clean Rooms.



> **Note**
>
> Le fournisseur de services de transcodage actuellement pris en charge est LiveRamp, qui est disponible dans les Régions AWS pays suivants : USA Est (Virginie du Nord), USA Est (Ohio) et USA Ouest (Oregon).

Rubriques

Utilisation des espaces de noms d'ID dans AWS Clean Rooms

Un espace de noms d'identification est une enveloppe entourant votre table d'identité qui vous permet de fournir des métadonnées expliquant votre ensemble de données et expliquant comment l'utiliser dans un flux de travail de mappage d'identifiants. 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.

Il existe deux types d'espaces de noms d'ID : source et cible. La source contient des configurations pour les données source qui seront traitées dans un flux de travail de mappage d'identifiants. La cible 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).

Vous pouvez soit créer un nouvel espace de noms d'ID, soit associer un espace existant. Pour plus d'informations sur la création d'un espace de noms d'ID dans Résolution des entités AWS, consultez la section Création d'un espace de noms d'ID dans le Guide de l'Résolution des entités AWS utilisateur.

Rubriques

Création et association d'un nouvel espace de noms d'ID

Chaque membre de la collaboration doit créer et associer un espace de noms ID Source ou un espace de noms ID Target avant de créer une table de mappage d'ID pour interroger les données d'identité.

Si vous avez déjà créé un espace de noms d'ID dans Résolution des entités AWS, passez directement àAssocier un espace de noms d'ID existant.

Pour créer et associer un nouvel espace de noms d'ID

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Résolution de l'entité, choisissez l'espace de noms Associate ID.
5. Sur la page espace de noms Associate ID, pour les données de résolution d'entité, choisissez Create ID namespace.

   La Résolution des entités AWS console apparaît dans un nouvel onglet.
6. Suivez les instructions de la page Create ID namespace de la Résolution des entités AWS console.

   a. Pour plus de détails, entrez le nom de l'espace de noms d'ID, la description, puis sélectionnez le type d'espace de noms d'ID (source ou cible).

   b. Pour la méthode de l'espace de noms ID, choisissez soit la méthode basée sur des règles pour le rapprochement basé sur des règles, soit les services du fournisseur pour le transcodage tiers.

   c. Spécifiez le type de saisie des données, en fonction de la méthode d'espace de noms ID que vous avez choisie.

   d. Choisissez Create ID namespace.
7. Retournez à la AWS Clean Rooms console.
8. Sur la page Espace de noms d'ID associé, pour les données de résolution d'entité, choisissez la source ou la cible de l'espace de noms d'Résolution des entités AWS ID que vous souhaitez associer à la collaboration dans la liste déroulante.
9. Pour obtenir des informations sur l'association, procédez comme suit.

   a. Entrez un nom pour l'espace de noms ID associé.

      Vous pouvez utiliser le nom par défaut ou renommer cet espace de noms d'ID.

   b. (Facultatif) Entrez une description de l'espace de noms ID.

La description facilite la rédaction de requêtes.

10. Spécifiez les autorisations AWS Clean Rooms d'accès en sélectionnant une option, puis en prenant les mesures recommandées.

Option	Action recommandée
AWS Clean Rooms Autoriser l'ajout et la gestion de la politique d'autorisation	AWS Clean Rooms crée un rôle de service avec la politique requise pour cette associati on.
Ajouter et gérer les autorisations manuellem ent	Effectuez l'une des actions suivantes : • Passez en revue la politique des ressource s et ajoutez-y les autorisations nécessair es. • Utilisez une politique existante en choisissant Ajouter une déclaration de politique. Vous devez disposer des autorisations nécessaires pour modifier les rôles et créer des politiques. **Note** Si vous ne pouvez pas modifier la politique de rôle, vous recevez un message d'erreur indiquant que vous n'avez pas AWS Clean Rooms trouvé la politique pour le rôle de service.

11. (Facultatif) Pour les configurations avancées des tables de mappage d'identifiants, modifiez les protections par défaut pour la colonne provenant de l'espace de noms d'identifiants.

    La table de mappage des identifiants est configurée par défaut pour autoriser uniquement un à la fois `INNER JOIN` sur la `sourceID` colonne et sur la `targetID` colonne. Vous pouvez modifier

cette configuration afin que la colonne provenant de cet espace de noms d'ID (soit `targetID`) `sourceID` soit autorisée n'importe où dans la requête.

Votre objectif	Option recommandée
Catégoriser la colonne en tant que « colonne de jointure » et ne l'autoriser que dans une clause `INNER JOIN`	Oui
Catégorisez la colonne en tant que « colonne de dimension » et autorisez-la n'importe où dans la requête, y compris dans une `JOIN` clause `WHERE` et dans les `GROUP BY` instructions de la requête. `SELECT`	Non, autoriser n'importe où dans la requête

12. (Facultatif) Si vous souhaitez activer les balises pour la ressource ID namepspace, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
13. Choisissez Associer.
14. Dans l'onglet Résolution des entités, sous le tableau des espaces de noms ID associés, consultez l'espace de noms ID associé et vérifiez que le type d'espace de noms ID est correct (source ou cible).

Une fois que tous les membres de la collaboration ont associé leurs espaces de noms d'identification, vous pouvez créer une table de mappage d'identifiants et interroger les données.

Associer un espace de noms d'ID existant

Dans cette procédure, chaque membre associe soit sa source d'espace de noms d'ID existante, soit sa cible d'espace de noms d'ID dans la collaboration.

Pour associer un espace de noms d'ID existant

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Résolution de l'entité, choisissez l'espace de noms Associate ID.

5. Sur la page Espace de noms d'ID associé, pour les données de résolution d'entité, choisissez la source ou la cible de l'espace de noms d'Résolution des entités AWS ID que vous souhaitez associer à la collaboration dans la liste déroulante.
6. Pour obtenir des informations sur l'association, procédez comme suit.

   a. Entrez un nom pour l'espace de noms ID associé.

      Vous pouvez utiliser le nom par défaut ou renommer cet espace de noms d'ID.

   b. (Facultatif) Entrez une description de l'espace de noms ID.

      La description facilite la rédaction de requêtes.
7. Spécifiez les autorisations AWS Clean Rooms d'accès en sélectionnant une option, puis en prenant les mesures recommandées.

Option	Action recommandée
AWS Clean Rooms Autoriser l'ajout et la gestion de la politique d'autorisation	AWS Clean Rooms crée un rôle de service avec la politique requise pour cette associati on.
Ajouter et gérer les autorisations manuellem ent	Effectuez l'une des actions suivantes : • Passez en revue la politique des ressource s et ajoutez-y les autorisations nécessair es. • Utilisez une politique existante en choisissant Ajouter une déclaration de politique. Vous devez disposer des autorisations nécessaires pour modifier les rôles et créer des politiques. **Note** Si vous ne pouvez pas modifier la politique de rôle, vous recevez un

Option	Action recommandée
	message d'erreur indiquant que vous n'avez pas AWS Clean Rooms trouvé la politique pour le rôle de service.

8. (Facultatif) Pour les configurations avancées des tables de mappage d'identifiants, modifiez les protections par défaut pour la colonne provenant de l'espace de noms d'identifiants.

   La table de mappage des identifiants est configurée par défaut pour autoriser uniquement un à la fois `INNER JOIN` sur la `sourceID` colonne et sur la `targetID` colonne. Vous pouvez modifier cette configuration afin que la colonne provenant de cet espace de noms d'ID (soit`targetID`) `sourceID` soit autorisée n'importe où dans la requête.

Votre objectif	Option recommandée
Catégorisez la colonne en tant que « colonne de jointure » et autorisez-la uniquement dans une `INNER JOIN` clause.	Oui
Catégorisez la colonne en tant que « colonne de dimension » et autorisez-la n'importe où dans la requête, y compris dans une `JOIN` clause`SELECT`,`WHERE`, et des `GROUP BY` instructions de la requête.	Non, autoriser n'importe où dans la requête

9. (Facultatif) Si vous souhaitez activer les balises pour la ressource ID namepspace, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
10. Choisissez Associer.
11. Dans l'onglet Résolution des entités, sous le tableau des espaces de noms ID associés, consultez l'espace de noms ID associé et vérifiez que le type d'espace de noms ID est correct (source ou cible).

Une fois que tous les membres de la collaboration ont associé leurs espaces de noms d'identification, vous pouvez créer une table de mappage d'identifiants et interroger les données.

Gestion des associations d'espaces de noms d'ID dans AWS Clean Rooms

Les rubriques suivantes décrivent comment gérer les associations d'espaces de noms d'ID à AWS Clean Rooms l'aide de la AWS Clean Rooms console.

Pour plus d'informations sur la façon de gérer les associations d'espaces de noms d'ID à l'aide du AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Rubriques

Modification des associations d'espaces de noms d'ID

En tant que membre de la collaboration, vous pouvez modifier les associations d'espaces de noms d'ID que vous avez créées.

Pour modifier une association d'espaces de noms d'ID

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Choisissez l'onglet Résolution de l'entité.
5. Pour les espaces de noms d'ID associés, choisissez un espace de noms d'ID.
6. Sur la page des détails de l'espace de nommage ID, faites défiler la page vers le bas pour afficher les détails de l'association de l'espace de nommage ID.
7. Choisissez Modifier.
8. Sur la page Modifier les associations d'espaces de noms ID, modifiez l'un des éléments suivants :

    a. Pour les détails de l'association, mettez à jour le nom ou la description.

    b. (Facultatif) Pour les configurations avancées des tables de mappage d'identifiants, modifiez les protections par défaut pour la colonne provenant de l'espace de noms d'identifiants.

La table de mappage des identifiants est configurée par défaut pour autoriser uniquement un à la fois `INNER JOIN` sur la `sourceID` colonne et sur la `targetID` colonne. Vous pouvez modifier cette configuration afin que la colonne provenant de cet espace de noms d'ID (soit`targetID`) `sourceID` soit autorisée n'importe où dans la requête.

Votre objectif	Option recommandée
Catégoriser la colonne en tant que « colonne de jointure » et ne l'autoriser que dans une clause `INNER JOIN`	Oui
Catégorisez la colonne en tant que « colonne de dimension » et autorisez-la n'importe où dans la requête, y compris dans une `JOIN` clause `WHERE` et dans les `GROUP BY` instructions de la requête. `SELECT`	Non, autoriser n'importe où dans la requête

9. Sélectionnez Enregistrer les modifications.

Dissociation des associations d'espaces de noms d'ID

En tant que membre de la collaboration, vous pouvez dissocier un espace de noms ID de la collaboration. Cette action empêche le membre autorisé à interroger la table.

> **Warning**
>
> Dissocier une association d'espaces de noms d'ID d'une collaboration supprime toutes les données des tables de mappage d'identifiants dérivées, les rendant ainsi ininterrogeables. Par exemple, si votre association d'espace de noms d'ID a été utilisée SOURCE dans trois tables de mappage d'ID différentes, toutes les données de ces tables de mappage d'ID seront supprimées lorsque vous dissocierez votre association d'espace de noms d'ID.

Pour dissocier une association d'espaces de noms ID

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Choisissez l'onglet Résolution de l'entité.
5. Pour les espaces de noms d'ID associés, sélectionnez le bouton d'option à côté de l'espace de noms d'ID que vous souhaitez dissocier.
6. Choisissez Dissocier.
7. Dans la boîte de dialogue, confirmez votre décision de déconnecter l'espace de noms ID en choisissant Dissocier. Cette action empêche tout membre autorisé à effectuer une requête d'accéder à la table de mappage des identifiants.

   Si un membre de la collaboration supprime l'un des espaces de noms d'identification, vous ne pouvez pas remplir à nouveau la table de mappage des identifiants si la source a quitté la collaboration.

   Même si la table de mappage des identifiants a déjà été remplie, la dissociation de l'espace de noms des identifiants signifie que vous ne pouvez plus exécuter de requêtes sur cette table.

Utilisation des tables de mappage d'identifiants dans AWS Clean Rooms

Une table de mappage d'identifiants est une ressource AWS Clean Rooms qui permet le mappage d'identité multipartite dans le cadre d'une collaboration.

Avant de créer une table de mappage d'ID, vous devez d'abord configurer les données source et cible en tant qu'espaces de noms d'ID.

Après avoir créé une table de mappage d'ID, vous utilisez un flux de travail de mappage d'ID pour traduire l'espace de noms d'ID source en espace de noms d'ID cible. Pour ce faire, vous pouvez utiliser une méthode basée sur des règles ou une méthode de transcodage des services du fournisseur.

Un flux de travail de mappage d'identification 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 flux de travail de mappage d'identification spécifiée. Ce flux de travail remplit une table de mappage d'identifiants.

Il existe deux méthodes de mappage des identifiants : le mappage des identifiants basé sur des règles ou le mappage des identifiants des fournisseurs de services :

- 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 fournisseur de services de transcodage actuellement pris en charge est LiveRamp. Tout membre de la collaboration abonné à LiveRamp Through AWS Data Exchange peut créer la table de mappage des identifiants. Si vous avez déjà souscrit un abonnement LiveRamp, mais pas par le biais de AWS Data Exchange celui-ci, contactez-nous LiveRamp pour obtenir une offre privée. Pour plus d'informations, consultez la section Abonnement à un service fournisseur AWS Data Exchange dans le guide de Résolution des entités AWS l'utilisateur.

Rubriques

Création et remplissage d'une nouvelle table de mappage d'identifiants

Avant de créer une table de mappage d'ID, vous devez d'abord disposer d'une source et d'une cible d'espace de noms d'ID associées. La source et la cible de l'espace de noms d'ID que vous associez à la collaboration doivent être configurées pour le type de mappage d'ID que vous souhaitez effectuer (mappage d'ID basé sur des règles ou mappage d'ID de services fournisseurs).

Après avoir créé une table de mappage d'identifiants, deux options s'offrent à vous. Vous pouvez le renseigner immédiatement, ce qui exécute le flux de travail de mappage des identifiants. Vous pouvez également attendre de remplir le tableau ultérieurement.

Une fois que la table de mappage des identifiants est correctement remplie, vous pouvez exécuter une requête de jointure multitable sur la table de mappage des identifiants pour les `sourceId` joindre aux données `targetId` et les analyser.

Rubriques

- Création d'une table de mappage d'identifiants (basée sur des règles)
- Création d'une table de mappage des identifiants (services du fournisseur)

Création d'une table de mappage d'identifiants (basée sur des règles)

Cette rubrique décrit le processus de création d'une table de mappage d'identifiants qui utilise des règles de correspondance pour traduire les données de première partie d'une source vers une cible.

Pour créer et remplir une nouvelle table de mappage d'identifiants à l'aide de la méthode basée sur des règles

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Résolution de l'entité, choisissez Créer une table de mappage d'identifiants.
5. Sur la page du tableau Créer un mappage d'identifiants, sous Paramètres de mappage d'identifiants, effectuez l'une des actions suivantes en fonction de votre objectif.

Votre objectif	Action recommandée
Création d'un nouveau flux de travail de mappage des identifiants	1. Laissez la case Créer un nouveau flux de travail de mappage d'identifiants cochée. 2. Passez à l'étape 6.
Réutiliser un flux de travail de mappage d'identifiants existant	1. Décochez la case Créer un nouveau flux de travail de mappage d'identifiants. 2. Sélectionnez un flux de travail de mappage des identifiants basé sur des règles dans la liste déroulante. 3. Passez à l'étape 9.

6. Sous Données d'identité, effectuez l'une des actions suivantes en fonction de votre scénario

Votre scénario	Action recommandée
Il n'existe qu'une seule source d'espace de noms d'ID et une seule cible d'espace de noms d'ID dans la collaboration	Affichez les associations d'espaces de noms source et cible ID.
Il existe plusieurs associations d'espaces de noms d'ID dans la collaboration.	Sélectionnez les associations d'espace de noms d'ID source et cible que vous souhaitez utiliser dans les listes déroulantes.

7. Sous Méthode, consultez la méthode de flux de travail de mappage d'identifiants sélectionnée : basée sur des règles
8. Pour les paramètres de règle, spécifiez les contrôles de règle, le type de comparaison et les configurations de correspondance des enregistrements.

   a. Pour les contrôles de règles, choisissez si vous souhaitez que les règles correspondantes soient fournies par l'espace de noms Target ou Source ID.

      Vous pouvez consulter les règles en activant Afficher les règles.

      Les contrôles de règles doivent être compatibles entre l'espace de noms d'ID source et cible à utiliser dans un flux de travail de mappage d'ID. 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. 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.

   c. Spécifiez le type de correspondance des enregistrements en choisissant l'une des options suivantes.

Votre objectif	Option recommandée
Limitez le type de correspondance d'enregistrements afin de ne stocker qu'un seul enregistrement correspondant	Une source pour une cible

Votre objectif	Option recommandée
dans la source pour chaque enregistr ement correspondant dans la cible lorsque vous créez le flux de travail de mappage d'identifiants.	
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**
>
> Les limites spécifiées pour les espaces de noms d'ID source et cible doivent être compatibles.

9. Pour obtenir des informations détaillées sur le mappage des identifiants, effectuez les actions suivantes.

   a. Entrez le nom d'une table de mappage d'identifiants.

      Vous pouvez utiliser le nom par défaut ou renommer cette table de mappage d'identifiants.

   b. (Facultatif) Entrez une description de la table de mappage des identifiants.

      La description facilite la rédaction de requêtes.

10. Spécifiez les autorisations d'AWS Clean Rooms accès en choisissant une option et en prenant les mesures recommandées.

Option	Action recommandée
AWS Clean Rooms Autoriser l'ajout et la gestion de la politique d'autorisation	AWS Clean Rooms crée un rôle de service avec la politique requise pour cette associati on.

Option	Action recommandée
Ajouter et gérer les autorisations manuellement	Effectuez l'une des actions suivantes : • Passez en revue la politique des ressources et ajoutez-y les autorisations nécessaires. • Utilisez une politique existante en choisissant Ajouter une déclaration de politique. Vous devez disposer des autorisations nécessaires pour modifier les rôles et créer des politiques. **Note** Si vous ne pouvez pas modifier la politique de rôle, vous recevez un message d'erreur indiquant que vous n'avez pas AWS Clean Rooms trouvé la politique pour le rôle de service.

11. Spécifiez les autorisations d'Résolution des entités AWS accès en choisissant une option et en prenant les mesures recommandées :

    Cette section n'est visible que si vous créez une nouvelle table de mappage d'identifiants.

Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	AWS Clean Rooms 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>`

Option	Action recommandée
	Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. Si vos données d'entrée sont cryptées, vous pouvez choisir Ces données sont cryptées par une KMS clé, puis saisir 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. 2. Affichez le rôle de service en choisissant le lien Afficher dans un lien IAM externe. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. Par défaut, AWS Clean Rooms ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires. 3. (Facultatif) Cochez la case Ajouter une politique préconfigurée avec les autorisat ions nécessaires pour ce rôle pour associer les autorisations nécessaires au rôle. Vous devez disposer des autorisat ions nécessaires pour modifier les rôles et créer des politiques.

12. (Facultatif) Spécifiez les paramètres supplémentaires en sélectionnant l'une des options suivantes :

    a. Pour le tableau de mappage des identifiants, effectuez l'une des actions suivantes en fonction de votre objectif.

Votre objectif	Action recommandée
Activer les paramètres de chiffrement personnalisés pour la table de mappage des identifiants	Choisissez Personnaliser les paramètres de chiffrement, puis entrez la AWS KMS clé. **Note** Cette KMS clé doit accorder les autorisations requises pour être utilisée dans le cadre Résolution des entités AWS de `cleanrooms.amazonaws.com` l'utilisation d'une politique KMS clé. Pour plus de détails sur les autorisations requises pour utiliser des chiffrements avec un flux de travail de mappage d'identifiants, voir Créer un rôle de travail dans le flux de travail Résolution des entités AWS dans le guide de l'Résolution des entités AWS utilisateur.
Activer les balises pour la ressource de table de mappage d'identifiants	Choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

b. Pour le flux de travail de mappage des identifiants, effectuez l'une des actions suivantes en fonction de votre objectif.

   Cette section n'est visible que si vous créez une nouvelle table de mappage d'identifiants.

Votre objectif	Action recommandée
Modifier le nom et la description du flux de travail de mappage des identifiants	Désactivez la case à cocher Conserver le même nom et la même description de la table de mappage d'identifiants et entrez un nouveau nom et une nouvelle descripti on du flux de travail de mappage d'identif iants.
Activer les balises pour la ressource de flux de travail de mappage des identifiants	Choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

13. Choisissez l'une des options suivantes en fonction de votre objectif.

Votre objectif	Option recommandée
Créez une table de mappage d'ID vide, mais n'exécutez pas le flux de travail de mappage d'ID	Créer une table de mappage d'identifiants Vous pouvez remplir le tableau de mappage des identifiants ultérieurement en suivant le Remplissage d'une table de mappage d'identifiants existante processus.
Créez la table de mappage des identifiants et exécutez le flux de travail de mappage des identifiants	Création et remplissage d'une table de mappage d'identifiants Le processus de mappage des identifiants commence. Au cours de ce processus, la table de mappage des identifiants est remplie avec une traductionIDs. Le processus de mappage des identifiants peut prendre quelques heures. Une fois que la table de mappage des identifiants est correctement remplie, vous pouvez interroger la table de mappage des

Votre objectif	Option recommandée
	identifiants pour les `sourceId` joindre aux données `targetId` et les analyser.

Création d'une table de mappage des identifiants (services du fournisseur)

Cette rubrique décrit le processus de création d'une table de mappage d'identifiants utilisant un service fournisseur (LiveRamp). Les services du LiveRamp fournisseur traduisent un ensemble de sources R en un autre ampIDs en utilisant soit un R maintenu, soit un R dérivéampIDs.

Pour créer une nouvelle table de mappage d'identifiants à l'aide de la méthode des services du fournisseur

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Résolution de l'entité, choisissez Créer une table de mappage d'identifiants.
5. Sur la page du tableau Créer un mappage d'identifiants, sous Paramètres de mappage d'identifiants, effectuez l'une des actions suivantes en fonction de votre objectif.

Votre objectif	Action recommandée
Création d'un nouveau flux de travail de mappage des identifiants	1. Laissez la case Créer un nouveau flux de travail de mappage d'identifiants cochée. 2. Passez à l'étape 6.
Réutiliser un flux de travail de mappage d'identifiants existant	1. Décochez la case Créer un nouveau flux de travail de mappage d'identifiants. 2. Sélectionnez un flux de travail de mappage des identifiants basé sur des règles dans la liste déroulante. 3. Passez à l'étape 9.

6. Sous Données d'identité, effectuez l'une des actions suivantes en fonction de votre scénario.

Votre scénario	Action recommandée
Il n'existe qu'une seule source d'espace de noms d'ID et une seule cible d'espace de noms d'ID dans la collaboration	Afficher les associations d'espaces de noms source et cible
Il existe plusieurs associations d'espaces de noms d'ID dans la collaboration.	Sélectionnez les associations d'espace de noms d'ID source et cible que vous souhaitez utiliser dans les listes déroulantes.

7. Sous Méthode, vérifiez que la méthode de flux de travail de mappage d'identifiants sélectionnée est un LiveRamp transcodage.
8. Pour les LiveRamp configurations, entrez les informations suivantes fournies par : LiveRamp

   - LiveRamp Gestionnaire d'identifiants ARN
   - LiveRamp directeur secret ARN

   Vous pouvez également choisir Importer à partir d'un flux de travail existant :
9. Pour obtenir des informations détaillées sur le mappage des identifiants, procédez comme suit.

   a. Entrez le nom d'une table de mappage d'identifiants.

      Vous pouvez utiliser le nom par défaut ou renommer cette table de mappage d'identifiants.

   b. (Facultatif) Entrez une description de la table de mappage des identifiants.

      La description facilite la rédaction de requêtes.
10. Spécifiez les autorisations d'AWS Clean Rooms accès en sélectionnant l'une des options suivantes :

Option	Action recommandée
AWS Clean Rooms Autoriser l'ajout et la gestion de la politique d'autorisation	AWS Clean Rooms crée un rôle de service avec la politique requise pour cette associati on.

Option	Action recommandée
Ajouter et gérer les autorisations manuellement	Effectuez l'une des actions suivantes : • Passez en revue la politique des ressources et ajoutez-y les autorisations nécessaires. • Utilisez une politique existante en choisissant Ajouter une déclaration de politique. Vous devez disposer des autorisations nécessaires pour modifier les rôles et créer des politiques. **Note** Si vous ne pouvez pas modifier la politique de rôle, vous recevez un message d'erreur indiquant que vous n'avez pas AWS Clean Rooms trouvé la politique pour le rôle de service.

11. Spécifiez les autorisations d'Résolution des entités AWS accès en sélectionnant une option et en prenant les mesures recommandées.

    Cette section n'est visible que si vous créez une nouvelle table de mappage d'identifiants.

Option	Action recommandée
Création et utilisation d'un nouveau rôle de service	AWS Clean Rooms 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>`

Option	Action recommandée
	Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques. Si vos données d'entrée sont cryptées, vous pouvez choisir l'option Ces données sont cryptées par une KMS clé, puis saisir 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. 2. Affichez le rôle de service en choisissant Afficher dans IAM. S'il n'existe aucun rôle de service existant, l'option Utiliser un rôle de service existant n'est pas disponible. Par défaut, AWS Clean Rooms ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires. 3. (Facultatif) Cochez la case Ajouter une politique préconfigurée avec les autorisations nécessair es pour ce rôle pour ajouter attacher les autorisat ions nécessaires au rôle. Vous devez disposer des autorisations nécessaires pour modifier les rôles et créer des politiques.

12. (Facultatif) Spécifiez les paramètres supplémentaires en sélectionnant l'une des options suivantes :

a. Pour le tableau de mappage des identifiants, effectuez l'une des actions suivantes en fonction de votre objectif.

Votre objectif	Action recommandée
Activer les paramètres de chiffrement personnalisés pour la table de mappage des identifiants	Choisissez Personnaliser les paramètres de chiffrement, puis entrez la AWS KMS clé. **Note** Cette KMS clé doit accorder les autorisations requises pour être utilisée dans le cadre Résolution des entités AWS de `cleanrooms.amazonaws.com` l'utilisation d'une politique KMS clé. Pour plus de détails sur les autorisations requises pour utiliser des chiffrements avec un flux de travail de mappage d'identifiants, voir Créer un rôle de travail dans le flux de travail Résolution des entités AWS dans le guide de l'Résolution des entités AWS utilisateur.
Activer les balises pour la ressource de table de mappage d'identifiants	Choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

b. Pour le flux de travail de mappage des identifiants, effectuez l'une des actions suivantes en fonction de votre objectif.

Cette section n'est visible que si vous créez une nouvelle table de mappage d'identifiants.

Votre objectif	Action recommandée
Modifier le nom et la description du flux de travail de mappage des identifiants	Désactivez la case à cocher Conserver le même nom et la même description de la table de mappage d'identifiants et entrez un nouveau nom et une nouvelle descripti on du flux de travail de mappage d'identif iants.
Activer les balises pour la ressource de flux de travail de mappage des identifiants	Choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.

13. Choisissez l'une des actions suivantes en fonction de votre objectif.

Votre objectif	Action recommandée
Créez une table de mappage d'ID vide, mais n'exécutez pas le flux de travail de mappage d'ID	Choisissez Créer une table de mappage d'identifiants. Vous pouvez remplir le tableau de mappage des identifiants ultérieurement en suivant le Remplissage d'une table de mappage d'identifiants existante processus.
Créez la table de mappage des identifiants et exécutez le flux de travail de mappage des identifiants	Choisissez Créer et renseigner la table de mappage des identifiants. Le processus de mappage des identifiants commence. Au cours de ce processus, la table de mappage des identifiants est remplie de données transcodéesIDs. Le processus de mappage des identifiants peut prendre quelques heures. Une fois que la table de mappage des identifiants est correctement remplie, vous pouvez interroger la table de mappage des

Votre objectif	Action recommandée
	identifiants pour les `sourceId` joindre aux données `targetId` et les analyser.

Remplissage d'une table de mappage d'identifiants existante

Lorsque de nouvelles données sont ajoutées à un espace de noms d'ID, utilisez ce flux de travail.

Pour remplir une table de mappage d'identifiants existante

1. Connectez-vous à la AWS Clean Rooms console AWS Management Console et ouvrez-la avec votre Compte AWS (si ce n'est pas encore fait).
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Résolution des entités, sous la section Tables de mappage des identifiants, effectuez l'une des opérations suivantes :

   - Choisissez une table de mappage d'identifiants, puis choisissez Remplir.
   - Sélectionnez le bouton d'option à côté de la table de mappage d'identifiants, puis sur la page de détails de la table de mappage d'identifiants, choisissez Remplir.

Le processus de mappage des identifiants commence. Au cours de ce processus, la table de mappage des identifiants est remplie de données transcodéesIDs. Le processus de mappage des identifiants peut prendre quelques heures.

Une fois que la table de mappage d'identifiants est correctement remplie, vous pouvez interroger la table de mappage d'identifiants pour la `sourceId` joindre à`targetId`.

Gestion des tables de mappage d'identifiants dans AWS Clean Rooms

Les rubriques suivantes décrivent comment gérer les tables de mappage d'identifiants à AWS Clean Rooms l'aide de la AWS Clean Rooms console.

Pour plus d'informations sur la gestion des tables de mappage d'identifiants à l'aide du AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Rubriques

Modification d'une table de mappage d'identifiants

En tant que membre de la collaboration, vous pouvez modifier la table de mappage des identifiants que vous avez créée.

Pour modifier une table de mappage d'identifiants

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Choisissez l'onglet Résolution de l'entité.
5. Pour les tables de mappage d'identifiants, choisissez une table.
6. Sur la page des détails de la table de mappage des identifiants, faites défiler la page vers le bas pour afficher les détails de la table de mappage des identifiants.
7. Choisissez Modifier.
8. Sur la page de la table de mappage Modifier l'ID, mettez à jour la description ou les informations d'accès au service.
9. Sélectionnez Enregistrer les modifications.

Supprimer une table de mappage d'identifiants

En tant que membre de la collaboration, vous pouvez supprimer une table de mappage d'identifiants que vous avez créée. Cette action empêche le membre autorisé à interroger la table.

> **Warning**
>
> La suppression d'une table de mappage supprime définitivement toutes les données renseignées.

Pour supprimer une table de mappage d'identifiants

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Choisissez l'onglet Résolution de l'entité.
5. Pour les tables de mappage d'identifiants, choisissez une table.
6. Sur la page des détails de la table de mappage des identifiants, faites défiler la page vers le bas pour afficher les tables de mappage des identifiants.
7. Choisissez une table de mappage d'identifiants, puis choisissez Supprimer.
8. Si vous êtes certain de vouloir supprimer la table de mappage des identifiants, choisissez Supprimer.

Utilisation de modèles d'analyse

Les modèles d'analyse fonctionnent avecRègle d'analyse personnalisée dans AWS Clean Rooms. Avec un modèle d'analyse, vous pouvez définir des paramètres pour vous aider à réutiliser la même requête. AWS Clean Rooms prend en charge un sous-ensemble de paramétrisation avec des valeurs littérales.

Les modèles d'analyse sont spécifiques à la collaboration. Pour chaque collaboration, les membres peuvent uniquement voir les requêtes de cette collaboration. Si vous envisagez d'utiliser la confidentialité différentielle dans le cadre d'une collaboration, vous devez vous assurer que vos modèles d'analyse sont compatibles avec la structure de requête à usage général de AWS Clean Rooms Differential Privacy.

Rubriques

- Création d'un modèle d'analyse
- Révision d'un modèle d'analyse
- Interrogation de tables configurées à l'aide d'un modèle d'analyse

Création d'un modèle d'analyse

Pour plus d'informations sur la création d'un modèle d'analyse à l'aide du AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Pour créer un modèle d'analyse à l'aide de la AWS Clean Rooms console

1. Connectez-vous à la console AWS Management Console et ouvrez-la avec la AWS Clean Rooms console Compte AWS qui fonctionnera en tant que créateur de collaboration.
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Modèles, accédez à la section Modèles d'analyse que vous avez créés.
5. Choisissez Créer un modèle d'analyse.
6. Sur la page Créer un modèle d'analyse, dans Détails, entrez un nom et une description facultative.
7. Pour les tables, consultez les tables configurées associées à la collaboration.

8. Pour la définition,

    a. Entrez la définition du modèle d'analyse.

    b. Choisissez Importer depuis pour importer une définition.

    c. (Facultatif) Spécifiez un paramètre dans l'SQLéditeur en saisissant deux points (`:`) devant le nom du paramètre.

    Par exemple :

    ```
    WHERE table1.date + :date_period > table1.date
    ```

9. Si vous avez déjà ajouté des paramètres, sous Paramètres — facultatif, pour chaque nom de paramètre, choisissez le type et la valeur par défaut (facultatif).
10. Si vous souhaitez activer les balises pour la ressource de table configurée, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
11. Sélectionnez Create (Créer).

Vous êtes maintenant prêt à :

- Informez le membre de votre collaboration qu'il peut consulter un modèle d'analyse. (Facultatif si vous souhaitez interroger vos propres données.)

Révision d'un modèle d'analyse

Une fois qu'un membre de la collaboration a créé un modèle d'analyse, vous pouvez le consulter et l'approuver. Une fois le modèle d'analyse approuvé, il peut entrer dans une requête AWS Clean Rooms.

Pour consulter un modèle d'analyse à l'aide de la AWS Clean Rooms console

1. Connectez-vous à la console AWS Management Console et ouvrez-la avec la AWS Clean Rooms console Compte AWS qui fonctionnera en tant que créateur de collaboration.
2. Dans le volet de navigation de gauche, sélectionnez Collaborations.
3. Choisissez la collaboration.
4. Dans l'onglet Modèles, accédez à la section Modèles d'analyse créés par d'autres membres.
5. Choisissez le modèle d'analyse dont le statut Peut être exécuté est Non nécessite votre révision.
6. Choisissez Examiner.

7. Consultez la présentation, la définition et les paramètres des règles d'analyse (le cas échéant).
8. Passez en revue les tables configurées répertoriées sous Tables référencées dans la définition.

   Le statut à côté de chaque table indiquera Modèle non autorisé.
9. Choisissez une table .

Si vous	Ensuite, choisissez
Approuver le modèle d'analyse	modèle sur table. Confirmez votre approbation en choisissant.
Ne pas approuver le modèle d'analyse	Interdire

Vous êtes maintenant prêt à utiliser le modèle d'analyse pour interroger les tables de données (en tant que membre habilité à effectuer des requêtes).

Interrogation de tables configurées à l'aide d'un modèle d'analyse

Cette procédure explique comment utiliser un modèle d'analyse dans la AWS Clean Rooms console pour interroger des tables configurées à l'aide de la règle d'analyse personnalisée.

Pour utiliser un modèle d'analyse pour interroger les tables configurées à l'aide de la règle d'analyse personnalisée

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration dont le statut de compétences de vos membres est Query.
4. Dans l'onglet Requêtes, sous Tables, consultez les tables et le type de règle d'analyse associé (règle d'analyse personnalisée).

> **Note**
>
> Si les tables attendues ne figurent pas dans la liste, c'est peut-être pour les raisons suivantes :
>
> - Les tables n'ont pas été associées.

- Aucune règle d'analyse n'est configurée pour les tables.

5. Dans la section Analyse, sélectionnez le modèle d'analyse dans la liste déroulante.
6. Entrez la valeur des paramètres à partir du modèle d'analyse que vous souhaitez utiliser dans la requête. La valeur doit correspondre au type de données spécifié par le paramètre. Vous pouvez utiliser des valeurs différentes chaque fois que vous exécutez le modèle d'analyse. Vide ou NULL les valeurs du paramètre ne sont pas prises en charge. L'utilisation de paramètres dans la LIMIT clause n'est pas non plus prise en charge.
7. Cliquez sur Exécuter.

> **Note**
>
> Vous ne pouvez pas exécuter la requête si le membre qui peut recevoir les résultats n'a pas configuré les paramètres des résultats de la requête.

8. Continuez à ajuster les paramètres et réexécutez votre requête, ou cliquez sur le bouton + pour démarrer une nouvelle requête dans un nouvel onglet.

Interrogation de données dans le cadre d'une collaboration

> **Note**
>
> Vous ne pouvez exécuter des requêtes que si le membre chargé de payer les coûts de calcul des requêtes a rejoint la collaboration en tant que membre actif.

En tant que membre habilité à effectuer une requête, vous pouvez effectuer l'une des opérations suivantes :

- Créez une SQL requête manuellement à l'aide de l'éditeur de SQL code.
- Utilisez l'interface utilisateur du générateur d'analyse pour créer une requête sans avoir à écrire de SQL code.
- Utilisez un modèle d'analyse approuvé.

Lorsque le membre habilité à effectuer une requête exécute une SQL requête sur les tables de la collaboration, il AWS Clean Rooms assume les rôles appropriés pour accéder aux tables en son nom. AWS Clean Rooms applique les règles d'analyse nécessaires à la requête d'entrée et à sa sortie.

Les règles d'analyse et les contraintes de sortie sont appliquées automatiquement. AWS Clean Rooms renvoie uniquement les résultats conformes aux règles d'analyse définies.

Pour les requêtes portant sur des données chiffrées, le membre qui peut recevoir les résultats reçoit le résultat chiffré AWS Clean Rooms qui doit être déchiffré.

AWS Clean Rooms prend en charge les SQL requêtes qui peuvent être différentes des autres moteurs de requêtes. Pour les spécifications, voir la AWS Clean Rooms SQLréférence. Si vous souhaitez exécuter des requêtes sur des tables de données protégées par une confidentialité différentielle, vous devez vous assurer que vos requêtes sont compatibles avec la structure de requête à usage général de AWS Clean Rooms Differential Privacy.

> **Note**
>
> Lorsque vous utilisez le calcul cryptographique pour Clean Rooms, toutes les SQL opérations ne génèrent pas de résultats valides. Par exemple, vous pouvez effectuer un COUNT sur

une colonne cryptée, mais effectuer un SUM sur des numéros cryptés entraîne des erreurs. En outre, les requêtes peuvent également donner des résultats incorrects. Par exemple, les requêtes dont les colonnes sont SUM scellées produisent des erreurs. Cependant, une GROUP BY requête sur des colonnes scellées semble réussir mais produit des groupes différents de ceux produits par une GROUP BY requête sur du texte clair.

Le membre qui paie les coûts de calcul des requêtes est facturé pour les requêtes exécutées dans le cadre de la collaboration.

Les rubriques suivantes expliquent comment interroger des données dans le cadre d'une collaboration à l'aide de la AWS Clean Rooms console.

Rubriques

- Interrogation de tables configurées à l'aide de l'éditeur de SQL code
- Interrogation des tables de mappage d'identifiants à l'aide de l'éditeur de SQL code
- Utilisation du générateur d'analyse
- Visualisation de l'impact de la confidentialité différentielle
- Affichage des requêtes récentes
- Affichage des détails de la requête

Pour plus d'informations sur la façon d'interroger des données ou d'afficher des requêtes en appelant directement l' AWS Clean Rooms `StartProtectedQuery`APIopération ou en utilisant le AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Pour plus d'informations sur la journalisation des requêtes, consultezConnexion à une requête AWS Clean Rooms.

> **Note**
>
> Si vous exécutez une requête sur des tables de données chiffrées, les résultats des colonnes chiffrées sont chiffrés.

Pour plus d'informations sur la réception des résultats des requêtes, consultezUtilisation des résultats de requête.

Interrogation de tables configurées à l'aide de l'éditeur de SQL code

En tant que membre habilité à effectuer des requêtes, vous pouvez créer une requête manuellement en écrivant SQL du code dans l'éditeur de SQL code. L'éditeur de SQL code se trouve dans la section Analyse de l'onglet Requêtes de la AWS Clean Rooms console.

L'éditeur de SQL code est affiché par défaut. Si vous souhaitez utiliser le générateur d'analyse pour créer des requêtes, consultezUtilisation du générateur d'analyse.

> **Important**
>
> Si vous commencez à écrire une SQL requête dans l'éditeur de code, puis que vous activez l'interface utilisateur du générateur d'analyse, votre requête n'est pas enregistrée.

AWS Clean Rooms prend en charge de nombreuses SQL commandes, fonctions et conditions. Pour plus d'informations, consultez la AWS Clean Rooms SQLréférence.

> **Tip**
>
> Si une maintenance planifiée a lieu pendant l'exécution d'une requête, celle-ci est interrompue et annulée. Vous devez relancer la requête.

Pour interroger les tables configurées à l'aide de l'éditeur SQL de code

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration dont le statut de compétences de vos membres est Query.
4. Dans l'onglet Requêtes, accédez à la section Analyse.

> **Note**
>
> La section Analyse s'affiche uniquement si le membre qui peut recevoir les résultats et le membre chargé de payer les coûts de calcul des requêtes ont rejoint la collaboration en tant que membre actif.

5. Dans l'onglet Requêtes, sous Tables, consultez la liste des tables et le type de règle d'analyse associé (règle d'analyse d'agrégation, règle d'analyse de liste ou règle d'analyse personnalisée).

> **Note**
>
> Si les tables attendues ne figurent pas dans la liste, c'est peut-être pour les raisons suivantes :
>
> - Les tables n'ont pas été associées.
> - Aucune règle d'analyse n'est configurée pour les tables.

6. (Facultatif) Pour afficher le schéma et les contrôles des règles d'analyse du tableau, développez le tableau en sélectionnant l'icône du signe plus (+).
7. Créez la requête en la saisissant dans l'éditeur de SQL code.

(Facultatif) Si vous souhaitez utiliser un exemple de requête	(Facultatif) Si vous souhaitez insérer des noms de colonnes ou des fonctions
1. Sélectionnez les trois points verticaux à côté du tableau. 2. Sous Insérer dans l'éditeur, sélectionnez Exemple de requête. **Note** L'insertion d'une requête d'exemple ajoute la requête déjà dans l'éditeur.	1. Sélectionnez les trois points verticaux à côté d'une colonne. 2. Sous Insérer dans l'éditeur, sélectionnez Nom de colonne. 3. Pour insérer manuellement une fonction autorisée sur une colonne, sélectionnez les trois points verticaux à côté d'une colonne, sélectionnez Insérer dans l'éditeur, puis sélectionnez le nom de la fonction autorisée

(Facultatif) Si vous souhaitez utiliser un exemple de requête	(Facultatif) Si vous souhaitez insérer des noms de colonnes ou des fonctions
L'exemple de requête apparaît. Toutes les tables répertoriées sous Tables sont incluses dans la requête. 3. Modifiez les valeurs de l'espace réservé dans la requête.	(par exemple INNER JOINSUM, SUMDISTINCT, ouCOUNT). 4. Appuyez sur Ctrl + Espace pour afficher les schémas de table dans l'éditeur de code. **Note** Les membres autorisés à effectuer des requêtes peuvent consulter et utiliser les colonnes de partition dans chaque association de tables configurée. Assurez-v ous que la colonne de partition est étiquetée en tant que colonne de partition dans la AWS Glue table sous-jacente à la table configurée. 5. Modifiez les valeurs de l'espace réservé dans la requête.

8. Pour la livraison des résultats, spécifiez qui peut recevoir les résultats dans Envoyer les résultats à.
9. Cliquez sur Exécuter.

> **Note**
>
> Vous ne pouvez pas exécuter la requête si le membre qui peut recevoir les résultats n'a pas configuré les paramètres des résultats de la requête.

10. Consultez les résultats.

    Pour de plus amples informations, veuillez consulter Utilisation des résultats de requête.

11. Continuez à ajuster les paramètres et réexécutez votre requête, ou cliquez sur le bouton + pour démarrer une nouvelle requête dans un nouvel onglet.

> **Note**
>
> AWS Clean Rooms vise à fournir un message d'erreur clair. Si un message d'erreur ne contient pas suffisamment de détails pour vous aider à résoudre le problème, contactez l'équipe chargée du compte. Fournissez-leur une description de la façon dont l'erreur s'est produite et du message d'erreur (y compris les éventuels identifiants). Pour de plus amples informations, veuillez consulter Résolution des problèmes AWS Clean Rooms.

Interrogation des tables de mappage d'identifiants à l'aide de l'éditeur de SQL code

La procédure suivante décrit comment exécuter une requête de jointure multitable sur la table de mappage d'ID pour joindre `sourceId` le`targetId`.

Avant de demander la table de mappage d'identifiants, celle-ci doit être correctement renseignée.

Pour interroger les tables de mappage d'identifiants à l'aide de l'éditeur de SQL code

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration dont le statut de capacité de vos membres est défini sur Exécuter des requêtes.
4. Dans l'onglet Requêtes, accédez à la section Analyse.

> **Note**
>
> La section Analyse s'affiche uniquement si le membre qui peut recevoir les résultats et le membre chargé de payer les coûts de calcul des requêtes ont rejoint la collaboration en tant que membre actif.

5. Dans l'onglet Requêtes, sous Tables, consultez la liste des tables de mappage d'ID (sous Géré par AWS Clean Rooms) et le type de règle d'analyse associé (règle d'analyse de table de mappage d'ID).

> **Note**
>
> Si vous ne voyez pas les tables de mappage d'identifiants que vous attendez dans la liste, c'est peut-être parce que les tables de mappage d'identifiants n'ont pas été correctement remplies. Pour de plus amples informations, veuillez consulter Remplissage d'une table de mappage d'identifiants existante.

6. Créez la requête en la saisissant dans l'éditeur de SQL code.

(Facultatif) Si vous souhaitez utiliser un exemple de requête	(Facultatif) Si vous souhaitez insérer un nom de table
1. Sélectionnez les trois points verticaux à côté du tableau. 2. Sous Insérer dans l'éditeur, sélectionnez Exemple de JOIN déclaration. **Note** L'insertion d'un exemple de JOIN statmenets ajoute la requête déjà dans l'éditeur. L'exemple de JOIN déclaration apparaît.	1. Sélectionnez les trois points verticaux à côté d'une colonne. 2. Sous Insérer dans l'éditeur, choisissez Nom de la table. 3. Modifiez les valeurs de l'espace réservé dans la requête.

(Facultatif) Si vous souhaitez utiliser un exemple de requête	(Facultatif) Si vous souhaitez insérer un nom de table
3. Modifiez les valeurs de l'espace réservé dans la requête.	

7. Cliquez sur Exécuter.

> **Note**
>
> Vous ne pouvez pas exécuter la requête si le membre qui peut recevoir les résultats n'a pas configuré les paramètres des résultats de la requête.

8. Consultez les résultats.

   Pour de plus amples informations, veuillez consulter Utilisation des résultats de requête.

9. Continuez à ajuster les paramètres et réexécutez votre requête, ou cliquez sur le bouton + pour démarrer une nouvelle requête dans un nouvel onglet.

> **Note**
>
> AWS Clean Rooms vise à fournir un message d'erreur clair. Si un message d'erreur ne contient pas suffisamment de détails pour vous aider à résoudre le problème, contactez l'équipe chargée du compte. Fournissez-leur une description de la façon dont l'erreur s'est produite et du message d'erreur (y compris les éventuels identifiants). Pour de plus amples informations, veuillez consulter Résolution des problèmes AWS Clean Rooms.

Utilisation du générateur d'analyse

Vous pouvez utiliser le générateur d'analyse pour créer des requêtes sans avoir à écrire de SQL code. Avec le générateur d'analyse, vous pouvez créer une requête pour une collaboration qui possède :

- Une table unique qui utilise la règle d'analyse d'agrégation sans JOIN obligation
- Deux tables (une pour chaque membre) qui utilisent toutes deux la règle d'analyse d'agrégation
- Deux tables (une pour chaque membre) qui utilisent toutes deux la règle d'analyse de liste

- Deux tables (une pour chaque membre) qui utilisent toutes deux la règle d'analyse d'agrégation et deux tables (une pour chaque membre) qui utilisent toutes deux la règle d'analyse de liste

Si vous souhaitez écrire des SQL requêtes manuellement, consultezInterrogation de tables configurées à l'aide de l'éditeur de SQL code.

Le générateur d'analyse apparaît sous forme d'option d'interface utilisateur du générateur d'analyse dans la section Analyse de l'onglet Requêtes de la AWS Clean Rooms console.

> **Important**
>
> Si vous activez l'interface utilisateur du générateur d'analyse, que vous commencez à créer une requête dans le générateur d'analyse, puis que vous désactivez l'interface utilisateur du générateur d'analyse, votre requête n'est pas enregistrée.

> **Tip**
>
> Si une maintenance planifiée a lieu pendant l'exécution d'une requête, celle-ci est interrompue et annulée. Vous devez relancer la requête.

Les rubriques suivantes expliquent comment utiliser le générateur d'analyse.

Rubriques

- Utiliser le générateur d'analyse pour interroger une seule table (agrégation)
- Utilisez le générateur d'analyse pour interroger deux tables (agrégation ou liste)

Utiliser le générateur d'analyse pour interroger une seule table (agrégation)

Cette procédure explique comment utiliser l'interface utilisateur du générateur d'analyse dans la AWS Clean Rooms console pour créer une requête. La requête concerne une collaboration comportant une seule table qui utilise la règle d'analyse d'agrégation sans JOIN obligation.

Pour utiliser le générateur d'analyse pour interroger une seule table

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration dont le statut de compétences de vos membres est Query.
4. Dans l'onglet Requêtes, sous Tables, consultez la table et le type de règle d'analyse associé. (Le type de règle d'analyse doit être la règle d'analyse d'agrégation.)

> **Note**
>
> Si le tableau que vous attendez ne s'affiche pas, c'est peut-être pour les raisons suivantes :
>
> - La table n'a pas été associée.
> - Aucune règle d'analyse n'est configurée dans le tableau.

5. Dans la section Analyse, activez l'interface utilisateur du générateur d'analyse.
6. Créez une requête.

   Si vous souhaitez voir toutes les mesures d'agrégation, passez à l'étape 9.

   a. Pour Choose metrics, passez en revue les métriques agrégées qui ont été présélectionnées par défaut et supprimez toute métrique si nécessaire.
   b. (Facultatif) Pour Ajouter des segments — facultatif, choisissez un ou plusieurs paramètres.

   > **Note**
   >
   > Ajouter des segments : cette option n'est affichée que si des dimensions sont spécifiées pour le tableau.

   c. (Facultatif) Pour Ajouter des filtres : facultatif, choisissez Ajouter un filtre, puis choisissez un paramètre, un opérateur et une valeur.

      Pour ajouter d'autres filtres, choisissez Ajouter un autre filtre.

      Pour supprimer un filtre, choisissez Supprimer.

   > **Note**
   >
   > ORDER BYn'est pas pris en charge pour les requêtes d'agrégation.
   > Seul l'ANDopérateur est pris en charge dans les filtres.

d. (Facultatif) Pour Ajouter une description — facultatif, entrez une description pour aider à identifier la requête dans la liste des requêtes.

7. Développez le SQLcode de prévisualisation.

   a. Affichez le SQL code généré à partir du générateur d'analyse.

   b. Pour copier le SQL code, choisissez Copier.

   c. Pour modifier le SQL code, choisissez Modifier dans l'éditeur de SQL code.

8. Cliquez sur Exécuter.

> **Note**
>
> Vous ne pouvez pas exécuter la requête si le membre qui peut recevoir les résultats n'a pas configuré les paramètres des résultats de la requête.

9. Continuez à ajuster les paramètres et réexécutez votre requête, ou cliquez sur le bouton + pour démarrer une nouvelle requête dans un nouvel onglet.

> **Note**
>
> AWS Clean Rooms vise à fournir un message d'erreur clair. Si un message d'erreur ne contient pas suffisamment de détails pour vous aider à résoudre le problème, contactez l'équipe chargée du compte. Fournissez-leur une description de la façon dont l'erreur s'est produite et du message d'erreur (y compris les éventuels identifiants). Pour de plus amples informations, veuillez consulter Résolution des problèmes AWS Clean Rooms.

Utilisez le générateur d'analyse pour interroger deux tables (agrégation ou liste)

Cette procédure décrit comment utiliser le générateur d'analyse de la AWS Clean Rooms console pour créer une requête pour une collaboration qui possède :

- Deux tables (une pour chaque membre) qui utilisent toutes deux la règle d'analyse d'agrégation
- Deux tables (une pour chaque membre) qui utilisent toutes deux la règle d'analyse de liste
- Deux tables (une pour chaque membre) qui utilisent toutes deux la règle d'analyse d'agrégation et deux tables (une pour chaque membre) qui utilisent toutes deux la règle d'analyse de liste

Pour utiliser le générateur d'analyse pour interroger deux tables

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration dont le statut de compétences de vos membres est Query.
4. Dans l'onglet Requêtes, sous Tables, consultez les deux tables et le type de règle d'analyse associé (règle d'analyse d'agrégation ou règle d'analyse de liste).

> **Note**
>
> Si les tables attendues ne figurent pas dans la liste, c'est peut-être pour les raisons suivantes :
>
> - Les tables n'ont pas été associées.
> - Aucune règle d'analyse n'est configurée pour les tables.

5. Dans la section Analyse, activez l'interface utilisateur du générateur d'analyse.
6. Créez une requête.

Si la collaboration contient deux tables qui utilisent la règle d'analyse d'agrégation et deux tables qui utilisent la règle d'analyse de liste, choisissez d'abord Agrégation ou Liste, puis suivez les instructions en fonction de la règle d'analyse sélectionnée.

Si les deux tables utilisent la règle d'analyse d'agrégation	Si les deux tables utilisent la règle d'analyse de liste
1. Pour Choose metrics, passez en revue les métriques agrégées qui ont été présélect ionnées par défaut et supprimez toute métrique si nécessaire. 2. Pour Match records, sélection nez un ou plusieurs enregistr ements.	1. Pour Choisir les attributs, passez en revue les attributs de liste présélectionnés par défaut et supprimez toute métrique si nécessaire. 2. Pour Match records, sélection nez un ou plusieurs enregistr ements.

Si les deux tables utilisent la règle d'analyse d'agrégation	Si les deux tables utilisent la règle d'analyse de liste

> **Note**
>
> Lorsque vous utilisez le générateur d'analyse, vous ne pouvez effectuer de correspondance que sur une seule paire de colonnes.

3. (Facultatif) Pour Ajouter des segments — facultatif, choisissez un ou plusieurs paramètres.

   > **Note**
   >
   > Ajouter des segments : cette option n'est affichée que si des dimensions sont spécifiées pour le tableau.

4. (Facultatif) Pour Ajouter des filtres : facultatif, choisissez Ajouter un filtre, puis choisissez un paramètre, un opérateur et une valeur.

   Pour ajouter d'autres filtres, choisissez Ajouter un autre filtre.

> **Note**
>
> Lorsque vous utilisez le générateur d'analyse, vous ne pouvez effectuer de correspondance que sur une seule paire de colonnes.

3. (Facultatif) Pour Ajouter des filtres : facultatif, choisissez Ajouter un filtre, puis choisissez un paramètre, un opérateur et une valeur.

   Pour ajouter d'autres filtres, choisissez Ajouter un autre filtre.

   Pour supprimer un filtre, choisissez Supprimer.

   > **Note**
   >
   > LIMITn'est pas pris en charge pour les requêtes de liste. Seul l'ANDopérateur est pris en charge dans les filtres.

4. (Facultatif) Pour Ajouter une description — facultatif, entrez une description pour aider à

Si les deux tables utilisent la règle d'analyse d'agrégation	Si les deux tables utilisent la règle d'analyse de liste
Pour supprimer un filtre, choisissez Supprimer. **Note** ORDER BYn'est pas pris en charge pour les requêtes d'agrégation. Seul l'ANDopérateur est pris en charge dans les filtres. 5. (Facultatif) Pour Ajouter une description — facultatif, entrez une description pour aider à identifier la requête dans la liste des requêtes récentes.	identifier la requête dans la liste des requêtes récentes.

7. Développez le SQLcode de prévisualisation.
   a. Affichez le SQL code généré à partir du générateur d'analyse.
   b. Pour copier le SQL code, choisissez Copier.
   c. Pour modifier le SQL code, choisissez Modifier dans l'éditeur de SQL code.
8. Cliquez sur Exécuter.

> **Note**
> Vous ne pouvez pas exécuter la requête si le membre qui peut recevoir les résultats n'a pas configuré les paramètres des résultats de la requête

9. Continuez à ajuster les paramètres et réexécutez votre requête, ou cliquez sur le bouton + pour démarrer une nouvelle requête dans un nouvel onglet.

> **Note**
>
> AWS Clean Rooms vise à fournir un message d'erreur clair. Si un message d'erreur ne contient pas suffisamment de détails pour vous aider à résoudre le problème, contactez l'équipe chargée du compte. Fournissez-leur une description de la façon dont l'erreur s'est produite et du message d'erreur (y compris les éventuels identifiants). Pour de plus amples informations, veuillez consulter Résolution des problèmes AWS Clean Rooms.

Visualisation de l'impact de la confidentialité différentielle

En général, l'écriture et l'exécution de requêtes ne changent pas lorsque la confidentialité différentielle est activée. Toutefois, vous ne pouvez pas exécuter de requête s'il ne reste pas suffisamment de budget de confidentialité. Au fur et à mesure que vous exécutez des requêtes et que vous consommez le budget de confidentialité, vous pouvez voir approximativement le nombre d'agrégations que vous pouvez exécuter et l'impact que cela pourrait avoir sur les requêtes futures.

Pour voir l'impact de la confidentialité différentielle dans une collaboration

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration dont le statut « Vos informations de membre » est « Exécuter des requêtes ».
4. Dans l'onglet Requêtes, sous Tables, consultez le budget de confidentialité restant. Ceci est affiché sous la forme du nombre estimé de fonctions d'agrégation restantes et de l'utilitaire utilisé (rendu sous forme de pourcentage).

   > **Note**
   >
   > Le nombre estimé de fonctions d'agrégation restantes et le pourcentage de l'utilitaire utilisé ne s'affichent que pour le membre autorisé à effectuer des requêtes.

5. Choisissez Afficher l'impact pour voir le niveau de bruit injecté dans les résultats et le nombre approximatif de fonctions d'agrégation que vous pouvez exécuter.

Affichage des requêtes récentes

Vous pouvez consulter les requêtes exécutées au cours des 90 derniers jours dans l'onglet Requêtes récentes.

> **Note**
>
> Si votre seule capacité de membre concerne les données Contribute et que vous n'êtes pas le membre qui paie les coûts de calcul des requêtes, l'onglet Requêtes n'apparaît pas sur la console.

Pour consulter les requêtes récentes

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez une collaboration.
4. Dans l'onglet Requêtes, sous Requêtes, consultez les requêtes exécutées au cours des 90 derniers jours.
5. Pour trier les requêtes récentes par statut, sélectionnez un statut dans la liste déroulante Tous les statuts.

   Les statuts sont les suivants : Soumis, Commencé, Annulé, Réussite, Échec et Expéré.

Affichage des détails de la requête

Vous pouvez consulter les détails de la requête en tant que membre habilité à exécuter des requêtes ou en tant que membre habilité à recevoir les résultats.

Pour afficher les détails de la requête

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez une collaboration.

4. Dans l'onglet Requêtes, effectuez l'une des opérations suivantes :

   - Cliquez sur le bouton d'option correspondant à la requête spécifique que vous souhaitez consulter, puis sélectionnez Afficher les détails.
   - Choisissez l'ID de requête protégé.

5. Sur la page Détails de la requête,

   - Si vous êtes le membre autorisé à exécuter des requêtes, consultez les détails de la requête, le SQLtexte et les résultats.

     Un message s'affiche pour confirmer que les résultats de la requête ont été transmis au membre autorisé à recevoir les résultats.
   - Si vous êtes le membre autorisé à recevoir les résultats, consultez les détails de la requête et les résultats.

Utilisation des résultats de requête

Le membre qui peut recevoir les résultats examine les résultats de la requête dans la AWS Clean Rooms console ou dans le compartiment Amazon S3 qu'il a spécifié lorsqu'il a rejoint la collaboration.

> **Note**
>
> Pour les tables de données chiffrées uniquement, le membre qui peut recevoir les résultats déchiffre les résultats de la requête en exécutant le client de chiffrement C3R en mode déchiffrement.

Les rubriques suivantes expliquent comment recevoir les résultats d'une requête à l'aide de la AWS Clean Rooms console.

Rubriques

- Réception des résultats d'une requête
- Modification des valeurs par défaut pour les paramètres des résultats de requête
- Utilisation du résultat de la requête dans d'autres AWS services

Pour plus d'informations sur la façon d'interroger des données ou d'afficher des requêtes en appelant AWS Clean Rooms API directement le ou en utilisant le AWS SDKs, consultez la AWS Clean Rooms APIréférence.

Pour plus d'informations sur la journalisation des requêtes, consultezConnexion à une requête AWS Clean Rooms.

> **Note**
>
> Si vous exécutez une requête sur des tables de données chiffrées, les résultats des colonnes chiffrées sont chiffrés.

Réception des résultats d'une requête

Les résultats de la requête se trouvent dans la section Paramètres par défaut des résultats de requête et dans la section Requêtes de l'onglet Requêtes de la AWS Clean Rooms console.

Pour recevoir les résultats d'une requête

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration dont le statut de capacité de vos membres est de recevoir des résultats.
4. Pour recevoir les résultats de la requête directement AWS Clean Rooms, dans l'onglet Requêtes, sous Requêtes, sous la colonne ID de requête protégé, sélectionnez la requête.
5. Sur la page Détails de la requête, sous Résultats, effectuez l'une des opérations suivantes :

Si tu veux...	Ensuite, choisissez...
Copiez les résultats.	Copy
Téléchargez les résultats.	Download **Note** Par défaut, le nom du fichier téléchargé est celui `Query id` qui était affiché lors de l'exécution de la requête. AWS Clean Rooms
Consultez les résultats dans Amazon S3.	Afficher dans Amazon S3 La console Amazon S3 s'ouvre dans un onglet séparé.

6. Si vous utilisez des données chiffrées, vous pouvez désormais déchiffrer les tables de données.

   Pour de plus amples informations, veuillez consulter Déchiffrer des tables de données avec le client de chiffrement C3R.

Modification des valeurs par défaut pour les paramètres des résultats de requête

En tant que membre habilité à recevoir des résultats, vous pouvez modifier les valeurs par défaut des paramètres des résultats de requête dans la AWS Clean Rooms console.

Pour modifier les valeurs par défaut des paramètres des résultats de requête

1. Connectez-vous à la AWS Clean Rooms 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, sélectionnez Collaborations.
3. Choisissez la collaboration dont le statut de capacité de vos membres est de recevoir des résultats.
4. Dans l'onglet Requêtes, sous Paramètres des résultats de requête, sélectionnez Modifier.
5. Sur la page Modifier les paramètres par défaut des résultats de requête, modifiez l'une des options suivantes, selon vos besoins :

    a. Sous Paramètres des résultats de requête, modifiez la destination des résultats dans Amazon S3 ou le format des résultats.

    b. Sous Accès au service, modifiez la méthode AWS Clean Rooms pour autoriser l'écriture dans le compartiment Amazon S3 et le format que vous avez spécifiés.

    Les paramètres de résultats de requête mis à jour apparaissent sur la page détaillée de la collaboration.

Utilisation du résultat de la requête dans d'autres AWS services

SQLla sortie de requête peut être utilisée pour les données de départ d'un modèle Clean Rooms ML. Pour plus d'informations, consultez AWS Clean Rooms ML.

Le résultat de la requête AWS Clean Rooms est disponible sur la console (si la console est utilisée pour exécuter des requêtes) et est téléchargé dans un compartiment Amazon S3 spécifié. À partir de là, vous pouvez utiliser le résultat de la requête dans d'autres services AWS services, tels qu'Amazon QuickSight et Amazon SageMaker, en fonction de la manière dont ces services utilisent les données d'Amazon S3.

Pour plus d'informations sur Amazon QuickSight, consultez la QuickSightdocumentation Amazon.

Pour plus d'informations sur Amazon SageMaker, consultez la SageMakerdocumentation Amazon.

Résolution des problèmes AWS Clean Rooms

Cette section décrit certains problèmes courants susceptibles de survenir lors de l'utilisation AWS Clean Rooms et explique comment les résoudre.

Problèmes

Une ou plusieurs tables référencées par la requête ne sont pas accessibles par le rôle de service associé. Le propriétaire de la table/du rôle doit autoriser le rôle de service à accéder à la table.

- Vérifiez que les autorisations pour le rôle de service sont configurées conformément aux exigences. Pour plus d'informations, consultezCon AWS Clean Rooms figuration.

L'un des ensembles de données sous-jacents possède un format de fichier non pris en charge.

- Assurez-vous que votre ensemble de données est dans l'un des formats de fichier pris en charge :
  - Parquet
  - RCFile
  - TextFile
  - SequenceFile
  - RegexSerde
  - OpenCSV
  - AVRO
  - JSON

Pour plus d'informations, consultez Formats de données pour AWS Clean Rooms.

Les résultats des requêtes ne sont pas ceux attendus lors de l'utilisation de l'informatique cryptographique pourClean Rooms.

Si vous utilisez l'informatique cryptographique pour Clean Rooms (C3R), vérifiez que votre requête utilise correctement les colonnes chiffrées :

- Les sealed colonnes ne sont utilisées que dans les SELECT clauses.
- Les fingerprint colonnes ne sont utilisées que dans JOIN les clauses (et GROUP BY les clauses sous certaines conditions).
- Que vous n'êtes que JOINing fingerprint des colonnes portant le même nom si les paramètres de collaboration l'exigent.

Pour plus d'informations, consultez Informatique cryptographique et the section called "Types de colonnes".

Sécurité dans AWS Clean Rooms

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Clean Rooms, voir AWSServices concernés par programme de conformité AWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Clean Rooms. Il vous explique comment procéder à la configuration AWS Clean Rooms pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS Clean Rooms ressources.

Table des matières

Protection des données dans AWS Clean Rooms

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Clean Rooms. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des AWS services que vous utilisez. 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 modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou 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 les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent AWS services.
- 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 point de terminaison. FIPS 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 AWS Clean Rooms ou d'autres AWS services utilisateurs 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 y inclure d'informations d'identification URL pour valider votre demande auprès de ce serveur.

Chiffrement au repos

AWS Clean Rooms chiffre toujours toutes les métadonnées du service au repos sans nécessiter de configuration supplémentaire. Ce chiffrement est automatique lorsque vous l'utilisez AWS Clean Rooms.

Clean Rooms ML chiffre toutes les données stockées dans le service au repos avec AWS KMS. Si vous choisissez de fournir votre propre KMS clé, le contenu de vos modèles similaires et de vos tâches de génération de segments similaires est chiffré au repos avec votre KMS clé.

> **Note**
>
> Vous pouvez utiliser les options de chiffrement d'Amazon S3 pour protéger vos données au repos.
> Pour plus d'informations, consultez la section Spécification du chiffrement Amazon S3 dans le guide de l'utilisateur Amazon S3.

Lorsque vous utilisez une table de mappage d'identifiants à l'intérieur AWS Clean Rooms, le service chiffre toutes les données stockées au repos avec AWS KMS. Si vous choisissez de fournir votre propre KMS clé, le contenu de votre table de mappage d'identifiants est crypté au repos avec votre KMS clé via Résolution des entités AWS. Pour plus de détails sur les autorisations requises pour utiliser des chiffrements avec un flux de travail de mappage d'identifiants, voir Créer un rôle de travail dans le flux de travail Résolution des entités AWS dans le guide de l'Résolution des entités AWS utilisateur.

Chiffrement en transit

AWS Clean Rooms utilise le protocole Transport Layer Security (TLS) et le chiffrement côté client pour le chiffrement en transit. La communication avec AWS Clean Rooms est toujours effectuée, de HTTPS sorte que vos données sont toujours cryptées pendant le transport. Cela inclut toutes les données en transit lors de l'utilisation de Clean Rooms ML.

Chiffrement des données sous-jacentes

Pour plus d'informations sur le chiffrement de vos données sous-jacentes, consultezInformatique cryptographique pour Clean Rooms.

Conservation des données dans AWS Clean Rooms

Lorsque vous créez un modèle similaire, Clean Rooms ML lit vos données d'entraînement, les transforme dans un format adapté à notre modèle ML et stocke les paramètres du modèle entraîné dans Clean Rooms ML. Clean Rooms ML ne conserve aucune copie de vos données d'entraînement. AWS Clean Rooms SQLles requêtes ne conservent aucune de vos données une fois la requête exécutée. Clean Rooms ML utilise ensuite le modèle entraîné pour résumer le comportement de tous vos utilisateurs. Clean Rooms ML stocke un ensemble de données au niveau utilisateur pour chaque utilisateur de vos données tant que votre modèle de sosie est actif.

Lorsque vous lancez une tâche de génération de segments similaires, Clean Rooms ML lit les données initiales, lit les résumés des comportements à partir du modèle de similarité associé et crée un segment similaire qui est stocké dans le service. AWS Clean Rooms Clean Rooms ML ne conserve pas de copie de vos données de départ. Clean Rooms ML stocke les résultats de la tâche au niveau utilisateur tant que celle-ci est active.

Si vos données de départ proviennent d'une SQL requête, le résultat de cette requête n'est stocké dans le service que pendant la durée de la tâche. Les résultats de la requête sont chiffrés au repos et en transit.

Si vous souhaitez supprimer les données de votre tâche de génération de modèles ou de segments similaires, utilisez le API pour les supprimer. Clean Rooms ML supprime de manière asynchrone toutes les données associées au modèle ou à la tâche. Une fois ce processus terminé, Clean Rooms ML supprime les métadonnées du modèle ou de la tâche et celles-ci ne sont plus visibles dans leAPI. Clean Rooms ML conserve les données supprimées pendant 3 jours à des fins de prévention de la reprise après sinistre. Une fois que la tâche ou le modèle n'est plus visible au API bout de 3 jours, toutes les données associées au modèle ou à la tâche sont définitivement supprimées.

Bonnes pratiques pour la collaboration en matière de données dans AWS Clean Rooms

Cette rubrique décrit les meilleures pratiques pour mener des collaborations de données dans AWS Clean Rooms.

AWS Clean Rooms suit le modèle de responsabilitéAWS partagée. AWS Clean Rooms propose des règles d'analyse que vous pouvez configurer pour renforcer votre capacité à protéger les données sensibles dans le cadre d'une collaboration. Les règles d'analyse que vous configurez dans AWS Clean Rooms appliqueront les restrictions (contrôles de requête et contrôles de sortie de requête) que vous avez configurées. Il vous incombe de déterminer les restrictions et de configurer les règles d'analyse en conséquence.

Les collaborations en matière de données peuvent impliquer bien plus que votre simple utilisation de AWS Clean Rooms. Pour vous aider à tirer le meilleur parti des collaborations de données, nous vous recommandons de suivre les meilleures pratiques suivantes en utilisant AWS Clean Rooms et en particulier en ce qui concerne les règles d'analyse.

Rubriques

Les meilleures pratiques avec AWS Clean Rooms

Vous êtes chargé d'évaluer le risque lié à chaque collaboration sur les données et de le comparer à vos exigences en matière de confidentialité, telles que les programmes et politiques de conformité externes et internes. Nous vous recommandons de prendre des mesures supplémentaires lors de l'utilisation de AWS Clean Rooms. Ces actions peuvent contribuer à mieux gérer les risques et à vous protéger contre les tentatives de tiers visant à réidentifier vos données (par exemple, attaques différenciées ou attaques par canal secondaire).

Par exemple, envisagez de faire preuve de diligence raisonnable à l'égard de vos autres collaborateurs et de conclure des accords juridiques avec eux avant de vous engager dans une collaboration. Pour surveiller l'utilisation de vos données, envisagez également d'adopter d'autres mécanismes d'audit lorsque vous utilisez AWS Clean Rooms.

Bonnes pratiques d'utilisation des règles d'analyse dans AWS Clean Rooms

Les règles d'analyse vous AWS Clean Rooms permettent de limiter les requêtes pouvant être exécutées en définissant des contrôles de requête sur une table configurée. Par exemple, vous pouvez définir un contrôle de requête indiquant comment une table configurée peut être jointe et quelles colonnes peuvent être sélectionnées. Vous pouvez également restreindre le résultat de la requête en définissant des contrôles des résultats de requête tels que des seuils d'agrégation sur

les lignes de sortie. Le service rejette toute requête et supprime les lignes non conformes aux règles d'analyse définies par les membres sur leurs tables configurées dans la requête.

Nous recommandons les 10 meilleures pratiques suivantes pour utiliser les règles d'analyse sur votre table configurée :

- Créez des tables configurées distinctes pour des cas d'utilisation de requêtes distincts (par exemple, planification d'audience ou attribution). Vous pouvez créer plusieurs tables configurées avec la même AWS Glue table sous-jacente.
- Spécifiez les colonnes de la règle d'analyse (par exemple, les colonnes de dimension, les colonnes de liste, les colonnes de jointure) qui sont nécessaires pour les requêtes dans le cadre d'une collaboration. Cela peut contribuer à atténuer le risque de différenciation des attaques ou de permettre à d'autres membres de rétroconcevoir vos données. Utilisez la fonctionnalité des colonnes autorisées pour noter les autres colonnes que vous souhaiterez peut-être rendre interrogeables à l'avenir. Pour personnaliser les colonnes qui peuvent être utilisées pour une collaboration donnée, créez des tables configurées supplémentaires avec la même AWS Glue table sous-jacente.
- Spécifiez dans la règle d'analyse les fonctions nécessaires à l'analyse dans le cadre de la collaboration. Cela peut contribuer à atténuer les risques liés à de rares erreurs de fonctionnement susceptibles de présenter des informations sur un point de données individuel. Pour personnaliser les fonctions qui peuvent être utilisées pour une collaboration donnée, créez des tables configurées supplémentaires avec la même AWS Glue table sous-jacente.
- Ajoutez des contraintes d'agrégation à toutes les colonnes dont les valeurs au niveau des lignes sont sensibles. Cela inclut les colonnes de votre table configurée qui existent également dans les tables des autres membres de la collaboration et les règles d'analyse en tant que contrainte d'agrégation. Cela inclut également les colonnes de votre table configurée qui ne sont pas interrogeables, c'est-à-dire les colonnes qui se trouvent dans votre table configurée mais qui ne figurent pas dans la règle d'analyse. Les contraintes d'agrégation peuvent contribuer à atténuer les risques liés à la corrélation des résultats des requêtes avec des données extérieures à la collaboration.
- Créez des collaborations de test et des règles d'analyse pour tester les restrictions créées avec des règles d'analyse spécifiées.
- Passez en revue les tables configurées par le collaborateur et les règles d'analyse des membres sur les tables configurées pour vérifier qu'elles correspondent à ce qui a été convenu pour la collaboration. Cela peut aider à atténuer les risques liés à l'ingénierie par les autres membres de leurs propres données pour exécuter des requêtes qui n'ont pas été convenues.

- Consultez l'exemple de requête fourni (console uniquement) qui est activé sur votre table configurée après avoir configuré la règle d'analyse.

> **Note**
>
> Outre l'exemple de requête fourni, d'autres requêtes sont possibles en fonction de la règle d'analyse, d'autres tables de membres de collaboration et de règles d'analyse.

- Vous pouvez ajouter ou mettre à jour une règle d'analyse pour une table configurée dans une collaboration. Lorsque vous le faites, passez en revue toutes les collaborations auxquelles la table configurée est associée et l'impact qui en résulte. Cela permet de s'assurer qu'aucune collaboration n'utilise de règles d'analyse obsolètes.
- Passez en revue les requêtes exécutées dans le cadre de la collaboration pour vérifier qu'elles correspondent aux cas d'utilisation ou aux requêtes convenus pour la collaboration. (Les requêtes sont disponibles dans les journaux des requêtes lorsque la fonctionnalité de journalisation des requêtes est activée.) Cela peut aider à atténuer les risques liés à l'exécution par les membres d'analyses non approuvées et aux attaques potentielles telles que les attaques par canal secondaire.
- Passez en revue les colonnes de table configurées utilisées dans les règles d'analyse des membres de la collaboration et dans les requêtes pour vérifier qu'elles correspondent à ce qui a été convenu dans le cadre de la collaboration. (Les requêtes sont disponibles dans les journaux de requêtes lorsque cette fonctionnalité est activée.) Cela peut aider à atténuer les risques liés à l'ingénierie par les autres membres de leurs propres données pour effectuer des requêtes qui n'ont pas été convenues.

Identity and Access Management pour AWS Clean Rooms

AWS Identity and Access Management (IAM) est un outil AWS service 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 AWS Clean Rooms ressources. IAMest un AWS service outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Gestion des accès à l'aide de politiques
- Comment AWS Clean Rooms fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour AWS Clean Rooms
- AWS politiques gérées pour AWS Clean Rooms
- Résolution des problèmes AWS Clean Rooms d'identité et d'accès
- Prévention du problème de l'adjoint confus entre services
- IAMcomportements pour le AWS Clean Rooms ML

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez AWS Clean Rooms.

Utilisateur du service : si vous utilisez le AWS Clean Rooms 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 AWS Clean Rooms 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 AWS Clean Rooms, consultez Résolution des problèmes AWS Clean Rooms d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des AWS Clean Rooms ressources de votre entreprise, vous avez probablement un accès complet à AWS Clean Rooms. C'est à vous de déterminer les AWS Clean Rooms 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 AWS Clean Rooms, voirComment AWS Clean Rooms 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 AWS Clean Rooms. Pour consulter des exemples de politiques AWS Clean Rooms basées sur l'identité que vous pouvez utiliser dansIAM, consultez. Exemples de politiques basées sur l'identité pour AWS Clean Rooms

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) ou l'authentification unique de votre entreprise 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 () pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. CLI 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 vos demandes vous-même, veuillez consulter la rubrique Processus de signature Signature Version 4 dans la Références générales AWS.

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, consultez Authentification multifactorielle dans le guide de AWS IAM Identity Center l'utilisateur et Utilisation de l'authentification multifactorielle (MFA) AWS 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 AWS services les ressources du compte. Cette identité est appelée Compte AWS utilisateur root. Vous pouvez y accéder en vous connectant à l'aide de l'adresse électronique et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes. Protégez

vos informations d'identification d'utilisateur root et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Utilisateur racine d'un compte AWS Informations d'identification et IAM identités dans le Références générales AWS.

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 AWS services 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 AWS services 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, voir Quand créer un IAM utilisateur (au lieu d'un rôle) 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. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console changeant de rôle. 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 Utilisation IAM des rôles 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 Création d'un rôle pour un fournisseur d'identité tiers 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 la rubrique 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 AWS services 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 AWS services utilisent des fonctionnalités dans d'autres AWS services. 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 AWS service, combinées à la demande AWS service 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 AWS services 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 Création d'un rôle auquel déléguer des autorisations AWS service 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. AWS service 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 font AWS CLI 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 Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) 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.

Chaque IAM entité (utilisateur ou rôle) démarre sans aucune autorisation. Par défaut, les utilisateurs ne peuvent rien faire, pas même changer leurs propres mots de passe. Pour autoriser un utilisateur à effectuer une opération, un administrateur doit lui associer une politique d'autorisations. Il peut également ajouter l'utilisateur à un groupe disposant des autorisations prévues. Lorsqu'un administrateur accorde des autorisations à un groupe, tous les utilisateurs de ce groupe se voient octroyer ces autorisations.

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 doté de 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 Création de IAM politiques 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 attacher à plusieurs utilisateurs, groupes et rôles dans 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 des politiques gérées et des 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. AWS services

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.

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 obtenues représentent la combinaison des politiques basées sur l'identité de l'entité et de ses limites d'autorisations. 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 remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, voir 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 OrganizationsSCPs, voir Comment SCPs travailler 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 AWS Clean Rooms fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Clean Rooms, découvrez quelles IAM fonctionnalités sont disponibles AWS Clean Rooms.

IAMfonctionnalités que vous pouvez utiliser avec AWS Clean Rooms

IAMfonctionnalité	AWS Clean Rooms soutien
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Partielle
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Partielle

IAMfonctionnalité	AWS Clean Rooms soutien
ACLs	Non
ABAC(balises dans les politiques)	Oui
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 du fonctionnement de la plupart des fonctionnalités AWS Clean Rooms et des autres AWS services IAM fonctionnalités, consultez la section AWS services relative à leur fonctionnement IAM dans le guide de IAM l'utilisateur.

Politiques basées sur l'identité pour AWS Clean Rooms

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 Création de IAM politiques 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 AWS Clean Rooms

Pour consulter des exemples de politiques AWS Clean Rooms basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Clean Rooms

Politiques basées sur les ressources au sein de AWS Clean Rooms

Prend en charge les politiques basées sur les ressources : partiel

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. AWS services

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, voir Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Le AWS Clean Rooms service ne prend en charge qu'un seul type de politique basée sur les ressources, appelée politique de ressources gérées par modèle similaire configuré, qui est attachée à un modèle similaire configuré. Cette politique définit les principaux autorisés à effectuer des actions sur le modèle similaire configuré.

Pour savoir comment associer une politique basée sur les ressources à un modèle similaire configuré, consultez. IAMcomportements pour le AWS Clean Rooms ML

Actions politiques pour AWS Clean Rooms

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 stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des AWS Clean Rooms actions, voir Actions définies par AWS Clean Rooms dans la référence d'autorisation de service.

Les actions de politique en AWS Clean Rooms cours utilisent le préfixe suivant avant l'action.

```
cleanrooms
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour consulter des exemples de politiques AWS Clean Rooms basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Clean Rooms

Ressources politiques pour AWS Clean Rooms

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 AWS Clean Rooms ressources et leurs caractéristiquesARNs, voir Ressources définies par AWS Clean Rooms 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 AWS Clean Rooms.

Pour consulter des exemples de politiques AWS Clean Rooms basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Clean Rooms

Clés de conditions de politique pour AWS Clean Rooms

Prend en charge les clés de condition de politique spécifiques au service : partiel

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 savoir comment le AWS Clean Rooms ML utilise les clés de condition de politique, consultez IAMcomportements pour le AWS Clean Rooms ML.

ACLsdans AWS Clean Rooms

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 AWS Clean Rooms

Supports ABAC (balises dans les politiques) : Oui

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 Qu'est-ce que c'est ABAC ? 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 AWS Clean Rooms

Prend en charge les informations d'identification temporaires : oui

Certains AWS services ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui AWS services fonctionnent avec des informations d'identification temporaires, consultez AWS services 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, consultez la section Passage à un 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 AWS Clean Rooms

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 AWS service, combinées à la demande AWS service 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 AWS services 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 AWS Clean Rooms

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 Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber AWS Clean Rooms les fonctionnalités. Modifiez les rôles de service uniquement lorsque AWS Clean Rooms vous recevez des instructions à cet effet.

Rôles liés à un service pour AWS Clean Rooms

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. AWS service 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 AWS Clean Rooms

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources AWS Clean Rooms . 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, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par AWS Clean Rooms, y compris le format de ARNs pour chacun des types de ressources, voir Actions, ressources et clés de condition AWS Clean Rooms dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console AWS Clean Rooms
- 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 AWS Clean Rooms 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 du Guide de IAM l'utilisateur. IAM

- 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 AWS service, 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 Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.
- 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 Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

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 AWS Clean Rooms

Pour accéder à la AWS Clean Rooms console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails AWS Clean Rooms des ressources de votre Compte AWS. Si vous créez une stratégie 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 stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement 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 AWS Clean Rooms console, associez également la politique AWS Clean Rooms `FullAccess` 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 AWS Clean Rooms

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 AWS service est lancée ou que de nouvelles API opérations sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques AWS gérées dans le Guide de IAM l'utilisateur.

AWS politique gérée : **`AWSCleanRoomsReadOnlyAccess`**

Vous pouvez vous rattacher `AWSCleanRoomsReadOnlyAccess` à vos IAM mandants.

Cette politique accorde des autorisations en lecture seule aux ressources et aux métadonnées dans le cadre d'une `AWSCleanRoomsReadOnlyAccess` collaboration.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `CleanRoomsRead`— Permet aux principaux d'accéder au service en lecture seule.
- `ConsoleDisplayTables`— Permet aux principaux d'accéder en lecture seule aux AWS Glue métadonnées nécessaires pour afficher les données relatives aux AWS Glue tables sous-jacentes sur la console.

- `ConsoleLogSummaryQueryLogs`— Permet aux principaux de consulter les journaux de requêtes.
- `ConsoleLogSummaryObtainLogs`— Permet aux principaux de récupérer les résultats du journal.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CleanRoomsRead",
   "Effect": "Allow",
   "Action": [
    "cleanrooms:BatchGet*",
    "cleanrooms:Get*",
    "cleanrooms:List*"
   ],
   "Resource": "*"
  },
  {
   "Sid": "ConsoleDisplayTables",
   "Effect": "Allow",
   "Action": [
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:GetSchema",
    "glue:GetSchemaVersion",
    "glue:BatchGetPartition"
   ],
   "Resource": "*"
  },
  {
   "Sid": "ConsoleLogSummaryQueryLogs",
   "Effect": "Allow",
   "Action": [
    "logs:StartQuery"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
```

```
    "Sid": "ConsoleLogSummaryObtainLogs",
    "Effect": "Allow",
    "Action": [
     "logs:GetQueryResults"
    ],
    "Resource": "*"
   }
  ]
}
```

AWS politique gérée : **AWSCleanRoomsFullAccess**

Vous pouvez vous rattacher `AWSCleanRoomsFullAccess` à vos IAM mandants.

Cette politique accorde des autorisations administratives qui permettent un accès complet (lecture, écriture et mise à jour) aux ressources et aux métadonnées d'une AWS Clean Rooms collaboration. Cette politique inclut l'accès pour effectuer des requêtes.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `CleanRoomsAccess`— Accorde un accès complet à toutes les actions sur toutes les ressources pour AWS Clean Rooms.
- `PassServiceRole`— Accorde l'accès pour transmettre un rôle de service uniquement au service (`PassedToService`condition) dont le nom contient cleanrooms « ».
- `ListRolesToPickServiceRole`— Permet aux directeurs de répertorier tous leurs rôles afin de choisir un rôle de service lors de l'utilisation AWS Clean Rooms.
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Permet aux principaux de voir le rôle du service et la politique correspondante dansIAM.
- `ListPoliciesToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dansIAM.
- `GetPolicyToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dansIAM.
- `ConsoleDisplayTables`— Permet aux principaux d'accéder en lecture seule aux AWS Glue métadonnées nécessaires pour afficher les données relatives aux AWS Glue tables sous-jacentes sur la console.

- `ConsolePickQueryResultsBucketListAll`— Permet aux principaux de choisir un compartiment Amazon S3 dans une liste de tous les compartiments S3 disponibles dans lesquels les résultats de leurs requêtes sont écrits.
- `SetQueryResultsBucket`— Permet aux principaux de choisir un compartiment S3 dans lequel les résultats de leurs requêtes sont écrits.
- `ConsoleDisplayQueryResults`— Permet aux principaux d'afficher les résultats de la requête au client, lus depuis le compartiment S3.
- `WriteQueryResults`— Permet aux principaux d'écrire les résultats de la requête dans un compartiment S3 appartenant au client.
- `EstablishLogDeliveries`— Permet aux principaux de fournir des journaux de requêtes au groupe de CloudWatch journaux Amazon Logs d'un client.
- `SetupLogGroupsDescribe`— Permet aux principaux d'utiliser le processus de création de groupes de CloudWatch journaux Amazon Logs.
- `SetupLogGroupsCreate`— Permet aux principaux de créer un groupe de CloudWatch journaux Amazon Logs.
- `SetupLogGroupsResourcePolicy`— Permet aux principaux de définir une politique de ressources sur le groupe de CloudWatch journaux Amazon Logs.
- `ConsoleLogSummaryQueryLogs`— Permet aux principaux de consulter les journaux de requêtes.
- `ConsoleLogSummaryObtainLogs`— Permet aux principaux de récupérer les résultats du journal.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CleanRoomsAccess",
   "Effect": "Allow",
   "Action": [
    "cleanrooms:*"
   ],
   "Resource": "*"
  },
  {
   "Sid": "PassServiceRole",
   "Effect": "Allow",
   "Action": [
```

```
    "iam:PassRole"
   ],
   "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*",
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ListRolesToPickServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:ListRoles"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetRoleAndListRolePoliciesToInspectServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:GetRole",
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
   ],
   "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*"
  },
  {
   "Sid": "ListPoliciesToInspectServiceRolePolicy",
   "Effect": "Allow",
   "Action": [
    "iam:ListPolicies"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetPolicyToInspectServiceRolePolicy",
   "Effect": "Allow",
   "Action": [
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
   ],
   "Resource": "arn:aws:iam::*:policy/*cleanrooms*"
  },
```

```
{
 "Sid": "ConsoleDisplayTables",
 "Effect": "Allow",
 "Action": [
  "glue:GetDatabase",
  "glue:GetDatabases",
  "glue:GetTable",
  "glue:GetTables",
  "glue:GetPartition",
  "glue:GetPartitions",
  "glue:GetSchema",
  "glue:GetSchemaVersion",
  "glue:BatchGetPartition"
 ],
 "Resource": "*"
},
{
 "Sid": "ConsolePickQueryResultsBucketListAll",
 "Effect": "Allow",
 "Action": [
  "s3:ListAllMyBuckets"
 ],
 "Resource": "*"
},
{
 "Sid": "SetQueryResultsBucket",
 "Effect": "Allow",
 "Action": [
  "s3:GetBucketLocation",
  "s3:ListBucketVersions"
 ],
 "Resource": "arn:aws:s3:::cleanrooms-queryresults*"
},
{
 "Sid": "WriteQueryResults",
 "Effect": "Allow",
 "Action": [
  "s3:ListBucket",
  "s3:PutObject"
 ],
 "Resource": "arn:aws:s3:::cleanrooms-queryresults*",
 "Condition": {
  "ForAnyValue:StringEquals": {
   "aws:CalledVia": "cleanrooms.amazonaws.com"
```

```
    }
   }
  },
  {
   "Sid": "ConsoleDisplayQueryResults",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject"
   ],
   "Resource": "arn:aws:s3:::cleanrooms-queryresults*"
  },
  {
   "Sid": "EstablishLogDeliveries",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs:DeleteLogDelivery",
    "logs:ListLogDeliveries"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "SetupLogGroupsDescribe",
   "Effect": "Allow",
   "Action": [
    "logs:DescribeLogGroups"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "SetupLogGroupsCreate",
   "Effect": "Allow",
```

```
    "Action": [
     "logs:CreateLogGroup"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "SetupLogGroupsResourcePolicy",
    "Effect": "Allow",
    "Action": [
      "logs:DescribeResourcePolicies",
     "logs:PutResourcePolicy"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "ConsoleLogSummaryQueryLogs",
    "Effect": "Allow",
    "Action": [
     "logs:StartQuery"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
   },
   {
    "Sid": "ConsoleLogSummaryObtainLogs",
    "Effect": "Allow",
    "Action": [
     "logs:GetQueryResults"
    ],
    "Resource": "*"
   }
  ]
}
```

AWS politique gérée : **AWSCleanRoomsFullAccessNoQuerying**

Vous pouvez joindre `AWSCleanRoomsFullAccessNoQuerying` à votreIAM principals.

Cette politique accorde des autorisations administratives qui permettent un accès complet (lecture, écriture et mise à jour) aux ressources et aux métadonnées d'une AWS Clean Rooms collaboration. Cette politique exclut l'accès pour effectuer des requêtes.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `CleanRoomsAccess`— Accorde un accès complet à toutes les actions sur toutes les ressources AWS Clean Rooms, à l'exception des requêtes dans le cadre de collaborations.
- `CleanRoomsNoQuerying`— Refuse explicitement `StartProtectedQuery` et `UpdateProtectedQuery` empêche les requêtes.
- `PassServiceRole`— Accorde l'accès pour transmettre un rôle de service uniquement au service (`PassedToService`condition) dont le nom contient cleanrooms « ».
- `ListRolesToPickServiceRole`— Permet aux directeurs de répertorier tous leurs rôles afin de choisir un rôle de service lors de l'utilisation AWS Clean Rooms.
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Permet aux principaux de voir le rôle du service et la politique correspondante dansIAM.
- `ListPoliciesToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dansIAM.
- `GetPolicyToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dansIAM.
- `ConsoleDisplayTables`— Permet aux principaux d'accéder en lecture seule aux AWS Glue métadonnées nécessaires pour afficher les données relatives aux AWS Glue tables sous-jacentes sur la console.
- `EstablishLogDeliveries`— Permet aux principaux de fournir des journaux de requêtes au groupe de CloudWatch journaux Amazon Logs d'un client.
- `SetupLogGroupsDescribe`— Permet aux principaux d'utiliser le processus de création de groupes de CloudWatch journaux Amazon Logs.
- `SetupLogGroupsCreate`— Permet aux principaux de créer un groupe de CloudWatch journaux Amazon Logs.

- `SetupLogGroupsResourcePolicy`— Permet aux principaux de définir une politique de ressources sur le groupe de CloudWatch journaux Amazon Logs.
- `ConsoleLogSummaryQueryLogs`— Permet aux principaux de consulter les journaux de requêtes.
- `ConsoleLogSummaryObtainLogs`— Permet aux principaux de récupérer les résultats du journal.
- `cleanrooms`— Gérez les collaborations, les modèles d'analyse, les tables configurées, les adhésions et les ressources associées au sein du AWS Clean Rooms service. Effectuez diverses opérations telles que la création, la mise à jour, la suppression, la liste et la récupération d'informations sur ces ressources.
- `iam`— Transmettez les rôles de service dont les noms contiennent `cleanrooms` « » au AWS Clean Rooms service. Répertoriez les rôles, les politiques et inspectez les rôles de service et les politiques liés au AWS Clean Rooms service.
- `glue`— Récupérez des informations sur les bases de données, les tables, les partitions et les schémas à partir de AWS Glue. Cela est nécessaire pour que le AWS Clean Rooms service affiche et interagisse avec les sources de données sous-jacentes.
- `logs`— Gérez les livraisons de journaux, les groupes de journaux et les politiques de ressources pour les CloudWatch journaux. Interrogez et récupérez les journaux relatifs au AWS Clean Rooms service. Ces autorisations sont nécessaires à des fins de surveillance, d'audit et de dépannage au sein du service.

La politique refuse également explicitement les actions `cleanrooms:StartProtectedQuery` et empêche les utilisateurs `cleanrooms:UpdateProtectedQuery` d'exécuter ou de mettre à jour directement les requêtes protégées, ce qui doit être fait par le biais des mécanismes AWS Clean Rooms contrôlés.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CleanRoomsAccess",
   "Effect": "Allow",
   "Action": [
    "cleanrooms:BatchGetCollaborationAnalysisTemplate",
    "cleanrooms:BatchGetSchema",
    "cleanrooms:BatchGetSchemaAnalysisRule",
    "cleanrooms:CreateAnalysisTemplate",
    "cleanrooms:CreateCollaboration",
```

```
    "cleanrooms:CreateConfiguredTable",
    "cleanrooms:CreateConfiguredTableAnalysisRule",
    "cleanrooms:CreateConfiguredTableAssociation",
    "cleanrooms:CreateMembership",
    "cleanrooms:DeleteAnalysisTemplate",
    "cleanrooms:DeleteCollaboration",
    "cleanrooms:DeleteConfiguredTable",
    "cleanrooms:DeleteConfiguredTableAnalysisRule",
    "cleanrooms:DeleteConfiguredTableAssociation",
    "cleanrooms:DeleteMember",
    "cleanrooms:DeleteMembership",
    "cleanrooms:GetAnalysisTemplate",
    "cleanrooms:GetCollaboration",
    "cleanrooms:GetCollaborationAnalysisTemplate",
    "cleanrooms:GetConfiguredTable",
    "cleanrooms:GetConfiguredTableAnalysisRule",
    "cleanrooms:GetConfiguredTableAssociation",
    "cleanrooms:GetMembership",
    "cleanrooms:GetProtectedQuery",
    "cleanrooms:GetSchema",
    "cleanrooms:GetSchemaAnalysisRule",
    "cleanrooms:ListAnalysisTemplates",
    "cleanrooms:ListCollaborationAnalysisTemplates",
    "cleanrooms:ListCollaborations",
    "cleanrooms:ListConfiguredTableAssociations",
    "cleanrooms:ListConfiguredTables",
    "cleanrooms:ListMembers",
    "cleanrooms:ListMemberships",
    "cleanrooms:ListProtectedQueries",
    "cleanrooms:ListSchemas",
    "cleanrooms:UpdateAnalysisTemplate",
    "cleanrooms:UpdateCollaboration",
    "cleanrooms:UpdateConfiguredTable",
    "cleanrooms:UpdateConfiguredTableAnalysisRule",
    "cleanrooms:UpdateConfiguredTableAssociation",
    "cleanrooms:UpdateMembership",
    "cleanrooms:ListTagsForResource",
    "cleanrooms:UntagResource",
    "cleanrooms:TagResource"
   ],
   "Resource": "*"
  },
  {
   "Sid": "CleanRoomsNoQuerying",
```

```
    "Effect": "Deny",
    "Action": [
     "cleanrooms:StartProtectedQuery",
     "cleanrooms:UpdateProtectedQuery"
    ],
    "Resource": "*"
   },
   {
    "Sid": "PassServiceRole",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*",
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "ListRolesToPickServiceRole",
    "Effect": "Allow",
    "Action": [
     "iam:ListRoles"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GetRoleAndListRolePoliciesToInspectServiceRole",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:ListRolePolicies",
     "iam:ListAttachedRolePolicies"
    ],
    "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*"
   },
   {
    "Sid": "ListPoliciesToInspectServiceRolePolicy",
    "Effect": "Allow",
    "Action": [
     "iam:ListPolicies"
    ],
```

```
    "Resource": "*"
   },
   {
    "Sid": "GetPolicyToInspectServiceRolePolicy",
    "Effect": "Allow",
    "Action": [
     "iam:GetPolicy",
     "iam:GetPolicyVersion"
    ],
    "Resource": "arn:aws:iam::*:policy/*cleanrooms*"
   },
   {
    "Sid": "ConsoleDisplayTables",
    "Effect": "Allow",
    "Action": [
     "glue:GetDatabase",
     "glue:GetDatabases",
     "glue:GetTable",
     "glue:GetTables",
     "glue:GetPartition",
     "glue:GetPartitions",
     "glue:GetSchema",
     "glue:GetSchemaVersion",
     "glue:BatchGetPartition"
    ],
    "Resource": "*"
   },
   {
    "Sid": "EstablishLogDeliveries",
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogDelivery",
     "logs:GetLogDelivery",
     "logs:UpdateLogDelivery",
     "logs:DeleteLogDelivery",
     "logs:ListLogDeliveries"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
```

```
{
 "Sid": "SetupLogGroupsDescribe",
 "Effect": "Allow",
 "Action": [
  "logs:DescribeLogGroups"
 ],
 "Resource": "*",
 "Condition": {
  "ForAnyValue:StringEquals": {
   "aws:CalledVia": "cleanrooms.amazonaws.com"
  }
 }
},
{
 "Sid": "SetupLogGroupsCreate",
 "Effect": "Allow",
 "Action": [
  "logs:CreateLogGroup"
 ],
 "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
 "Condition": {
  "ForAnyValue:StringEquals": {
   "aws:CalledVia": "cleanrooms.amazonaws.com"
  }
 }
},
{
 "Sid": "SetupLogGroupsResourcePolicy",
 "Effect": "Allow",
 "Action": [
   "logs:DescribeResourcePolicies",
  "logs:PutResourcePolicy"
 ],
 "Resource": "*",
 "Condition": {
  "ForAnyValue:StringEquals": {
   "aws:CalledVia": "cleanrooms.amazonaws.com"
  }
 }
},
{
 "Sid": "ConsoleLogSummaryQueryLogs",
 "Effect": "Allow",
 "Action": [
```

```
    "logs:StartQuery"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
   "Sid": "ConsoleLogSummaryObtainLogs",
   "Effect": "Allow",
   "Action": [
    "logs:GetQueryResults"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politique gérée : **AWSCleanRoomsMLReadOnlyAccess**

Vous pouvez vous rattacher `AWSCleanRoomsMLReadOnlyAccess` à vos IAM mandants.

Cette politique accorde des autorisations en lecture seule aux ressources et aux métadonnées dans le cadre d'une `AWSCleanRoomsMLReadOnlyAccess` collaboration.

Cette politique inclut les autorisations suivantes :

- `CleanRoomsConsoleNavigation`— Permet d'accéder aux écrans de la AWS Clean Rooms console.
- `CleanRoomsMLRead`— Permet aux principaux d'accéder en lecture seule au service Clean Rooms ML.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CleanRoomsConsoleNavigation",
            "Effect": "Allow",
            "Action": [
                "cleanrooms:GetCollaboration",
                "cleanrooms:GetConfiguredAudienceModelAssociation",
                "cleanrooms:GetMembership",
                "cleanrooms:ListAnalysisTemplates",
                "cleanrooms:ListCollaborationAnalysisTemplates",
                "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
```

```
                "cleanrooms:ListCollaborations",
                "cleanrooms:ListConfiguredTableAssociations",
                "cleanrooms:ListConfiguredTables",
                "cleanrooms:ListMembers",
                "cleanrooms:ListMemberships",
                "cleanrooms:ListProtectedQueries",
                "cleanrooms:ListSchemas",
                "cleanrooms:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CleanRoomsMLRead",
            "Effect": "Allow",
            "Action": [
                "cleanrooms-ml:Get*",
                "cleanrooms-ml:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politique gérée : **AWSCleanRoomsMLFullAccess**

Vous pouvez vous rattacher `AWSCleanRoomsMLFullAcces` à vos IAM mandants. Cette politique accorde des autorisations administratives qui permettent un accès complet (lecture, écriture et mise à jour) aux ressources et aux métadonnées nécessaires à Clean Rooms ML.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `CleanRoomsMLFullAccess`— Accorde l'accès à toutes les actions de Clean Rooms ML.
- `PassServiceRole`— Accorde l'accès pour transmettre un rôle de service uniquement au service (`PassedToService`condition) dont le nom contient cleanrooms-ml « ».
- `CleanRoomsConsoleNavigation`— Permet d'accéder aux écrans de la AWS Clean Rooms console.
- `CollaborationMembershipCheck`— Lorsque vous lancez une tâche de génération d'audience (segment similaire) dans le cadre d'une collaboration, le service Clean Rooms ML appelle `ListMembers` pour vérifier que la collaboration est valide, que l'appelant est un membre actif et

que le propriétaire du modèle d'audience configuré est un membre actif. Cette autorisation est toujours requise ; la navigation dans la console n'SIDest requise que pour les utilisateurs de la console.

- `AssociateModels`— Permet aux directeurs d'associer un modèle Clean Rooms ML à votre collaboration.
- `TagAssociations`— Permet aux principaux d'ajouter des balises à l'association entre un modèle similaire et une collaboration.
- `ListRolesToPickServiceRole`— Permet aux directeurs de répertorier tous leurs rôles afin de choisir un rôle de service lors de l'utilisation AWS Clean Rooms.
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Permet aux principaux de voir le rôle du service et la politique correspondante dansIAM.
- `ListPoliciesToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dansIAM.
- `GetPolicyToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dansIAM.
- `ConsoleDisplayTables`— Permet aux principaux d'accéder en lecture seule aux AWS Glue métadonnées nécessaires pour afficher les données relatives aux AWS Glue tables sous-jacentes sur la console.
- `ConsolePickOutputBucket`— Permet aux principaux de sélectionner des compartiments Amazon S3 pour les sorties du modèle d'audience configurées.
- `ConsolePickS3Location`— Permet aux principaux de sélectionner l'emplacement dans un compartiment pour les sorties du modèle d'audience configurées.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CleanRoomsMLFullAccess",
            "Effect": "Allow",
            "Action": [
                "cleanrooms-ml:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PassServiceRole",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/cleanrooms-ml*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cleanrooms-ml.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CleanRoomsConsoleNavigation",
            "Effect": "Allow",
            "Action": [
                "cleanrooms:GetCollaboration",
                "cleanrooms:GetConfiguredAudienceModelAssociation",
                "cleanrooms:GetMembership",
                "cleanrooms:ListAnalysisTemplates",
                "cleanrooms:ListCollaborationAnalysisTemplates",
                "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
                "cleanrooms:ListCollaborations",
                "cleanrooms:ListConfiguredTableAssociations",
                "cleanrooms:ListConfiguredTables",
                "cleanrooms:ListMembers",
                "cleanrooms:ListMemberships",
                "cleanrooms:ListProtectedQueries",
                "cleanrooms:ListSchemas",
                "cleanrooms:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CollaborationMembershipCheck",
            "Effect": "Allow",
            "Action": [
                "cleanrooms:ListMembers"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": ["cleanrooms-ml.amazonaws.com"]
```

```
                }
            }
        },
        {
            "Sid": "AssociateModels",
            "Effect": "Allow",
            "Action": [
                "cleanrooms:CreateConfiguredAudienceModelAssociation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAssociations",
            "Effect": "Allow",
            "Action": [
                "cleanrooms:TagResource"
            ],
            "Resource": "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
        },
        {
            "Sid": "ListRolesToPickServiceRole",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GetRoleAndListRolePoliciesToInspectServiceRole",
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:ListRolePolicies",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:role/service-role/cleanrooms-ml*",
                "arn:aws:iam::*:role/role/cleanrooms-ml*"
            ]
        },
        {
            "Sid": "ListPoliciesToInspectServiceRolePolicy",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GetPolicyToInspectServiceRolePolicy",
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicy",
                "iam:GetPolicyVersion"
            ],
            "Resource": "arn:aws:iam::*:policy/*cleanroomsml*"
        },
        {
            "Sid": "ConsoleDisplayTables",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:GetSchema",
                "glue:GetSchemaVersion",
                "glue:BatchGetPartition"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ConsolePickOutputBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ConsolePickS3Location",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
```

```
            ],
            "Resource": "arn:aws:s3:::*cleanrooms-ml*"
        }
    ]
}
```

AWS Clean Rooms mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Clean Rooms 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 RSS fil sur la page Historique du AWS Clean Rooms document.

Modification	Description	Date
AWSCleanRoomsFullAccessNoQuerying – Mise à jour de la politique existante	Ajout de cleanrooms:BatchGetSchemaAnalysisRule à CleanRoomsAccess	13 mai 2024
AWSCleanRoomsFullAccess – Mise à jour de la politique existante	L'ID AWSCleanRoomsFullAccess de déclaration a été mis ConsolePickQueryResultsBucket à jour SetQueryResultsBucket dans cette politique afin de mieux représenter les autorisations, car celles-ci sont nécessaires pour définir le compartiment des résultats des requêtes avec et sans la console.	21 mars 2024
AWSCleanRoomsMLReadOnlyAccess : nouvelle politique AWSCleanRoomsMLFullAccess : nouvelle politique	Ajouté AWSCleanRoomsMLReadOnlyAccess et AWSCleanRoomsMLFullAccess pour prendre en charge le AWS Clean Rooms ML.	29 novembre 2023
AWSCleanRoomsFullAccessNoQuerying – Mise à jour de la politique existante	Ajout de cleanrooms:CreateAnalysisTemplatecleanrooms:GetAnalysisTemplate,cleanrooms:UpdateAnalysisTemplate, cleanrooms	31 juillet 2023

Modification	Description	Date
	:DeleteAnalysisTemplate,cleanrooms:ListAnalysisTemplates,cleanrooms:GetCollaborationAnalysisTemplate,cleanrooms:BatchGetCollaborationAnalysisTemplate, et cleanrooms:ListCollaborationAnalysisTemplates CleanRoomsAccess pour activer la nouvelle fonctionnalité de modèles d'analyse.	
AWSCleanRoomsFullAccessNoQuerying – Mise à jour de la politique existante	Ajoutécleanrooms:ListTagsForResource,cleanrooms:UntagResource, et cleanrooms:TagResource pour CleanRoomsAccess activer le balisage des ressources.	21 mars 2023
AWS Clean Rooms a commencé à suivre les modifications	AWS Clean Rooms a commencé à suivre les modifications apportées AWS à ses politiques gérées.	12 janvier 2023

Résolution des problèmes AWS Clean Rooms 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 AWS Clean Rooms etIAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS Clean Rooms
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Clean Rooms ressources

Je ne suis pas autorisé à effectuer une action dans AWS Clean Rooms

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit lorsque l'`mateojacksonIAM`utilisateur essaie d'utiliser la console pour afficher les détails d'une *`my-example-widget`* ressource fictive mais ne dispose pas des `cleanrooms:`*`GetWidget`* autorisations fictives.

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

Dans ce cas, la stratégie de Mateo doit être mise à jour pour l'autoriser à accéder à la ressource *`my-example-widget`* à l'aide de l'action `cleanrooms:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

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 AWS Clean Rooms.

Certains vous AWS services 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 AWS Clean Rooms. 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 AWS Clean Rooms 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 en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS Clean Rooms en charge, consultezComment AWS Clean Rooms 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 de politiques basées sur les ressources pour l'accès entre comptes, consultez la section En quoi les IAM rôles diffèrent des politiques basées sur les ressources dans le Guide de l'utilisateur. IAM

Prévention du problème de l'adjoint confus entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner un problème de confusion chez les adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés de contexte de condition `aws:SourceArn`globale dans les politiques de ressources afin de limiter les autorisations qui AWSClean Rooms accordent un autre

service à la ressource. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services.

Le moyen le plus efficace de se protéger contre le problème de confusion des adjoints consiste à utiliser la clé de contexte de la condition `aws:SourceArn` globale avec l'intégralité ARN de la ressource. Dans AWSClean Rooms, vous devez également comparer avec la clé de `sts:ExternalId` condition.

La valeur de `aws:SourceArn` doit être définie sur ARN l'appartenance au rôle assumé.

L'exemple suivant montre comment vous pouvez utiliser la clé de contexte de condition `aws:SourceArn` globale AWSClean Rooms pour éviter le problème de confusion des adjoints.

> **Note**
>
> L'exemple de politique s'applique à la politique de confiance du rôle de service AWSClean Rooms utilisé pour accéder aux données des clients.
> La valeur de *membershipID* est votre numéro de AWSClean Rooms membre de la collaboration.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowIfExternalIdMatches",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringLike": {
                    "sts:ExternalId": "arn:aws:*:aws-region:*:dbuser:*/membershipID*"
                }
            }
        },
        {
            "Sid": "AllowIfSourceArnMatches",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "cleanrooms.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ForAnyValue:ArnEquals": {
                    "aws:SourceArn": "arn:aws:cleanrooms:aws-
region:123456789012:membership/membershipID"
                }
            }
        }
    ]
}
```

IAMcomportements pour le AWS Clean Rooms ML

Emplois multi-comptes

Clean Rooms ML permet à une autre personne d'accéder en toute sécurité Compte AWS à certaines ressources créées par l'un sur son compte Compte AWS. Lorsqu'un client de Compte AWS A fait appel `StartAudienceGenerationJob` à une `ConfiguredAudienceModel` ressource appartenant à Compte AWS B, Clean Rooms ML en crée deux ARNs pour la tâche. L'un ARN en Compte AWS A et l'autre en Compte AWS B. Ils ARNs sont identiques sauf pour le leur Compte AWS.

Clean Rooms ML en crée deux ARNs pour les tâches afin que les deux comptes puissent appliquer leurs propres IAM politiques aux tâches. Par exemple, les deux comptes peuvent utiliser le contrôle d'accès basé sur des balises et appliquer les politiques de leur AWS organisation. La tâche traite les données des deux comptes, de sorte que les deux comptes peuvent supprimer la tâche et les données associées. Aucun des deux comptes ne peut empêcher l'autre compte de supprimer la tâche.

Il n'y a qu'une seule exécution de tâche et les deux comptes peuvent voir la tâche lorsqu'ils appellent`ListAudienceGenerationJobs`. Les deux comptes peuvent appeler le `GetDelete`, et `Export` APIs au travail en utilisant le ARN avec leur propre Compte AWS identifiant.

Aucun des deux ne Compte AWS peut accéder à la tâche s'il utilise un identifiant ARN avec l'autre Compte AWS identifiant.

Le nom de la tâche doit être unique au sein d'un Compte AWS. Le nom en Compte AWS B est *`$accountA-$name`*. Le nom choisi par Compte AWS A est préfixé par Compte AWS A lorsque le travail est affiché dans B. Compte AWS

Pour qu'un compte croisé réussisse, Compte AWS B doit autoriser cette action `StartAudienceGenerationJob` à la fois sur la nouvelle tâche en Compte AWS B et sur la nouvelle tâche `ConfiguredAudienceModel` en Compte AWS B en utilisant une politique de ressources similaire à l'exemple suivant :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Clean-Rooms-<CAMA ID>",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "accountA"
                ]
            },
            "Action": [
                "cleanrooms-ml:StartAudienceGenerationJob"
            ],
            "Resource": [
                "arn:aws:cleanrooms-ml:us-west-1:AccountB:configured-audience-
model/id",
                "arn:aws:cleanrooms-ml:us-west-1:AccountB:audience-generation-job/*"
            ],
            // optional - always set by AWS Clean Rooms
"Condition":{"StringEquals":{"cleanrooms-ml:CollaborationId":"UUID"}}
        }
    ]
}
```

Si vous utilisez le AWS Clean Rooms ML API pour créer un modèle similaire configuré avec `manageResourcePolicies` défini sur true, AWS Clean Rooms crée cette politique pour vous.

De plus, la politique d'identité de l'appelant dans Compte AWS A doit être `StartAudienceGenerationJob` autorisée. `arn:aws:cleanrooms-ml:us-west-1:AccountA:audience-generation-job/*` Il existe donc trois IAM ressources d'action `StartAudienceGenerationJob` : la tâche Compte AWS A, la tâche Compte AWS B et la tâche Compte AWS B. `ConfiguredAudienceModel`

> **Warning**
>
> La Compte AWS personne qui a démarré la tâche reçoit un événement du journal AWS CloudTrail d'audit concernant la tâche. Le Compte AWS propriétaire du `ConfiguredAudienceModel` ne reçoit aucun événement du journal d' AWS CloudTrail audit.

Tâches de balisage

Lorsque vous définissez le `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` paramètre de`CreateConfiguredAudienceModel`, toutes les tâches de génération de segments similaires de votre compte créées à partir de ce modèle de similarité configuré comportent par défaut les mêmes balises que le modèle de similarité configuré. Le modèle de similarité configuré est le parent et la tâche de génération de segments de similarité est l'enfant.

Si vous créez une tâche dans votre propre compte, les balises de requête de la tâche remplacent les balises parentes. Les offres d'emploi créées par d'autres comptes ne créent jamais de tags dans votre compte. Si vous définissez une tâche `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` et qu'un autre compte la crée, il existe deux copies de la tâche. La copie de votre compte contient les balises de ressource parent et la copie du compte de l'auteur de la tâche contient les balises de la demande.

Validation des collaborateurs

Lorsque vous accordez des autorisations à d'autres membres d'une AWS Clean Rooms collaboration, la politique de ressources doit inclure la clé de condition`cleanrooms-ml:CollaborationId`. Cela garantit que le `collaborationId` paramètre est inclus dans la StartAudienceGenerationJobdemande. Lorsque le `collaborationId` paramètre est inclus dans la demande, Clean Rooms ML confirme que la collaboration existe, que l'auteur de la tâche est un membre actif de la collaboration et que le propriétaire du modèle similaire configuré est un membre actif de la collaboration.

Lorsque AWS Clean Rooms vous gérez la politique de ressources de votre modèle similaire configurée (le `manageResourcePolicies` paramètre est `TRUE` dans la CreateConfiguredAudienceModelAssociation demande), cette clé de condition sera définie dans la politique de ressources. Par conséquent, vous devez spécifier le `collaborationId` in StartAudienceGenerationJob.

Accès intercomptes

Ne `StartAudienceGenerationJob` peut être appelé que sur plusieurs comptes. Tous les autres Clean Rooms ML ne APIs peuvent être utilisés qu'avec les ressources de votre propre compte. Cela garantit la confidentialité de vos données d'entraînement, de la configuration de votre modèle similaire et d'autres informations.

Clean Rooms ML ne révèle jamais Amazon S3 ni les AWS Glue emplacements d'un compte à l'autre. L'emplacement des données de formation, l'emplacement de sortie du modèle similaire configuré et l'emplacement de départ des tâches pour la génération de segments similaires ne sont jamais visibles sur tous les comptes. À moins que la journalisation des requêtes ne soit activée dans la collaboration, les données initiales ne sont pas visibles sur tous les comptes, que les données initiales proviennent d'une SQL requête ou que la requête elle-même soit activée. Si vous avez `Get` une tâche de génération d'audience soumise par un autre compte, le service n'indique pas l'emplacement initial.

Validation de conformité pour AWS Clean Rooms

Pour savoir si un programme AWS services de conformité AWS service s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez AWS services 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 AWS services 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 AWS services 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 AWS services 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 AWS service 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 AWS service 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 AWS service 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.

Résilience dans AWS Clean Rooms

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. 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 AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Sécurité de l'infrastructure dans AWS Clean Rooms

En tant que service géré, AWS Clean Rooms il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez API les appels AWS publiés pour accéder AWS Clean Rooms via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Sécurité du réseau

Lors des AWS Clean Rooms lectures depuis votre compartiment S3 pendant l'exécution d'une requête, le trafic entre Amazon S3 AWS Clean Rooms et Amazon S3 est acheminé de manière sécurisée via le réseau AWS privé. Le trafic en vol est signé à l'aide du protocole Amazon Signature Version 4 (SIGv4) et crypté à l'aide HTTPS de. Ce trafic est autorisé en fonction du rôle de IAM service que vous avez défini pour votre table configurée.

Vous pouvez vous connecter par programmation AWS Clean Rooms via un point de terminaison. Pour obtenir la liste des points de terminaison de service, consultez la section AWS Clean Rooms Points de terminaison et quotas dans le. Références générales AWS

Tous les points de terminaison de service sont uniquement disponiblesHTTPS. Vous pouvez utiliser les points de terminaison Amazon Virtual Private Cloud (VPC) au cas où vous souhaiteriez vous connecter AWS Clean Rooms depuis votre connexion Internet VPC et si vous ne souhaitez pas disposer d'une connexion Internet. Pour plus d'informations, consultez la section Accès aux AWS services AWS PrivateLink dans le AWS PrivateLink Guide.

Vous pouvez attribuer IAM des IAM politiques à vos principaux qui utilisent les clés de SourceVpce contexte aws : pour empêcher votre IAM principal de ne pouvoir passer des appels que AWS Clean Rooms via un VPC point de terminaison et non via Internet.

Accès AWS Clean Rooms ou AWS Clean Rooms ML à l'aide d'un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez l'utiliser AWS PrivateLink pour créer une connexion privée entre votre cloud privé virtuel (VPC) AWS Clean Rooms et/ou AWS Clean Rooms ML. Vous pouvez accéder au AWS Clean Rooms AWS Clean Rooms ML comme s'il se trouvait dans votre VPC ordinateur, sans utiliser de passerelle Internet, d'NATappareil, de VPN connexion ou de AWS Direct Connect connexion. Les instances de votre VPC ordinateur n'ont pas besoin d'adresses IP publiques pour y accéder AWS Clean Rooms.

Vous établissez cette connexion privée en créant un point de terminaison d'interface optimisé par AWS PrivateLink. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Il s'agit d'interfaces réseau gérées par le demandeur qui servent de point d'entrée pour le trafic destiné à AWS Clean Rooms.

Pour plus d'informations, consultez Accès aux AWS services via AWS PrivateLink dans le Guide AWS PrivateLink .

Considérations relatives à AWS Clean Rooms

Avant de configurer un point de terminaison d'interface pour AWS Clean Rooms, consultez les considérations du AWS PrivateLink guide.

AWS Clean Rooms et le AWS Clean Rooms ML prennent en charge l'envoi d'appels à toutes leurs API actions via le point de terminaison de l'interface.

VPCLes politiques de point de terminaison ne sont pas prises en charge pour AWS Clean Rooms ou AWS Clean Rooms ML. Par défaut, l'accès complet à AWS Clean Rooms et AWS Clean Rooms ML est autorisé via le point de terminaison de l'interface. Vous pouvez également associer un groupe de sécurité aux interfaces réseau du point de terminaison afin de contrôler le trafic vers AWS Clean Rooms ou le AWS Clean Rooms ML via le point de terminaison de l'interface.

Créez un point de terminaison d'interface pour AWS Clean Rooms

Vous pouvez créer un point de terminaison d'interface pour AWS Clean Rooms ou AWS Clean Rooms ML à l'aide de la VPC console Amazon ou du AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide AWS PrivateLink .

Créez un point de terminaison d'interface pour AWS Clean Rooms utiliser le nom de service suivant.

```
com.amazonaws.region.cleanrooms
```

Créez un point de terminaison d'interface pour AWS Clean Rooms ML en utilisant le nom de service suivant.

```
com.amazonaws.region.cleanrooms-ml
```

Si vous activez le mode privé DNS pour le point de terminaison de l'interface, vous pouvez API envoyer des demandes AWS Clean Rooms en utilisant son DNS nom régional par défaut. Par exemple, `cleanrooms-ml.us-east-1.amazonaws.com`.

Surveillance AWS Clean Rooms

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS Clean Rooms et des performances de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller AWS Clean Rooms, signaler tout problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos fichiers journaux à partir d'instances Amazon EC2 et d'autres sources. AWS CloudTrail Amazon CloudWatch Logs peut surveiller les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.

  Clean Rooms ML autorise les tâches entre comptes pour certaines actions d'API. La personne Compte AWS qui a démarré la tâche reçoit l'événement du journal AWS CloudTrail d'audit correspondant à la tâche. Pour plus d'informations, consultez IAMcomportements pour le AWS Clean Rooms ML.
- 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.

Journalisation des appels d'API AWS Clean Rooms avec AWS CloudTrail

AWS Clean Roomsest intégré àAWS CloudTrail, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou unAWS service dansAWS Clean Rooms. CloudTrail capture les appels d'API vers enAWS Clean Rooms tant qu'événements. Les appels capturés incluent des appels de la console AWS Clean Rooms et les appels de code vers les opérations d'API AWS Clean Rooms. Si vous créez un journal d'activité, vous pouvez activer la livraison continue d' CloudTrailévénements à un compartiment Amazon S3, y compris des événements pourAWS Clean Rooms. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la CloudTrail console dans Historique des événements. Les informations collectées par

CloudTrail, vous permettent de déterminer quelle demande a été envoyée àAWS Clean Rooms, l'adresse IP source à partir de laquelle la demande a été effectuée, qui a effectué la demande, quand, ainsi que d'autres informations.

Pour en savoir plus CloudTrail, consultez le Guide deAWS CloudTrail l'utilisateur.

AWS Clean Roomsinformations dans CloudTrail

CloudTrail est activé dans votreCompte AWS lors de la création de ce dernier. Lorsqu'une activité a lieu dansAWS Clean Rooms, cette activité est enregistrée dans un CloudTrail événement avec d'autresAWS service événements dans Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements dans votre Compte AWS, y compris les événements pour AWS Clean Rooms, créez un journal d'activité. Un journal CloudTrail de suivi permet de livrer des fichiers journaux dans 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 d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. En outre, vous pouvez configurer d'autresAWS services pour analyser plus en profondeur les données d'événement collectées dans les CloudTrail journaux et agir sur celles-ci. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs Régions
- Réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes lesAWS Clean Rooms actions sont enregistrées CloudTrail et documentées dans la référence deAWS Clean Rooms l'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 :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur 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 requête a été effectuée par un autre AWS service.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Présentation des AWS Clean Rooms entrées des fichiers journaux

Un journal de suivi est une configuration qui permet la remise d'événements sous forme de fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux peuvent contenir une ou plusieurs entrées de journal. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend 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 de pile ordonnée des appels d'API publics. Ils ne suivent aucun ordre précis.

Exemples d'AWS Clean Rooms CloudTrail événements

Les exemples suivants illustrent CloudTrail des événements pour :

Rubriques

- StartProtectedQuery (réussite)
- StartProtectedQuery(échec)

StartProtectedQuery (réussite)

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE_PRINCIPAL_ID",
        "arn": "arn:aws:sts::123456789012:assumed-role/query-runner/jdoe",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "EXAMPLE_PRINCIPAL_ID",
                "arn": "arn:aws:iam::123456789012:role/query-runner",
                "accountId": "123456789012",
                "userName": "query-runner"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-07T19:34:32Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-07T19:53:32Z",
    "eventSource": "cleanrooms.amazonaws.com",
    "eventName": "StartProtectedQuery",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "203.0.113.1",
    "userAgent": "aws-internal/3",
    "requestParameters": {
        "resultConfiguration": {
            "outputConfiguration": {
                "s3": {
                    "resultFormat": "CSV",
                    "bucket": "cleanrooms-queryresults-jdoe-test",
                    "keyPrefix": "test"
                }
            }
        },
        "sqlParameters": "***",
        "membershipIdentifier": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "type": "SQL"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "protectedQuery": {
            "createTime": 1680897212.279,
            "id": "f5988bf1-771a-4141-82a8-26fcc4e41c9f",
            "membershipArn": "arn:aws:cleanrooms:us-east-2:123456789012:membership/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "membershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "resultConfiguration": {
                "outputConfiguration": {
```

```
                    "s3": {
                        "bucket": "cleanrooms-queryresults-jdoe-test",
                        "keyPrefix": "test",
                        "resultFormat": "CSV"
                    }
                }
            },
            "sqlParameters": "***",
            "status": "SUBMITTED"
        }
    },
    "requestID": "7464211b-2277-4b55-9723-fb4f259aefd2",
    "eventID": "f7610f5e-74b9-420f-ae43-206571ebcbf7",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

StartProtectedQuery(échec)

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE_PRINCIPAL_ID",
        "arn": "arn:aws:sts::123456789012:assumed-role/query-runner/jdoe",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE_PRINCIPAL_ID",
                "arn": "arn:aws:iam::123456789012:role/query-runner",
                "accountId": "123456789012",
                "userName": "query-runner"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-07T19:34:32Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2023-04-07T19:47:27Z",
    "eventSource": "cleanrooms.amazonaws.com",
    "eventName": "StartProtectedQuery",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "203.0.113.1",
    "userAgent": "aws-internal/3",
    "errorCode": "ValidationException",
    "requestParameters": {
        "resultConfiguration": {
            "outputConfiguration": {
                "s3": {
                    "resultFormat": "CSV",
                    "bucket": "cleanrooms-queryresults-jdoe-test",
                    "keyPrefix": "test"
                }
            }
        },
        "sqlParameters": "***",
        "membershipIdentifier": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "type": "SQL"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "message": "Column(s) [identifier] is not allowed in select"
    },
    "requestID": "e29f9f74-8299-4a83-9d18-5ddce7302f07",
    "eventID": "c8ee3498-8e4e-44b5-87e4-ab9477e56eb5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Création de AWS Clean Rooms ressources avec AWS CloudFormation

AWS Clean Rooms est intégré à AWS CloudFormation un service qui vous aide à modéliser et à configurer vos AWS ressources. Grâce à cette intégration, vous pouvez 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, et qui AWS CloudFormation fournit et configure ces ressources pour vous. Les exemples de ressources incluent les collaborations, les tables configurées, les associations de tables configurées et les adhésions.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos AWS Clean Rooms ressources de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis fournissez les mêmes ressources à plusieurs reprises Comptes AWS et Régions AWS.

AWS Clean Rooms et AWS CloudFormation modèles

Pour fournir et configurer des ressources AWS Clean Rooms et des services associés, vous devez comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous n'êtes pas familiarisé avec JSON ou YAML, 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.

AWS Clean Rooms prend en charge la création de collaborations, de tables configurées, d'associations de tables configurées et d'adhésions à AWS CloudFormation. Pour plus d'informations, notamment des exemples de modèles JSON et YAML pour les collaborations, les tables configurées, les associations de tables configurées et les adhésions, consultez la référence aux types de AWS Clean Rooms ressources dans le guide de l'AWS CloudFormation utilisateur.

Les modèles suivants sont disponibles :

- Modèle d'analyse

  Spécifiez un modèle d' AWS Clean Rooms analyse, y compris un nom, une description, un format, une source, des paramètres et des balises.

  Pour plus d'informations, consultez les rubriques suivantes :

AWS::CleanRooms::AnalysisTemplate dans le guide de l'utilisateur AWS Clean Rooms

CreateAnalysisTemplate dans la Référence d'API AWS Clean Rooms

- Collaboration

  Spécifiez une AWS Clean Rooms collaboration, y compris un nom, une description, un type, des paramètres et des balises.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::CleanRooms::Collaboration dans le guide de l'utilisateur AWS CloudFormation

  CreateCollaboration dans la Référence d'API AWS Clean Rooms

- Table configurée

  Spécifiez une table configurée dans AWS Clean Rooms, y compris les colonnes autorisées, la méthode d'analyse, la description, le nom, la référence de la table, le budget de confidentialité et les balises. Les tables configurées représentent une référence à une table existante dans le AWS Glue Data Catalog qui a été configurée pour être utilisée dans AWS Clean Rooms. Une table configurée contient une règle d'analyse qui détermine la manière dont les données peuvent être utilisées.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::CleanRooms::ConfiguredTable dans le guide de l'utilisateur AWS CloudFormation

  CreateConfiguredTable dans la Référence d'API AWS Clean Rooms

- Association de tables configurée

  Spécifiez une association de table configurée dans AWS Clean Rooms, y compris l'ID, la description, l'ID de membre, le nom, le rôle, le nom de ressource Amazon (ARN) et les balises. Une association de tables configurée lie une table configurée à une collaboration.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::CleanRooms::ConfiguredTableAssociation dans le guide de l'utilisateur AWS CloudFormation

  CreateConfiguredTableAssociation dans la Référence d'API AWS Clean Rooms

- Adhésion

  Spécifiez l'adhésion à un identifiant de collaboration spécifique et rejoignez la collaboration dans AWS Clean Rooms.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::CleanRooms::Membership dans le guide de l'utilisateur AWS CloudFormation

  CreateMembership dans la Référence d'API AWS Clean Rooms
- Modèle de budget de confidentialité

  Spécifiez un modèle de budget de AWS Clean Rooms confidentialité, y compris un budget de confidentialité, le bruit ajouté par requête et une actualisation mensuelle du budget de confidentialité.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::CleanRooms::PrivacyBudgetTemplate dans le guide de l'utilisateur AWS CloudFormation

  CreatePrivacyBudgetTemplate dans la Référence d'API AWS Clean Rooms
- Créer un ensemble de données de formation

  Spécifiez un jeu de données d'entraînement pour un modèle Clean Rooms ML à partir d'un AWS Glue tableau.

  Pour plus d'informations, consultez les rubriques suivantes :

  AWS::CleanRoomsML::TrainingDataset dans le guide de l'utilisateur AWS CloudFormation

  CreateTrainingDatasetdans la référence de l'API Clean Rooms ML

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 API Reference

- Guide de l’utilisateur de l’interface de ligne de commande AWS CloudFormation

Quotas pour AWS Clean Rooms

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux AWS service. Sauf indication contraire, chaque quota est spécifique à un Région AWS. Vous pouvez demander des augmentations pour certains quotas, tandis que d'autres quotas ne peuvent pas être augmentés.

Pour consulter les quotas pour AWS Clean Rooms, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez AWSservices, puis sélectionnez AWS Clean Rooms.

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 Quotas de service, utilisez le formulaire d'augmentation des limites de service.

Vous Compte AWS disposez des quotas suivants relatifs à AWS Clean Rooms.

Ressource	Par défaut	Description
Membres invités par collaboration	5	Nombre maximum de membres invités par collaboration
Abonnements par compte	100	Nombre maximum d'adhésions pour un compte
Collaborations créées par compte	10	Nombre maximum de collaborations créées par compte
Tables configurées par compte	60	Nombre maximum de tables configurées pouvant être créées par un compte
Table des associations par membre	25	Nombre maximum de tables associées par membre actif
Demandes continues simultanées par membre	5	Nombre maximum de requêtes en cours simultanées par membre

Ressource	Par défaut	Description
Colonnes par liste d'autorisation de table configurée	100	Nombre maximum de colonnes pouvant être autorisées par table configurée
Tables configurées par requête protégée	15	Nombre maximal de tables configurées dans une requête protégée
Modèles d'analyse par membre	25	Nombre maximum de modèles d'analyse par membre
Modèle de similarité configuré (modèle d'audience) associations par membre	5	Nombre maximum d'associations de modèles similaires configurées par membre.
Associations d'espaces de noms d'ID par membre	10	Nombre maximum d'associations d'espaces de noms d'identification par membre.
Tables de mappage d'identifiants	5	Nombre maximum de tables de mappage d'identifiants par membre.

Limites des paramètres de ressources

Ressource	Par défaut	Description
Taille de la règle d'analyse	100 Ko	Taille maximale de JSON pour une règle d'analyse
Longueur du texte de la requête	90 Ko (8 Ko pour les requêtes de confidentialité différentielles)	Longueur de texte maximale pour une instruction de SQL requête
Durée d'exécution de la requête	12 heures	Durée maximale pendant laquelle une requête est

Ressource	Par défaut	Description
		exécutée avant l'expiration du délai
Taille de sortie du fichier de données de requête	6,2 GO	Taille maximale d'un fichier de sortie d'une requête protégée

Vous Compte AWS avez les quotas de API transaction suivants par seconde (TPS) par compte et par point de terminaison.

Limitations d'API

Ressource	Limite de débit	Description
Taux de `BatchGetCollaborationAnalysisTemplate` demandes	5 TPS	Nombre maximum d'`BatchGetCollaborationAnalysisTemplate` APIappels par seconde
Taux de `BatchGetSchema` demandes	5 TPS	Nombre maximum d'`BatchGetSchema` APIappels par seconde
Taux de `CreateAnalysisTemplate` demandes	5 TPS	Nombre maximum d'`CreateAnalysisTemplate` APIappels par seconde
Taux de `CreateCollaboration` demandes	5 TPS	Nombre maximum d'`CreateCollaboration` APIappels par seconde
Taux de `CreateConfiguredAudienceModelAssociation` demandes	5 TPS	Nombre maximal d'appels `CreateConfiguredAudienceModelAssociation` par seconde

Ressource	Limite de débit	Description
Taux de CreateConfiguredTable demandes	5 TPS	Nombre maximal d'appels CreateConfiguredTable par seconde
Taux de CreateConfiguredTableAnalysisRule demandes	5 TPS	Nombre maximal d'appels CreateConfiguredTableAnalysisRule par seconde
Taux de CreateConfiguredTableAssociation demandes	5 TPS	Nombre maximal d'appels CreateConfiguredTableAssociation par seconde
Taux de CreateMembership demandes	5 TPS	Nombre maximal d'appels CreateMembership par seconde
Taux de CreatePrivacyBudgetTempate demandes	5 TPS	Nombre maximal d'appels CreatePrivacyBudgetTemplate par seconde
Taux de DeleteAnalysisTemplate demandes	5 TPS	Nombre maximal d'appels DeleteAnalysisTemplate par seconde
Taux de DeleteCollaboration demandes	5 TPS	Nombre maximal d'appels DeleteCollaboration par seconde
Taux de DeleteConfiguredAudienceModelAssociation demandes	5 TPS	Nombre maximal d'appels DeleteConfiguredAudienceModelAssociation par seconde

Ressource	Limite de débit	Description
Taux de DeleteConfiguredTable demandes	5 TPS	Nombre maximal d'appels DeleteConfiguredTable par seconde
Taux de DeleteConfiguredTableAnalysisRule demandes	5 TPS	Nombre maximal d'appels DeleteConfiguredTableAnalysisRule par seconde
Taux de DeleteConfiguredTableAssociation demandes	5 TPS	Nombre maximal d'appels DeleteConfiguredTableAssociation par seconde
Taux de DeleteMember demandes	5 TPS	Nombre maximal d'appels DeleteMember par seconde
Taux de DeleteMembership demandes	5 TPS	Nombre maximal d'appels DeleteMembership par seconde
Taux de DeletePrivacyBudgetTemplate demandes	5 TPS	Nombre maximal d'appels DeletePrivacyBudgetTemplate par seconde
Taux de GetAnalysisTemplate demandes	5 TPS	Nombre maximal d'appels GetAnalysisTemplate par seconde
Taux de GetCollaboration demandes	5 TPS	Nombre maximal d'appels GetCollaboration par seconde

Ressource	Limite de débit	Description
Taux de `GetCollaborationConfiguredAudienceModelAssociation` demandes	5 TPS	Nombre maximal d'appels `GetCollaborationConfiguredAudienceModelAssociation` par seconde
Taux de `GetCollaborationPrivacyBudgetTemplate` demandes	5 TPS	Nombre maximal d'appels `GetCollaborationPrivacyBudgetTemplate` par seconde
Taux de `GetConfiguredAudienceModelAssociation` demandes	5 TPS	Nombre maximal d'appels `GetConfiguredAudienceModelAssociation` par seconde
Taux de `GetConfiguredTable` demandes	5 TPS	Nombre maximal d'appels `GetConfiguredTable` par seconde
Taux de `GetConfiguredTableAnalysisRule` demandes	5 TPS	Nombre maximal d'appels `GetConfiguredTableAnalysisRule` par seconde
Taux de `GetConfiguredTableAssociation` demandes	20 TPS	Nombre maximal d'appels `GetConfiguredTableAssociation` par seconde
Taux de `GetMembership` demandes	5 TPS	Nombre maximal d'appels `GetMembership` par seconde
Taux de `GetPrivacyBudgetTemplate` demandes	5 TPS	Nombre maximal d'appels `GetPrivacyBudgetTemplate` par seconde

Ressource	Limite de débit	Description
Taux de `GetProtectedQuery` demandes	20 TPS	Nombre maximal d'appels `GetProtectedQuery` par seconde
Taux de `GetSchema` demandes	5 TPS	Nombre maximal d'appels `GetSchema` par seconde
Taux de `GetSchemaAnalysisRule` demandes	5 TPS	Nombre maximal d'appels `GetSchemaAnalysisRule` par seconde
Taux de `ListAnalysisTemplates` demandes	5 TPS	Nombre maximal d'appels `ListAnalysisTemplates` par seconde
Taux de `ListCollaborationConfiguredAudienceModelAssociations` demandes	5 TPS	Nombre maximal d'appels `ListCollaborationConfiguredAudienceModelAssociations` par seconde
Taux de `ListCollaborationPrivacyBudgets` demandes	5 TPS	Nombre maximal d'appels `ListCollaborationPrivacyBudgets` par seconde
Taux de `ListCollaborationPrivacyBudgetTemplates` demandes	5 TPS	Nombre maximal d'appels `ListCollaborationPrivacyBudgetTemplates` par seconde
Taux de `ListCollaborations` demandes	5 TPS	Nombre maximal d'appels `ListCollaborations` par seconde

Ressource	Limite de débit	Description
Taux de `ListConfiguredAudienceModelAssociations` demandes	5 TPS	Nombre maximal d'appels `ListConfiguredAudienceModelAssociations` par seconde
Taux de `ListConfiguredTableAssociations` demandes	5 TPS	Nombre maximal d'appels `ListConfiguredTableAssociations` par seconde
Taux de `ListConfiguredTables` demandes	5 TPS	Nombre maximal d'appels `ListConfiguredTables` par seconde
Taux de `ListMembers` demandes	5 TPS	Nombre maximal d'appels `ListMembers` par seconde
Taux de `ListMemberships` demandes	5 TPS	Nombre maximal d'appels `ListMemberships` par seconde
Taux de `ListPrivacyBudgets` demandes	5 TPS	Nombre maximal d'appels `ListPrivacyBudgets` par seconde
Taux de `ListPrivacyBudgetTemplates` demandes	5 TPS	Nombre maximal d'appels `ListPrivacyBudgetTemplates` par seconde
Taux de `ListProtectedQueries` demandes	5 TPS	Nombre maximal d'appels `ListProtectedQueries` par seconde
Taux de `ListSchemas` demandes	5 TPS	Nombre maximal d'appels `ListSchemas` par seconde

Ressource	Limite de débit	Description
Taux de `StartProtectedQuery` demandes	5 TPS	Nombre maximal d'appels `StartProtectedQuery` par seconde
Taux de `UpdateAnalysisTemplate` demandes	5 TPS	Nombre maximal d'appels `UpdateAnalysisTemplate` par seconde
Taux de `UpdateCollaboration` demandes	5 TPS	Nombre maximal d'appels `UpdateCollaboration` par seconde
Taux de `UpdateConfiguredAudienceModelAssociation` demandes	5 TPS	Nombre maximal d'appels `UpdateConfiguredAudienceModelAssociation` par seconde
Taux de `UpdateConfiguredTable` demandes	5 TPS	Nombre maximal d'appels `UpdateConfiguredTable` par seconde
Taux de `UpdateConfiguredTableAnalysisRule` demandes	5 TPS	Nombre maximal d'appels `UpdateConfiguredTableAnalysisRule` par seconde
Taux de `UpdateConfiguredTableAssociation` demandes	5 TPS	Nombre maximal d'appels `UpdateConfiguredTableAssociation` par seconde
Taux de `UpdatePrivacyBudgetTemplate` demandes	5 TPS	Nombre maximal d'appels `UpdatePrivacyBudgetTemplate` par seconde

AWS Clean Rooms Quotas API de limitation du ML

Ressource	Limite de débit	Description
Taux de `CreateAudienceModel` demandes	1 TPS taux, 3 TPS rafales	Nombre maximum d'`CreateAudienceModel` APIappels par seconde
Taux de `CreateConfiguredAudienceModel` demandes	10 TPS	Nombre maximum d'`CreateConfiguredAudienceModel` APIappels par seconde
Taux de `CreateTrainingDataset` demandes	10 TPS	Nombre maximum d'`CreateTrainingDataset` APIappels par seconde
Taux de `DeleteAudienceGenerationJob` demandes	2 TPS taux, 10 TPS rafales	Nombre maximum d'`DeleteAudienceGenerationJob` APIappels par seconde
Taux de `DeleteAudienceModel` demandes	2 TPS taux, 10 TPS rafales	Nombre maximum d'`DeleteAudienceModel` APIappels par seconde
Taux de `DeleteConfiguredAudienceModel` demandes	10 TPS	Nombre maximum d'`DeleteConfiguredAudienceModel` APIappels par seconde
Taux de `DeleteConfiguredAudienceModelPolicy` demandes	25 TPS	Nombre maximum d'`DeleteConfiguredAudienceModelPolicy` APIappels par seconde

Ressource	Limite de débit	Description
Taux de `DeleteTrainingDataset` demandes	10 TPS	Nombre maximum d'`DeleteTrainingDataset` APIappels par seconde
Taux de `GetAudienceGenerationJob` demandes	50 TPS	Nombre maximum d'`GetAudienceGenerationJob` APIappels par seconde
Taux de `GetAudienceModel` demandes	50 TPS	Nombre maximum d'`GetAudienceModel` APIappels par seconde
Taux de `GetConfiguredAudienceModel` demandes	50 TPS	Nombre maximum d'`GetConfiguredAudienceModel` APIappels par seconde
Taux de `GetConfiguredAudienceModelPolicy` demandes	50 TPS	Nombre maximum d'`GetConfiguredAudienceModelPolicy` APIappels par seconde
Taux de `GetTrainingDataset` demandes	50 TPS	Nombre maximum d'`GetTrainingDataset` APIappels par seconde
Taux de `ListAudienceExportJobs` demandes	50 TPS	Nombre maximum d'`ListAudienceExportJobs` APIappels par seconde

Ressource	Limite de débit	Description
Taux de `ListAudienceGenerationJobs` demandes	50 TPS	Nombre maximum d'`ListAudienceGenerationJobs` APIappels par seconde
Taux de `ListAudienceModels` demandes	50 TPS	Nombre maximum d'`ListAudienceModels` APIappels par seconde
Taux de `ListConfiguredAudienceModels` demandes	50 TPS	Nombre maximum d'`ListConfiguredAudienceModels` APIappels par seconde
Taux de `ListTagsForResource` demandes	50 TPS	Nombre maximum d'`ListTagsForResource` APIappels par seconde
Taux de `ListTrainingDatasets` demandes	50 TPS	Nombre maximum d'`ListTrainingDatasets` APIappels par seconde
Taux de `PutConfiguredAudienceModelPolicy` demandes	25 TPS	Nombre maximum d'`PutConfiguredAudienceModelPolicy` APIappels par seconde
Taux de `StartAudienceExportJob` demandes	1 TPS taux, 3 TPS rafales	Nombre maximum d'`StartAudienceExportJob` APIappels par seconde
Taux de `StartAudienceGenerationJob` demandes	1 TPS taux, 5 TPS rafales	Nombre maximum d'`StartAudienceGenerationJob` APIappels par seconde

Ressource	Limite de débit	Description
Taux de `TagResource` demandes	10 TPS	Nombre maximum d'`TagResource` APIappels par seconde
Taux de `UntagResource` demandes	50 TPS	Nombre maximum d'`UntagResource` APIappels par seconde
Taux de `UpdateConfiguredAudienceModel` demandes	10 TPS	Nombre maximum d'`UpdateConfiguredAudienceModel` APIappels par seconde

Nom	Par défaut	Ajusta	Description
Nombre d'emplois d'exportation d'audience actif par travail de génération d'audience	Chaque région prise en charge : 25	Non	Le nombre maximum de tâches d'exportation d'audience actives pour une tâche de génération d'audience
Tâches d'exportation d'audience en attente ou en cours par client	Chaque Région prise en charge : 20	Non	Le nombre maximum de tâches d'exportation d'audience en attente ou en cours par client
Tâches de génération d'audience en attente ou en cours par client	Par région prise en charge : 10	Oui	Le nombre maximum de tâches de génération d'audience en attente ou en cours par client
Modèles d'audience en attente ou en cours par client	Chaque région prise en charge : 2	Oui	Le nombre maximum de tâches de formation sur les modèles d'audience

Nom	Par défaut	Ajusta	Description
			en attente ou en cours par client

Quotas ML pour Clean Rooms

Ressource	Par défaut	Description
Ensembles de données	par tâche	
Nombre maximum d'interac tions	20 milliards	Nombre maximum d'interac tions autorisées dans les données d'entraînement. Les entrées plus importantes sont échantillonnées vers le bas.
Nombre minimal d'interactions	1 million	
Nombre maximum d'utilisa teurs distincts pour la formation sur les modèles similaires	1 million	Si d'autres sont inclus, seuls les 100 millions les plus populaires sont utilisés, classés en fonction du nombre d'interactions.
Nombre minimal d'utilisateurs distincts pour la formation sur les modèles similaires	100 000	
Nombre minimum d'utilisa teurs pour la tâche d'exporta tion portant sur un segment similaire (public)	10 000	
Nombre maximum d'éléments distincts utilisés pour l'entraîn ement des modèles.	1 million	Vous pouvez inclure jusqu'à 50 millions d'articles, mais seul le million le plus populaire est utilisé.

Ressource	Par défaut	Description
Nombre maximal de colonnes d'entités dans le jeu de données d'entraînement.	10	
Nombre minimum d'éléments distincts par utilisateur	2	AWS Clean Rooms Le ML nécessite que chaque ligne ou utilisateur possède au moins deux éléments, y compris des éléments répétés.
Taille maximale de l'audience initiale	500 000	
Taille minimale de l'audience initiale	500	Le fournisseur de données de formation peut définir cette valeur à une valeur aussi basse que 25.
APIs	par client	
Nombre total de jeux de données d'entraînement actifs	500	
Nombre total de modèles similaires actifs (modèles d'audience)	500	
Nombre total de modèles similaires configurés actifs (modèles d'audience)	10 000	
Nombre total de jobs de génération de segments similaires (audience) terminés	Aucune limite	

Ressource	Par défaut	Description
Nombre total de jobs terminés dans un segment similaire à l'exportation (public)	Aucune limite	
Durée maximale d'une tâche de génération de modèle similaire (modèle d'audience)	1 jour (24 heures)	
Durée maximale d'une tâche de génération de segments similaires (audience)	10 heures	Une fois que vous avez fourni une graine, Clean Rooms ML met au maximum 10 heures pour générer un segment similaire. Si vous utilisez une SQL requête comme donnée de départ, l'exécution de la requête peut prendre jusqu'à 12 heures, en plus des 10 heures nécessaires pour générer le segment similaire.
Pourcentage minimum pour une classe de taille de segment (audience)	1 %	
Pourcentage maximal pour un groupe de taille de segment (audience)	20 %	
Taille absolue minimale pour un compartiment de taille de segment (audience)	1 % du nombre d'utilisateurs distincts	
Taille absolue maximale pour un compartiment de taille de segment (audience)	20 % du nombre d'utilisateurs distincts	

Historique du document pour le guide de AWS Clean Rooms l'utilisateur

Le tableau suivant décrit les versions de documentation pour AWS Clean Rooms.

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
Protection de la confidentialité améliorée, création d'audiences similaires, choix de plusieurs destinataires de résultats	Vous pouvez protéger vos données tout en autorisant les requêtes d'activation complexes à l'aide d'analyses supplémentaires et de la règle d'analyse de collaboration. Vous pouvez créer des modèles d'audience similaires à partir de SQL requêtes ou de modèles d'analyse. Vous pouvez sélectionner plusieurs membres pour recevoir les résultats.	24 juillet 2024
Résolution de l'entité en AWS Clean Rooms	Avec Résolution des entités AWS in AWS Clean Rooms, vous pouvez créer une table de mappage d'identifiants entre deux espaces de noms d'identification pour interroger les données d'événements dans des espaces d'identité disparates.	23 juillet 2024

Mise à jour de la politique existante	La nouvelle autorisation suivante a été ajoutée à la politique `AWSCleanRoomsFullAccessNoQuerying` gérée : `cleanrooms:BatchGetSchemaAnalysisRule` .	13 mai 2024
AWS Clean Rooms ML est désormais entièrement disponible	AWS Clean Rooms Le ML fournit une méthode d'amélioration de la confidentialité permettant à deux parties d'identifier des utilisateurs similaires dans leurs données sans avoir à partager leurs données entre elles.	3 avril 2024
Mise à jour de la politique existante	L'ID de déclaration dans la politique `AWSCleanRoomsFullAccess` gérée a été mis ConsolePickQueryResultsBucket à jour de SetQueryResultsBucket pour mieux représenter les autorisations depuis les autorisations.	21 mars 2024
Nouvelles politiques gérées pour le machine AWS Clean Rooms learning	Deux nouvelles politiques gérées ont été ajoutées : `AWSCleanRoomsMLReadOnlyAccess` et`AWSCleanRoomsMLFullAccess` .	29 novembre 2023

AWS Clean Rooms ML (aperçu)	AWS Clean Rooms Le ML fournit une méthode d'amélioration de la confidentialité permettant à deux parties d'identifier des utilisateurs similaires dans leurs données sans avoir à partager leurs données entre elles.	29 novembre 2023
AWS Clean Rooms Confidentialité différentielle (version préliminaire)	Les clients peuvent désormais utiliser la confidentialité AWS Clean Rooms différentielle pour protéger la vie privée de leurs utilisateurs.	29 novembre 2023
Configuration du paiement	Le créateur de la collaboration peut désormais configurer le membre autorisé à exécuter des requêtes ou un autre membre de la collaboration pour qu'il soit facturé pour les coûts de calcul des requêtes.	14 novembre 2023
Durée d'exécution de la requête - mise à jour	La durée maximale d'exécution d'une requête avant la mise à jour du délai d'expiration passe de 4 heures à 12 heures.	6 octobre 2023

AWS CloudFormation ressources - mise à jour	AWS Clean Rooms a ajouté les nouvelles ressources suivantes : `AWS::CleanRooms::Membership ProtectedQueryOutputConfiguration AWS::CleanRooms::Membership ProtectedQueryResultConfiguration , etAWS::CleanRooms::Membership ProtectedQueryS3OutputConfiguration .`	7 septembre 2023
AWS CloudFormation ressources - mise à jour	AWS Clean Rooms a ajouté les nouvelles ressources suivantes : `AWS::CleanRooms::AnalysisTemplate etAWS::CleanRooms::ConfiguredTable AnalysisRuleCustom .`	31 août 2023
Capacités distinctes des membres	Le créateur de la collaboration peut désormais désigner un membre en tant que membre habilité à effectuer des requêtes et un autre membre en tant que membre habilité à recevoir les résultats. Cela permet au créateur de la collaboration de s'assurer que le membre autorisé à effectuer une requête n'a pas accès aux résultats de la requête.	30 août 2023

AWS Clean Rooms Glossaire	Mise à jour portant uniquement sur la documentation pour ajouter un glossaire des termes. AWS Clean Rooms	30 août 2023
Support pour Apache Iceberg les tableaux (aperçu)	AWS Clean Rooms supporte désormais Apache Iceberg les tables (aperçu).	25 août 2023
Mise à jour des quotas	La section Quotas a été mise à jour pour refléter le nouveau quota par défaut d'abonnements par compte.	9 août 2023
Mise à jour de la politique existante	Les nouvelles autorisations suivantes ont été ajoutées à la politique `AWSCleanRoomsFullAccessNoQuerying` gérée : `cleanrooms:CreateAnalysisTemplate` `cleanrooms:GetAnalysisTemplate` , `cleanrooms:UpdateAnalysisTemplate` `cleanrooms:DeleteAnalysisTemplate` ,`cleanrooms:ListAnalysisTemplates` ,`cleanrooms:GetCollaborationAnalysisTemplate` ,`cleanrooms:BatchGetCollaborationAnalysisTemplate` , et `cleanrooms:ListCollaborationAnalysisTemplates` .	31 juillet 2023

Modèles d'analyse et règle d'analyse personnalisée	AWS Clean Rooms prend désormais en charge les modèles d'analyse et la règle d'analyse personnalisée. Les modèles d'analyse permettent aux collaborateurs de créer ou d'importer leur propre SQL requête personnalisée à utiliser dans le cadre de la collaboration. Avec la règle d'analyse personnalisée, le propriétaire de la table peut approuver des SQL requêtes personnalisées sur ses tables configurées.	31 juillet 2023
Les règles d'analyse prennent en charge la condition `OR` logique	AWS Clean Rooms les règles d'analyse prennent désormais en charge la condition `OR` logique de la JOIN clause.	29 juin 2023
CloudFormation intégration	AWS Clean Rooms s'intègre désormais à AWS CloudFormation.	15 juin 2023
Générateur d'analyses	Les membres autorisés à effectuer des requêtes et à recevoir des résultats peuvent désormais exécuter des requêtes sur certaines tables sans écrire de SQL code à l'aide de l'interface utilisateur du générateur d'analyse.	15 juin 2023

SQLfonctions	Mise à jour de documentation uniquement pour clarifier les fonctions prises en chargeSQL .	5 mai 2023
Dépannage	Mise à jour basée uniquement sur la documentation pour ajouter une section de résolution des problèmes courants.	27 avril 2023
Types de données pris en charge pour AWS Clean Rooms	Mise à jour relative à la documentation uniquement pour ajouter une nouvelle section répertoriant les types de AWS Glue Data Catalog données pris en charge.	26 avril 2023
Exemples d' AWS CloudTrail événements	Mise à jour de documentation uniquement pour ajouter des exemples d' CloudTrail événements pour StartProtectedQuery (réussite) et StartProtectedQuery (échec).	20 avril 2023
Mise à jour de la politique existante	Les nouvelles autorisations suivantes ont été ajoutées à la politique `AWSCleanRoomsFullAccessNoQuerying` gérée :`cleanrooms:ListTagsForResource` ,`cleanrooms:UntagResource` , et`cleanrooms:TagResource` . Pour plus d'informations, consultez la section Politiques AWS gérées.	21 mars 2023

Disponibilité générale	AWS Clean Rooms est désormais disponible pour tous.	21 mars 2023
Version préliminaire	Version préliminaire du guide de AWS Clean Rooms l'utilisateur	12 janvier 2023

AWS Clean Rooms Glossaire

Consultez ce glossaire pour vous familiariser avec la terminologie utilisée pour AWS Clean Rooms.

Règle d'analyse d'agrégation

La restriction de requête qui autorise les requêtes qui regroupent l'analyse COUNT en SUM utilisant ou AVG fonctionnant selon des dimensions facultatives. Ces requêtes ne révéleront pas d'informations au niveau des lignes.

Prend en charge des cas d'utilisation tels que la planification des campagnes, la portée médiatique, la fréquence et la mesure des conversions.

Les autres types de règles d'analyse sont personnalisées et listées.

Règles d'analyse

Les restrictions de requête qui autorisent un type de requête spécifique.

Le type de règle d'analyse détermine le type d'analyse qui peut être exécuté sur la table configurée. Chaque type possède une structure de requête prédéfinie. Vous contrôlez la manière dont les colonnes de votre table peuvent être utilisées dans la structure par le biais des commandes de requête.

Les types de règles d'analyse sont l'agrégation, la liste et les règles personnalisées.

Modèle d'analyse

Une requête pré-approuvée spécifique à la collaboration qui peut être réutilisée.

Prend en charge les SQL requêtes personnalisées prises en charge dans AWS Clean Rooms.

Peut contenir des paramètres là où une valeur littérale peut généralement apparaître dans une SQL requête. Pour plus d'informations sur les types de paramètres pris en charge, consultez la section Types de données dans la AWS Clean Rooms SQLréférence.

Les modèles d'analyse fonctionnent uniquement avec la règle d'analyse personnalisée.

Client de chiffrement C3R

Le client de chiffrement Cryptographic Computing for Clean Rooms (C3R).

Utilisé pour chiffrer et déchiffrer des données, C3R est un système de chiffrement SDK côté client doté d'une interface de ligne de commande.

Colonne en texte clair

Colonne qui n'est protégée cryptographiquement ni pour une construction, ni pour une JOIN SELECT SQL construction.

Les colonnes en texte clair peuvent être utilisées dans n'importe quelle partie de la SQL requête.

Collaboration

Limite logique sécurisée AWS Clean Rooms dans laquelle les membres peuvent effectuer des SQL requêtes sur des tables configurées.

Les collaborations sont créées par le créateur de la collaboration.

Seuls les membres qui ont été invités à participer à la collaboration peuvent rejoindre la collaboration.

Une collaboration ne peut avoir qu'un seul membre qui peut interroger des données, un membre qui peut recevoir les résultats et un membre payant les coûts de calcul des requêtes.

Tous les membres peuvent consulter la liste des participants invités à la collaboration avant de rejoindre la collaboration.

Créateur de collaboration

Le membre qui crée une collaboration.

Il n'y a qu'un seul créateur de collaboration par collaboration.

Seul le créateur de la collaboration peut retirer des membres de la collaboration ou supprimer la collaboration.

Table configurée

Chaque table configurée représente une référence à une table existante dans le AWS Glue Data Catalog qui a été configurée pour être utilisée dans AWS Clean Rooms. Une table configurée contient une règle d'analyse qui détermine la manière dont les données peuvent être utilisées.

Actuellement, AWS Clean Rooms prend en charge l'association de données stockées dans Amazon Simple Storage Service (Amazon S3) qui sont cataloguées via. AWS Glue

Pour plus d'informations à ce sujet AWS Glue, consultez le guide du AWS Glue développeur.

Les tables configurées peuvent être associées à une ou plusieurs collaborations.

> **Note**
>
> AWS Clean Rooms ne prend actuellement pas en charge les emplacements de compartiment Amazon S3 enregistrés auprès de AWS Lake Formation.

Règle d'analyse personnalisée

La restriction de requête qui autorise un ensemble spécifique de requêtes préapprouvées (modèles d'analyse) ou autorise un ensemble spécifique de comptes capables de fournir des requêtes utilisant vos données.

Prend en charge des cas d'utilisation tels que l'attribution au premier contact, les analyses incrémentielles et les analyses de découverte d'audience.

Soutient la confidentialité différentielle.

Les autres types de règles d'analyse sont l'agrégation et la liste.

Déchiffrement

Le 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.

Confidentialité différentielle

Une technique mathématiquement rigoureuse qui protège les données de collaboration contre le membre qui peut recevoir des résultats en apprenant sur une personne en particulier.

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.

Colonne d'empreintes digitales

Colonne protégée cryptographiquement pour une JOIN SQL construction.

Méthode de workflow de mappage des identifiants

Comment souhaitez-vous que le mappage des identifiants soit effectué.

Il existe deux méthodes de flux de travail de mappage d'identifiants :

- Mappage d'ID basé 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'ID.
- Mappage des identifiants des services fournisseurs : 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.

  AWS Clean Rooms est actuellement prise en charge en LiveRamp tant que méthode de flux de travail de mappage des identifiants basée sur les services des fournisseurs de services. Vous devez être abonné à LiveRamp through AWS Data Exchange pour utiliser cette méthode. Pour plus d'informations, consultez la section Abonnement à un service fournisseur AWS Data Exchange dans le guide de Résolution des entités AWS l'utilisateur.

Table de mappage des identifiants

Une ressource AWS Clean Rooms qui permet soit des règles de correspondance de première partie, soit un transcodage d'identité multipartite dans le cadre d'une collaboration.

Une table de mappage d'identifiants est une référence à une table existante dans le AWS Glue Data Catalog. Il contient une règle d'analyse des tables de mappage d'identifiants qui détermine la manière dont les données peuvent être consultées. AWS Clean Rooms Les tables de mappage d'identifiants peuvent être associées à une ou plusieurs collaborations.

Règle d'analyse des tables de mappage d'identifiants

Type de règle d'analyse gérée par AWS Clean Rooms et utilisée pour joindre des données d'identité disparates afin de faciliter les requêtes. Il est automatiquement ajouté aux tables de mappage des identifiants et ne peut pas être modifié. Elle hérite des comportements des autres règles d'analyse de la collaboration, à condition que ces règles d'analyse soient homogènes.

Workflow de mappage des identifiants

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

Espace de noms ID

Une ressource AWS Clean Rooms 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.

Association d'espaces de noms ID

Association d'une ressource d'espace de noms d'identification qui vous aide à découvrir les entrées dans leur flux de travail de mappage d'identifiants.

Règle d'analyse des listes

La restriction de requête qui autorise les requêtes qui génèrent une analyse attributaire au niveau des lignes du chevauchement entre cette table et les tables du membre qui peut effectuer la requête.

Prend en charge des cas d'utilisation tels que l'enrichissement et la création ou la suppression d'audience.

Les autres types de règles d'analyse sont l'agrégation et les règles personnalisées.

Membre

Un AWS client participant à une collaboration.

Un membre est identifié à l'aide de son Compte AWS.

Tous les membres peuvent fournir des données.

Membre pouvant poser des questions

Le membre qui peut interroger des données dans le cadre de la collaboration.

Un seul membre peut effectuer une requête par collaboration, et ce membre est immuable.

Un utilisateur administratif peut utiliser les autorisations AWS Identity and Access Management (IAM) pour contrôler lequel de ses IAM principaux utilisateurs (tels que les utilisateurs ou les rôles) peut interroger des données dans le cadre de la collaboration. Pour de plus amples informations, veuillez consulter Création d'un rôle de service pour lire les données.

Membre pouvant recevoir les résultats

Le membre qui peut recevoir les résultats de la requête. Le membre qui peut recevoir les résultats spécifie les paramètres des résultats de requête pour la destination Amazon S3 et le format des résultats de requête.

Un seul membre peut recevoir des résultats par collaboration, et ce membre est immuable.

Membre payant les frais de calcul des requêtes

Le membre responsable du paiement des frais de calcul des requêtes.

Un seul membre est responsable du paiement des coûts de calcul des requêtes par collaboration, et ce membre est immuable.

Si le créateur de la collaboration n'a indiqué aucun membre payant les frais de calcul des requêtes, le membre habilité à effectuer les requêtes est le payeur par défaut.

Le membre qui paie les frais de calcul des requêtes reçoit une facture pour les requêtes exécutées dans le cadre de la collaboration.

Membres

Ressource créée lorsqu'un membre rejoint une collaboration.

Toutes les ressources que le membre associe à une collaboration font partie de l'adhésion ou sont associées à l'adhésion.

Seul le membre propriétaire de l'adhésion peut ajouter, supprimer ou modifier les ressources de cette adhésion.

Colonne étanche

Colonne protégée cryptographiquement pour une SELECT SQL construction.

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.