



Guide de l'utilisateur

# AWS Clean Rooms



# AWS Clean Rooms: Guide de l'utilisateur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

---

# Table of Contents

Qu'est-ce qu'AWS Clean Rooms ? .....	1
Utilisez-vous AWS Clean Rooms pour la première fois ? .....	2
Fonctionnement d'AWS Clean Rooms .....	2
Services connexes .....	4
Accès à AWS Clean Rooms .....	5
Tarification de AWS Clean Rooms .....	6
Facturation pour AWS Clean Rooms .....	6
Règles d'analyse .....	7
Types de règles d'analyse .....	8
Cas d'utilisation pris en charge .....	8
Contrôles pris en charge .....	10
Règle d'analyse d'agrégation .....	12
Structure et syntaxe des requêtes d'agrégation .....	12
Règle d'analyse d'agrégation : contrôles des requêtes .....	20
Règle d'analyse d'agrégation : contrôles des résultats des requêtes .....	25
Structure des règles d'analyse d'agrégation .....	26
Règle d'analyse d'agrégation - exemple .....	27
Résolution des problèmes liés aux règles d'analyse d'agrégation .....	32
Règle d'analyse des listes .....	33
Structure et syntaxe des requêtes de liste .....	33
Règle d'analyse des listes : contrôles des requêtes .....	37
Structure prédéfinie des règles d'analyse des listes .....	39
Règle d'analyse des listes - exemple .....	40
Règle d'analyse personnalisée .....	42
Structure prédéfinie des règles d'analyse personnalisées .....	43
Exemple de règle d'analyse personnalisée .....	44
Règle d'analyse personnalisée avec confidentialité différentielle .....	47
AWS Clean Rooms Confidentialité différentielle .....	50
Confidentialité différentielle .....	50
Comment AWS Clean Rooms fonctionne la confidentialité différentielle .....	51
Considérations .....	52
Politique de confidentialité différentielle .....	52
Fonctionnalités SQL .....	54
Alternatives courantes pour les constructions SQL non prises en charge .....	68

Conseils et exemples relatifs aux requêtes SQL .....	69
Limites .....	70
AWS Clean Rooms ML .....	72
AWS Clean Rooms ML .....	72
Comment fonctionne le AWS Clean Rooms ML .....	73
Protection de la vie privée du AWS Clean Rooms ML .....	74
Métriques du modèle .....	75
Travailler avec AWS Clean Rooms ML .....	76
Utilisation de modèles similaires (fournisseur de données de formation) .....	77
Utilisation de segments similaires (fournisseur de données de départ) .....	80
Étapes suivantes .....	82
Informatique cryptographique .....	83
Considérations .....	84
Autoriser les données mélangéescleartext et cryptées dans vos tableaux .....	85
Autoriser les valeurs répétées dansfingerprint les colonnes .....	85
Assouplissement des restrictions relatives au nom desfingerprint colonnes .....	86
Déterminer commentNULL les valeurs sont représentées .....	87
Types de fichiers et de données pris en charge .....	87
fichiers CSV .....	88
Parquetfichiers .....	91
Chiffrement de valeurs autres que des chaînes .....	92
Noms de colonnes .....	93
Normalisation des noms d'en-têtes de colonne .....	93
Types de colonnes .....	93
Fingerprintcolonnes .....	94
Colonnes étanches .....	94
Cleartextcolonnes .....	96
Paramètres .....	96
Paramètre Autorisercleartext les colonnes .....	96
Paramètre Autoriser les doublons .....	97
Paramètre AutorisationJOIN des colonnes avec des noms différents .....	98
Paramètre de préservationNULL des valeurs .....	100
Indicateurs facultatifs .....	101
--csvInputNULLValuedrapeau .....	102
--csvOutputNULLValuedrapeau .....	102
--enableStackTracesdrapeau .....	103

--dryRundrapeau .....	103
--tempDirdrapeau .....	104
Requêtes avec C3R .....	104
Requêtes qui se ramifient surNULL .....	105
Mappage d'une colonne source à plusieurs colonnes cibles .....	105
Utiliser les mêmes données pourJOIN les deuxSELECT requêtes .....	105
Consignes .....	105
Implications sur les performances pour les types de colonnes .....	106
Résolution des problèmes liés à l'augmentation imprévue de la taille du texte chiffré .....	130
Journalisation des requêtes .....	133
Réception des journaux de requêtes .....	134
Utilisation des journaux de requêtes .....	135
Con AWS Clean Rooms figuration .....	136
Inscrivez-vous pour AWS .....	136
Configurer les rôles de service pour AWS Clean Rooms .....	136
Création d'un utilisateur administrateur .....	137
Création d'un rôle IAM pour un membre de la collaboration .....	138
Création d'un rôle de service pour lire les données .....	139
Créez un rôle de service pour recevoir des résultats .....	143
Configuration des rôles de service pour le AWS Clean Rooms ML .....	147
Création d'un rôle de service pour lire les données d'entraînement .....	147
Création d'un rôle de service pour écrire un segment similaire .....	151
Création d'un rôle de service pour lire les données de départ .....	156
Création d'une collaboration .....	160
Créez une collaboration .....	160
Étapes suivantes .....	168
Création d'un abonnement et adhésion à une collaboration .....	169
Créez un abonnement et rejoignez une collaboration .....	169
Étapes suivantes .....	172
Préparation de tableaux de données .....	173
Étape 1 : Exécuter les prérequis .....	173
Étape 2 : (Facultatif) Préparez vos données pour le calcul cryptographique .....	174
Étape 3 : Chargez votre tableau de données sur Amazon S3 .....	174
Étape 4 : Création d'une AWS Glue table .....	175
Étapes suivantes .....	176
Formats de données .....	176

Formats de données pris en charge .....	176
Types de données pris en charge .....	177
Types de compression de fichiers pourAWS Clean Rooms .....	178
Chiffrement côté serveur pourAWS Clean Rooms .....	178
Tables Apache Iceberg .....	179
Types de données pris en charge pour les tables Iceberg .....	180
Préparation de tables de données chiffrées .....	182
Étape 1 : Exécuter les prérequis .....	182
Étape 2 : Téléchargez le client de chiffrement C3R .....	183
(Facultatif) Étape 3 : Afficher les commandes disponibles dans le client de chiffrement C3R ....	184
Étape 4 : générer un schéma de chiffrement pour un fichier tabulaire .....	184
Exemple : génération d'un schéma de chiffrement pour une fingerprint colonne et une cleartext colonne .....	188
Exemple : génération d'un schéma de chiffrement avec des cleartext colonnes sealedfingerprint, et .....	190
Étape 5 : Création d'une clé secrète partagée .....	192
Exemple : génération de clés à l'aide de OpenSSL .....	192
Exemple : génération de clés lors de l'Windowsutilisation PowerShell .....	193
Étape 6 : Stocker la clé secrète partagée dans une variable d'environnement .....	193
Stocker la clé dans une variable d'environnement lors de Windows l'utilisation PowerShell ..	194
Stocker la clé dans une variable d'environnement sur Linux ou macOS .....	194
Étape 7 : Chiffrer les données .....	194
Étape 8 : vérifier le chiffrement des données .....	195
(Facultatif) Créez un schéma (utilisateurs avancés) .....	196
Schémas de tables cartographiées et positionnelles .....	197
Création d'une table configurée .....	207
Création d'une table configurée .....	207
Étapes suivantes .....	208
Configuration d'une règle d'analyse sur une table configurée .....	209
Configuration d'une règle d'analyse d'agrégation pour une table (flux guidé) .....	210
Configuration d'une règle d'analyse de liste pour une table (flux guidé) .....	213
Configuration d'une règle d'analyse personnalisée pour une table (flux guidé) .....	215
Configuration d'une règle d'analyse pour une table (éditeur JSON) .....	217
Étapes suivantes .....	219
Associer une table configurée à une collaboration .....	220
Associer une table configurée depuis la page détaillée de la table configurée .....	221

Associer une table configurée depuis la page détaillée de la collaboration .....	224
Étapes suivantes .....	227
Configuration d'une politique de confidentialité différentielle .....	228
Configuration d'une politique de confidentialité différentielle (flux guidé) .....	228
Étapes suivantes .....	219
Utilisation de modèles d'analyse .....	230
Création d'un modèle d'analyse .....	230
Révision d'un modèle d'analyse .....	231
Interrogation de tables configurées à l'aide d'un modèle d'analyse .....	232
Interrogation de données dans le cadre d'une collaboration .....	234
Utilisation de l'éditeur de code SQL .....	235
Utilisation du générateur d'analyse .....	238
Utiliser le générateur d'analyse pour interroger une seule table (agrégation) .....	239
Utilisez le générateur d'analyse pour interroger deux tables (agrégation ou liste) .....	241
Interrogation de données avec confidentialité différentielle .....	245
Affichage des requêtes récentes .....	246
Affichage des détails de la requête .....	247
Réception des résultats de requêtes .....	248
Recevoir les résultats d'une requête .....	248
Modifier les valeurs par défaut pour les paramètres des résultats de requête .....	249
Utilisation du résultat de la requête dans d'autresServices AWS .....	250
Décryptage des tables de données .....	251
Gestion d'AWS Clean Rooms .....	253
Gérer les collaborations .....	253
Collaborations d'édition .....	254
Supprimer des collaborations .....	258
Afficher les collaborations .....	258
Afficher les tables et les règles d'analyse .....	259
Afficher les journaux d'utilisation différentiels de confidentialité .....	259
Surveillance du statut des membres .....	260
Supprimer un membre d'une collaboration .....	260
Quitter une collaboration .....	261
Modification des associations de tables configurées .....	262
Dissociation des tables configurées .....	263
Modifier une politique de confidentialité différentielle .....	263
Supprimer une politique de confidentialité différentielle .....	264

Affichage des paramètres de confidentialité différentiels calculés .....	265
Gestion des tables configurées .....	266
Modification des détails d'une table configurée .....	267
Modification des balises de tableau configurées .....	267
Modification d'une règle d'analyse de table configurée .....	268
Suppression d'une règle d'analyse de table configurée .....	268
Résolution des problèmes .....	270
Une ou plusieurs tables référencées par la requête ne sont pas accessibles par leur rôle de service associé. Le propriétaire de la table/du rôle doit accorder au rôle de service l'accès à la table. ....	270
Le format de fichier de l'un des ensembles de données sous-jacents n'est pas pris en charge. ....	270
Les résultats des requêtes ne correspondent pas aux attentes lors de l'utilisation du calcul cryptographique pour Clean Rooms. ....	271
Sécurité .....	272
Protection des données .....	273
Chiffrement au repos .....	274
Chiffrement en transit .....	274
Chiffrement des données sous-jacentes .....	274
Conservation des données .....	275
Bonnes pratiques .....	275
Les meilleures pratiques avec AWS Clean Rooms .....	276
Bonnes pratiques d'utilisation des règles d'analyse dans AWS Clean Rooms .....	276
Gestion de l'identité et des accès .....	278
Public ciblé .....	279
Authentification par des identités .....	280
Gestion des accès à l'aide de politiques .....	284
Comment AWS Clean Rooms fonctionne avec IAM .....	286
Exemples de politiques basées sur l'identité .....	294
AWS politiques gérées .....	297
Résolution des problèmes .....	318
Prévention du cas de figure de l'adjoint désorienté entre services .....	320
Comportements IAM pour le ML AWS Clean Rooms .....	322
Validation de conformité .....	325
Résilience .....	326
Sécurité de l'infrastructure .....	327



Sécurité du réseau .....	327
AWS PrivateLink .....	328
Considérations .....	328
Création d'un point de terminaison d'interface .....	328
Surveillance .....	330
CloudTrail journaux .....	330
AWS Clean Rooms informations dans CloudTrail .....	331
Présentation des AWS Clean Rooms entrées des fichiers journaux .....	332
Exemples d'AWS Clean Rooms CloudTrail événements .....	332
AWS CloudFormation ressources .....	336
AWS Clean Rooms et AWS CloudFormation modèles .....	336
En savoir plus sur AWS CloudFormation .....	338
Quotas .....	340
Historique de la documentation .....	356
Glossaire .....	363
Règle d'analyse d'agrégation .....	363
Règles d'analyse .....	363
Modèle d'analyse .....	363
Client de chiffrement C3R .....	364
Colonne en texte clair .....	364
Collaboration .....	364
Créateur de collaboration .....	364
Table configurée .....	365
Règle d'analyse personnalisée .....	365
Déchiffrement .....	365
Confidentialité différentielle .....	365
Chiffrement .....	366
Colonne d'empreintes digitales .....	366
Règle d'analyse des listes .....	366
Membre .....	366
Membre pouvant poser des questions .....	366
Membre pouvant recevoir les résultats .....	367
Membre payant les frais de calcul des requêtes .....	367
Membres .....	367
Colonne étanche .....	367
.....	ccclxviii

# Qu'est-ce qu'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 requêtes SQL 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 RoomsML](#) 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. La seconde partie apporte ses données de départ à une collaboration et crée un segment similaire aux données d'entraînement.

La vidéo suivante explique plus en détail AWS Clean Rooms.

[AWS Clean Rooms](#)

# Utilisez-vous AWS Clean Rooms pour la première fois ?

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

- [Fonctionnement d'AWS Clean Rooms](#)
- [Accès à AWS Clean Rooms](#)
- [Con AWS Clean Rooms figuration](#)
- [Glossaire AWS Clean Rooms](#)

## Fonctionnement d'AWS Clean Rooms

Le flux de travail suivant 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.

En résumé, le flux de travail pour AWS Clean Rooms est le suivant :

1. 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](#).
2. 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 ARN de rôle de service à 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.

3. Le [membre 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 pour Clean Rooms.)

 Note

AWS Clean Rooms supporte AWS Glue les tables. Pour plus d'informations sur l'introduction de vos données AWS Glue, consultez [Étape 3 : Chargez votre tableau de données sur Amazon S3](#).

1. Le membre nomme la [table configurée](#) et choisit les colonnes à utiliser dans la collaboration.
2. Le membre [configure l'une des règles d'analyse suivantes pour la table configurée](#) :
  - [Règle d'analyse d'agrégation](#) ou [règle d'analyse de liste](#) : pour contrôler le type d'analyse qui peut être exécuté sur la table.
  - [Règle d'analyse personnalisée](#) : pour autoriser un ensemble spécifique de requêtes préapprouvées ou un ensemble spécifique de comptes pouvant fournir des requêtes utilisant vos données. Permet au membre d'activer la confidentialité différentielle pour se protéger contre les tentatives d'identification des utilisateurs.

 Note

Le membre peut configurer la règle d'analyse à tout moment avant d'associer ses tables configurées à la collaboration.

4. Le membre [associe ses tables configurées à la collaboration](#) et attribue AWS Clean Rooms un rôle de service pour accéder à ses 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.

5. Le membre habilité à effectuer des requêtes [exécute des requêtes SQL sur les tables configurées](#).

Les requêtes ne peuvent être exécutées que si le membre chargé de payer les coûts de calcul des requêtes a rejoint la collaboration en tant que membre actif.

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 à l'étape 3.b.

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 (voir étape 8).

6. Le [membre qui peut recevoir les résultats](#) examine les résultats dans la AWS Clean Rooms console ou dans le compartiment Amazon S3 qu'il a spécifié.
7. Le [membre qui paie les coûts de calcul des requêtes](#) est facturé pour les requêtes exécutées dans le cadre de la collaboration.
8. [\(Facultatif\) 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.](#)

## Services connexes

Les éléments suivants Services AWS 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 plus d'informations, consultez [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 Service AWS l'activité.

Pour plus d'informations, consultez [Journalisation des appels d'API AWS Clean Rooms avec AWS CloudTrail](#).

## Accès à AWS Clean Rooms

Vous pouvez y accéder AWS Clean Rooms par le biais des options suivantes :

- Directement via la AWS Clean Rooms console à l'[adresse https://console.aws.amazon.com/cleanrooms/](https://console.aws.amazon.com/cleanrooms/).
- Par programmation via l'API. AWS Clean Rooms Pour plus d'informations, consultez la page [Référence de l'API AWS Clean Rooms](#).

## Tarification de 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, consultez [Créez 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.

Exemple 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.

Exemple 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.

Les tableaux suivants présentent un résumé comparatif des types de règles 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	<a href="#">Agrégation</a>	<a href="#">List</a>	<a href="#">Personnalis</a> <a href="#">isé</a>
Analyses prises en charge	Requêtes qui regroupent des statistiques à l'aide des fonctions COUNT, SUM et AVG 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 courants	Analyse des segments,	Enrichissement,	Attribution directe, analyses

Cas d'utilisation	<a href="#">Agrégation</a>	<a href="#">List</a>	<a href="#">Personnalisé</a>
	mesure, attribution	création de segments	incrémentielles, découverte de l'audience
Constructeurs SQL	<ul style="list-style-type: none"> <li>• <a href="#">Déclaratives</a> <a href="#">JOIN</a> : INNER JOIN</li> <li>• <a href="#">Fonctions d'agrégation</a> <a href="#">ion</a> : COUNT/ COUNT DISTINCT, SUM/ SUM DISTINCT et AVG</li> <li>• <a href="#">Fonctions scalaires</a> : sous-ensemble limité</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Déclaratives</a> <a href="#">JOIN</a> : INNER JOIN</li> <li>• Fonctions scalaires : Aucune</li> </ul>	La plupart des fonctions et constructeurs SQL sont disponibles avec la commande SELECT
Sous-requêtes et expressions de table communes (CTE)	Non	Non	Oui

Cas d'utilisation	<a href="#">Agrégation</a>	<a href="#">List</a>	<a href="#">Personnalisé</a>
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	<a href="#">Agrégation</a>	<a href="#">List</a>	<a href="#">Personnalisé</a>
Mécanisme de commande	<p>Contrôler la manière dont les données de la table peuvent être utilisées dans une requête</p> <p>(Par exemple, autorisez COUNT et SUM de la colonne hashed_email.)</p>	<p>Contrôler la manière dont les données de la table peuvent être utilisées dans une requête</p> <p>(Par exemple, autorisez l'utilisation de la colonne hashed_email uniquement pour la connexion.)</p>	<p>Contrôler les requêtes autorisées à s'exécuter sur la table</p> <p>(Par exemple, autorisez uniquement les requêtes définies dans les modèles d'analyse « Requête personnalisée 1 ».)</p>

Contrôle	<u>Agrégation</u>	<u>List</u>	<u>Personnalis</u> <u>isé</u>
Techniques intégrées d'amélioration de la confidentialité	<ul style="list-style-type: none"> <li>• Match à l'aveugle</li> <li>• Agrégation requise</li> <li>• Seuil d'agrégation minimum &gt;=</li> <li>• 2 Structure de requête prédéfinie</li> </ul>	<ul style="list-style-type: none"> <li>• Match à l'aveugle</li> <li>• Chevauchement requis</li> <li>• Structure de requête prédéfinie</li> </ul>	Confidentialité différentielle
Vérifiez la requête avant de pouvoir l'exécuter	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

Dans AWS 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 dans [Structure et syntaxe des requêtes d'agrégation](#).

Les paramètres de la règle d'analyse, définis dans [Règle 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
<i>select_aggregate_function_expression</i>	<p>Une liste séparée par des virgules contenant les expressions suivantes :</p> <ul style="list-style-type: none"> <li>• <i>select_aggregation_function_expression</i></li> <li>• <i>select_aggregate_expression</i></li> </ul>	SELECT SUM(PRICE), user_segment
	<p><b>Note</b></p> <p>Il doit y en avoir au moins un <i>select_aggregation_function_expression</i> dans le <i>select_aggregate_expression</i> .</p>	
<i>select_aggregation_function_expression</i>	Une ou plusieurs fonctions d'agrégation prises en charge sont appliquées à une ou plusieurs colonnes. Seules	AVG(PRICE) COUNT(DISTINCT user_id)

Expression	Définition	Exemples
	<p>les colonnes sont autorisées comme arguments des fonctions d'agrégation.</p> <div data-bbox="592 384 1031 892"><p> <b>Note</b></p><p>Il doit y en avoir au moins un <code>select_aggregation_function_expression</code> dans le <code>select_aggregate_expression</code>.</p></div>	

Expression	Définition	Exemples
<i>select_grouping_column_expression</i>	<p>Expression qui peut contenir n'importe quelle expression utilisant les éléments suivants :</p> <ul style="list-style-type: none"><li>• Nom des colonnes de la table</li><li>• Fonctions scalaires prises en charge</li><li>• Littéraux de chaîne</li><li>• Littéraux numériques</li></ul>	<p>TRUNC(timestampColumn)</p> <p>UPPER(campaignName)</p>

 **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](#).



Expression	Définition	Exemples
<i>table_expression</i>	<p>Table, ou jointure de tables, reliant des expressions conditionnelles de jointure à <code>join_condition</code> .</p> <p><code>join_condition</code> renvoie une valeur booléenne.</p> <p>Les <code>table_expression</code> supports :</p> <ul style="list-style-type: none"><li>• Un JOIN type spécifique (INNERJOIN)</li><li>• La condition de comparaison de l'égalité au sein d'un <code>join_condition</code> (=)</li><li>• Opérateurs logiques (AND,OR).</li></ul>	<pre>FROM consumer_table INNER JOIN provider_ table ON consumer_table.ide ntifier1 = provider_ table.identifiaer1 AND consumer_table .identifiaer2 = provider_table.ide ntifier2</pre>

Expression	Définition	Exemples
<i>where_expression</i>	<p>Expression conditionnelle qui renvoie une valeur booléenne . Il peut être composé des éléments suivants :</p> <ul style="list-style-type: none"> <li>• Nom des colonnes de la table</li> <li>• Fonctions scalaires prises en charge</li> <li>• Opérateurs mathématiques</li> <li>• Littéraux de chaîne</li> <li>• Littéraux numériques</li> </ul> <p>Les conditions de comparaison prises en charge sont (=, &gt;, &lt;, &lt;=, &gt;=, &lt;&gt;, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL).</p> <p>Les opérateurs logiques pris en charge sont (AND, OR).</p> <p>where_expression C'est facultatif.</p>	<pre>WHERE where_condition  WHERE price &gt; 100  WHERE TRUNC(timestampColumn) = '1/1/2022'  WHERE timestampColumn = timestampColumn2 - 14</pre>
<i>group_by_expression</i>	<p>Liste d'expressions séparées par des virgules qui répondent aux exigences du <code>select_grouping_column_expression</code></p>	<pre>GROUP BY TRUNC(timestampColumn), UPPER(campaignName), segment</pre>

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

Expression	Définition	Exemples
<i>order_by_expression</i>	<p>Liste d'expressions séparées par des virgules qui est compatible avec les mêmes exigences définies dans la section <code>select_aggregate_expression</code> définie précédemment.</p> <p><code>order_by_expression</code> C'est facultatif.</p> <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p><code>order_by_expression</code> autorisations ASC et DESC paramètres. Pour plus d'informations, consultez la section Paramètres ASC DESC dans le manuel <a href="#">AWS Clean RoomsSQL Reference</a>.</p> </div>	<p>ORDER BY SUM(SALES), UPPER(campaignName)</p>

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](#)
- [Commandes de jointure](#)
- [Contrôles dimensionnels](#)
- [Fonctions scalaires](#)

### 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.	<p>aggregateColumns peut être utilisé dans une fonction d'agrégation dans les ORDER BY expressions SELECTHAVING,, et.</p> <p>Certains aggregateColumns peuvent également être classés dans la catégorie « A » joinColumn (définis ultérieurement).</p> <p>Given ne aggregateColumn peut pas également</p>

Contrôle	Définition	Utilisation
		être classé dans la catégorie <code>dimensionColumn</code> (défini ultérieurement).
<code>function</code>	Les fonctions COUNT, SUM et AVG que vous autorisez à utiliser en plus de <code>aggregateColumns</code> .	<code>function</code> peut être appliqué à un <code>aggregateColumns</code> 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 de `table_expression`. AWS Clean Rooms prend uniquement en charge INNER JOIN. INNER JOIN Les 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 du JOIN. 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.	<p>Un spécifique joinColumn peut également être classé dans la catégorie aggregateColumn (voir <a href="#">Contrôles d'agrégation</a>).</p> <p>La même colonne ne peut pas être utilisée à la fois comme joinColumn et dimensionColumns (voir plus loin).</p> <p>À moins qu'il n'ait également été classé comme un aggregateColumn, a ne joinColumn peut être</p>

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.	<p>Si vous activez ce paramètre , un INNER JOIN est requis. Si vous n'activez pas ce paramètre, un INNER JOIN est facultatif.</p> <p>En supposant que vous activez 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).</p>

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
<code>dimensionColumns</code>	Les colonnes (le cas échéant) que vous autorisez le membre autorisé à effectuer une requête à utiliser dans <code>SELECT</code> WHERE, <code>GROUPBY</code> , et <code>ORDERBY</code> .	<p>A <code>dimensionColumn</code> peut être utilisé dans <code>SELECT (select_grouping_column_expression )WHERE, GROUPBY, et ORDERBY</code>.</p> <p>La même colonne ne peut pas être à la fois a <code>dimensionColumn joinColumn</code> , a et/ ou <code>anaggregateColumn</code> .</p>

## Fonctions scalaires

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

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

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 Rooms prend 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 <code>aggregateColumn</code> 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 <code>aggregateColumn</code> que la ligne de sortie doit avoir (par exemple, <code>COUNT DISTINCT</code> ) pour qu'elle soit renvoyée dans les résultats de la requête.	La valeur <code>minimum</code> 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": [
      "identifiant"
    ],
    "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
- `CAST` si 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.hashemail)
FROM
  sales companyA
  INNER JOIN returns companyB ON companyA.identifrier = companyB.identifrier
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, consultez [Règle d'analyse d'agrégation - exemple](#).

## Règle d'analyse des listes

Dans AWS 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, consultez [Structure prédéfinie des règles d'analyse des listes](#).

Les paramètres de la règle d'analyse de liste, définis dans [Règle 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
<i>select_list_expression</i>	<p>Liste séparée par des virgules contenant au moins un nom de colonne de table.</p> <p>Un DISTINCT paramètre est obligatoire.</p> <div data-bbox="592 1165 1031 1864" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Ils <i>select_list_expression</i> peuvent aliaser les colonnes avec ou sans le AS paramètre. Il prend également en charge le TOP paramètre. Pour plus d'informations, consultez la <a href="#">référence AWS Clean Rooms SQL</a>.</p> </div>	SELECT DISTINCT segment

Expression	Définition	Exemples
<i>table_expression</i>	<p>Une table, ou une jointure de tables, <code>join_condition</code> à laquelle la connecter <code>join_condition</code> .</p> <p><code>join_condition</code> renvoie une valeur booléenne.</p> <p>Les <code>table_expression</code> supports :</p> <ul style="list-style-type: none"><li>• Un type de JOIN spécifique (INNERJOIN)</li><li>• Les conditions de comparaison de l'égalité au sein d'un <code>join_condition</code> (=)</li><li>• Opérateurs logiques (AND,OR).</li></ul>	<pre>FROM consumer_table INNER JOIN provider_ table ON consumer_table.ide ntifier1 = provider_ table.identifiaer1 AND consumer_table .identifiaer2 = provider_table.ide ntifier2</pre>

Expression	Définition	Exemples
<i>where_expression</i>	<p>Expression conditionnelle qui renvoie une valeur booléenne . Il peut être composé des éléments suivants :</p> <ul style="list-style-type: none"> <li>• Nom des colonnes de la table</li> <li>• Opérateurs mathématiques</li> <li>• Littéraux de chaîne</li> <li>• Littéraux numériques</li> </ul> <p>Les conditions de comparaison prises en charge sont (=, &gt;, &lt;, &lt;=, &gt;=, &lt;&gt;, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL).</p> <p>Les opérateurs logiques pris en charge sont (AND, OR).</p> <p><i>where_expression</i> C'est facultatif.</p>	<pre>WHERE state + '_' + city = 'NY_NYC'</pre> <pre>WHERE timestampColumn = timestampColumn2 - 14</pre>
<i>limit_expression</i>	<p>Cette expression doit prendre un entier positif. Il peut également être échangé avec un paramètre TOP.</p> <p><i>limit_expression</i> C'est facultatif.</p>	<pre>LIMIT 100</pre>

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 Rooms ne 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
```

**INNER** Les 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 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 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 du JOIN. 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
<code>joinColumns</code>	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.	<p><code>joinColumn</code> et <code>listColumn</code> (voir <a href="#">Contrôles de liste</a>).</p> <p><code>joinColumn</code> ne peut être utilisé dans aucune autre partie de la requête que INNER JOIN.</p>

## 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'WHERE instruction).

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

## 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": [  
    "identifiant1",  
    "identifiant2"  
  ],  
  "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": [  
    "identifieur2"  
  ],  
  "listColumns": [  
    "segment3",  
    "segment4"  
  ]  
}
```

`joinColumns`— L'entreprise B permet à l'entreprise A de se joindre à elle pour `identifieur2` 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 `identifieur2` déterminer laquelle correspondrait à cette collaboration. Ils n'en ont pas ajouté d'autres `joinColumns` parce qu'ils pensaient `identifieur2` 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.identifieur2 = companyB.identifieur2
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 une requête, 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.hashemail = provider.hashemail
WHERE MONTH(labeleddata.purchasedate) > :campaignmonth
AND testgroup = :group
"
}

```

10 L'entreprise A ajoute son compte (par exemple, 657845239416) 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": [
    "657845239416"
  ]
}

```

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-1:657835239466:membership/41327cc4-bbf0-43f1-b70c-a160dddceb08/analysistemplate/1ff1bf9d-781c-418d-a6ac-2b80c09d6292"  
]  
}
```

14 L'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 dans 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 dans [Structure 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.hashemail` 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, consultez [Fonctionnalités SQL de AWS Clean Rooms Differential Privacy](#).

# 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](#)
- [Comment AWS Clean Rooms fonctionne la confidentialité différentielle](#)
- [Politique de confidentialité différentielle](#)
- [Fonctionnalités SQL de AWS Clean Rooms Differential Privacy](#)
- [Conseils et exemples de requêtes relatives à la confidentialité différentielle](#)
- [Limites de la confidentialité AWS Clean Rooms différentielle](#)

## 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 Differential Privacy 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 le [Politique 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

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 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 requêtes SQL. 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 pendant 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 actions de l'API du modèle de budget de confidentialité.

## Fonctionnalités SQL de AWS Clean Rooms Differential Privacy

AWS Clean Rooms La confidentialité différentielle utilise une structure de requête polyvalente pour prendre en charge les requêtes SQL complexes. 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	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
Fonctions d'agrégation	<ul style="list-style-type: none"> <li>Fonction ANY_VALUE</li> <li>Fonction APPROXIMATE PERCENTILE_DISC</li> <li>Fonction AVG</li> <li>Fonctions COUNT et COUNT DISTINCT</li> <li>Fonction LISTAGG</li> <li>Fonction MAX</li> <li>Fonction MEDIAN</li> <li>Fonction MIN</li> <li>Fonction PERCENTILE_CONT</li> </ul>	<p>Soutenu à la condition que les CTE utilisant des tables protégées par la confidentialité différentielle doivent aboutir à des données contenant des enregistrements au niveau de l'utilisateur. Vous devez écrire l'expression SELECT dans ces CTE en utilisant le `SELECT userIDentifierColumn...` format.</p>	<p>Agrégations prises en charge : AVG, COUNT, COUNT DISTINCT, STDDEV et SUM.</p>

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
	<ul style="list-style-type: none"> <li>Fonctions STDDEV_SAMP et STDDEV_POP</li> <li>Fonctions SUM et SUM DISTINCT</li> <li>Fonctions VAR_SAMP et VAR_POP</li> </ul>		
CTE	clause WITH, sous-requête de clause WITH	Soutenu à la condition que les CTE utilisant des tables protégées par la confidentialité différentielle doivent aboutir à des données contenant des enregistrements au niveau de l'utilisateur. Vous devez écrire l'expression SELECT dans ces CTE en utilisant le `SELECT userIdent ifierColu mn...'` format.	N/A
Sous-requêtes	Sous-requête de liste SELECT, sous-requête de clause FROM, sous-requête de clause WHERE	Non pris en charge. Les sous-requêtes de la requête qui font référence à une table dont la confidentialité différentielle est activée ne sont pas prises en charge. Réécrivez vos sous-requêtes sous forme d'expressions de table communes (CTE).	



Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
Clauses d'adhésion	<ul style="list-style-type: none"> <li>• JOINT INTÉRIEUR</li> <li>• JOINTURE GAUCHE</li> <li>• JOINTURE DROITE</li> <li>• ADHÉSION COMPLÈTE</li> <li>• [JOIN] OU opérateur</li> <li>• CROSS JOIN</li> </ul>	<p>Supportée à la condition que seules les fonctions JOIN 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.</p> <p>Les fonctions CROSS JOIN ne sont pas prises en charge lors de la combinaison de deux relations ou plus lorsque la confidentialité différentielle est activée.</p>	
Définir les opérateurs	UNION, UNION ALL, INTERSECT, EXCEPT   MINUS (ce sont des synonymes)	Tous sont pris en charge	Non pris en charge

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
Fonctions de fenêtrage	Fonctions d'agrégation <ul style="list-style-type: none"> <li>• Fonction de fenêtrage AVG</li> <li>• Fonction de fenêtrage COUNT</li> <li>• Fonction de fenêtrage CUME_DIST</li> <li>• Fonction de fenêtrage DENSE_RANK</li> <li>• Fonction de fenêtrage FIRST_VALUE</li> <li>• Fonction de fenêtrage LAG</li> <li>• Fonction de fenêtrage LAST_VALUE</li> <li>• Fonction de fenêtrage LEAD</li> <li>• Fonctions de fenêtrage MAX</li> <li>• Fonctions de la fenêtrage MEDIAN</li> <li>• Fonctions de la fenêtrage MIN</li> <li>• Fonction de fenêtrage NTH_VALUE</li> </ul>	Tous sont pris en charge à condition que la colonne d'identifiant utilisateur de la clause de partition de la fonction de fenêtrage soit requise lorsque vous interrogez une relation avec la confidentialité différentielle activée.	Non pris en charge

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
	<ul style="list-style-type: none"><li>• Fonction de fenêtrage RATIO_TO_REPORT</li><li>• Fonctions de fenêtrage STDDEV_SAMP et STDDEV_POP (STDDEV_SAMP et STDDEV sont des synonymes)</li><li>• Fonctions de la fenêtrage SUM</li><li>• Fonctions de fenêtrage VAR_SAMP et VAR_POP (VAR_SAMP et VARIANCE sont des synonymes)</li></ul>		
	<p>Fonctions de classement</p> <ul style="list-style-type: none"><li>• Fonction de fenêtrage DENSE_RANK</li><li>• Fonction de fenêtrage NTILE</li><li>• Fonction de fenêtrage PERCENT_RANK</li><li>• Fonction de fenêtrage RANK</li></ul>		

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
	<ul style="list-style-type: none"> <li>Fonction de fenêtrage ROW_NUMBER</li> </ul>		
Expressions conditionnelles	<ul style="list-style-type: none"> <li>Expression de condition CASE</li> <li>Expression COALESCE</li> <li>Fonctions GREATEST et LEAST</li> <li>Fonctions NVL et COALESCE</li> <li>Fonction NVL2</li> <li>Fonction NULLIF</li> </ul>	Tous sont pris en charge	Non pris en charge
Conditions	<ul style="list-style-type: none"> <li>Condition de comparaison</li> <li>Conditions logiques</li> <li>Conditions de correspondance de modèles</li> <li>ENTRE les conditions de gamme</li> <li>Condition null</li> </ul>	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	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
Fonctions date-heure	<ul style="list-style-type: none"> <li>• Fonctions date et heure dans les transactions</li> <li>• Opérateur de concaténation</li> <li>• Fonctions ADD_MONTHS</li> <li>• Fonction CONVERT_T IMEZONE</li> <li>• Fonction CURRENT_DATE</li> <li>• Fonction DATEADD</li> <li>• Fonction DATEDIFF</li> <li>• fonctions DATE_PART</li> <li>• Fonction DATE_TRUNC</li> <li>• Fonction EXTRACT</li> <li>• Fonction GETDATE</li> <li>• Fonctions TIMEOFDAY</li> <li>• Fonction TO_TIMESTAMP</li> <li>• Parties de date pour les fonctions de date ou d'horodatage</li> </ul>	Tous sont pris en charge	Tous sont pris en charge

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
Fonctions de chaîne	<ul style="list-style-type: none"> <li>• opérateur    (concaténation)</li> <li>• Fonction BTRIM</li> <li>• Fonction CHAR_LENGTH</li> <li>• Fonction CHARACTER_LENGTH</li> <li>• Fonction CHARINDEX</li> <li>• Fonction CONCAT</li> <li>• Fonctions LEFT et RIGHT</li> <li>• Fonction LEN</li> <li>• Fonction LENGTH</li> <li>• Fonction LOWER</li> <li>• Fonctions LPAD et RPAD</li> <li>• Fonction LTRIM</li> <li>• Fonctions POSITION</li> <li>• Fonction REGEXP_COUNT</li> <li>• Fonction REGEXP_INSTR</li> <li>• Fonction REGEXP_REPLACE</li> <li>• Fonction REGEXP_SUBSTR</li> </ul>	Tous sont pris en charge	Tous sont pris en charge

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
	<ul style="list-style-type: none"> <li>• Fonction REPEAT</li> <li>• Fonction REPLACE</li> <li>• Fonction REPLICATE</li> <li>• Fonction REVERSE</li> <li>• Fonction RTRIM</li> <li>• Fonction SOUNDEX</li> <li>• Fonction SPLIT_PART</li> <li>• Fonction STRPOS</li> <li>• Fonction SUBSTRING</li> <li>• Fonction TEXTLEN</li> <li>• Fonction TRANSLATE</li> <li>• Fonctions TRIM</li> <li>• Fonction UPPER</li> </ul>		
Fonctions de formatage des types de données	<ul style="list-style-type: none"> <li>• Fonction CAST</li> <li>• TO_CHAR</li> <li>• Fonction TO_DATE</li> <li>• TO_NUMBER</li> <li>• Chaînes de format datetime</li> <li>• Chaînes de format numériques</li> </ul>	Tous sont pris en charge	Tous sont pris en charge

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
Fonctions de hachage	<ul style="list-style-type: none"><li>• Fonction MD5</li><li>• Fonction SHA</li><li>• Fonction SHA1</li><li>• Fonction SHA2</li><li>• MURMUR3_32_HASH</li></ul>	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	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
Fonctions mathématiques	<ul style="list-style-type: none"> <li>• Fonction ABS</li> <li>• Fonction ACOS</li> <li>• Fonction ASIN</li> <li>• Fonction ATAN</li> <li>• Fonction ATAN2</li> <li>• Fonction CBRT</li> <li>• Fonction CEILING (ou CEIL)</li> <li>• Fonction COS</li> <li>• Fonction COT</li> <li>• Fonction DEGREES</li> <li>• Fonction DEXP</li> <li>• Fonction LTRIM</li> <li>• Fonction DLOG1</li> <li>• Fonction DLOG10</li> <li>• Fonction EXP</li> <li>• Fonction FLOOR</li> <li>• Fonction LN</li> <li>• Fonction LOG</li> <li>• Fonction MOD</li> <li>• Fonction PI</li> <li>• Fonction POWER</li> <li>• Fonction RADIANS</li> <li>• Fonction RANDOM</li> <li>• Fonction ROUND</li> <li>• Fonction SIGN</li> <li>• Fonction SIN</li> <li>• Fonctions SQRT</li> </ul>	Tous sont pris en charge	Tous sont pris en charge

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
	<ul style="list-style-type: none"> <li>Fonction TRUNC</li> </ul>		
Fonctions d'informations sur le type SUPER	<ul style="list-style-type: none"> <li>Fonction DECIMAL_P PRECISION</li> <li>Fonction DECIMAL_SCALE</li> <li>Fonction IS_ARRAY</li> <li>Fonction IS_BIGINT</li> <li>Fonction IS_CHAR</li> <li>Fonction IS_DECIMAL</li> <li>Fonction IS_FLOAT</li> <li>Fonction IS_INTEGER</li> <li>Fonction IS_OBJECT</li> <li>Fonction IS_SCALAR</li> <li>Fonction IS_SMALLINT</li> <li>Fonction IS_VARCHAR</li> <li>Fonction JSON_TYPEOF</li> </ul>	Tous sont pris en charge	Tous sont pris en charge

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
Fonctions VARBYTE	<ul style="list-style-type: none"> <li>Fonction FROM_HEX</li> <li>Fonction FROM_VARBYTE</li> <li>Fonction TO_HEX</li> <li>Fonction TO_VARBYTE</li> </ul>	Tous sont pris en charge	Tous sont pris en charge
JSON	<ul style="list-style-type: none"> <li>Fonction CAN_JSON_PARSE</li> <li>Fonction JSON_EXTRACT_ARRAY_ELEMENT_TEXT</li> <li>Fonction JSON_EXTRACT_PATH_TEXT</li> <li>Fonction JSON_PARSE</li> <li>Fonction JSON_SERIALIZE</li> <li>Fonction JSON_SERIALIZED_TO_VARBYTE</li> </ul>	Tous sont pris en charge	Tous sont pris en charge

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT finale
Fonctions de tableau	<ul style="list-style-type: none"> <li>• Fonction array</li> <li>• Fonction array_concat</li> <li>• Fonction array_flatten</li> <li>• Fonction get_array_length</li> <li>• Fonction split_to_array</li> <li>• Fonction subarray</li> </ul>	Non pris en charge	Non pris en charge
GRUPE PAR ÉTENDU	ENSEMBLES DE REGROUPEMENT, ROLLUP, CUBE	Non pris en charge	Non pris en charge
Opération de tri	ORDER BY	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	LIMITE, DÉCALAGE	Non pris en charge dans les CTE utilisant des tables protégées par la confidentialité différentielle	Tous sont pris en charge

Nom court	Constructions SQL	Expressions de table communes (CTE)	Clause SELECT 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 SQL non prises en charge

Catégorie	construction SQL	Autrement
Fonctions de fenêtrage	<ul style="list-style-type: none"> <li>• LISTAGG</li> <li>• PERCENTILE_CONT</li> <li>• PERCENTILE_DISC</li> </ul>	Vous pouvez utiliser la fonction d'agrégation équivalente avec GROUP BY.
Symboles d'opérateurs mathématiques	<ul style="list-style-type: none"> <li>• \$column   / 2</li> <li>• \$column  / 2</li> <li>• \$column ^ 2</li> </ul>	<ul style="list-style-type: none"> <li>• CBRT</li> <li>• SQRT</li> <li>• PUISSANCE (\$column, 2)</li> </ul>
Fonctions scalaires	<ul style="list-style-type: none"> <li>• SYSDATE</li> <li>• \$column : :entier</li> <li>• convertir (type, \$column)</li> </ul>	<ul style="list-style-type: none"> <li>• CURRENT_DATE</li> <li>• CAST \$column EN TANT QU'entier</li> <li>• CAST \$column, type AS</li> </ul>
Littéraux	INTERVALLE « 1 SECONDE »	INTERVALLE « 1 » SECONDE
Limitation des lignes	TOP n	LIMITE n

Catégorie	construction SQL	Autrement
Joindre	<ul style="list-style-type: none"><li>• USING</li><li>• NATURAL</li></ul>	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 constructions SQL, telles que les expressions de table communes (CTE) pour la préparation des données et les fonctions d'agrégation couramment utilisées telles que, ou. COUNT 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 à l'aide de CTE sur des données combinées. Comme son CTE utilise des tables protégées de confidentialité différentielles, l'annonceur inclut la colonne d'identifiant d'utilisateur de ces tables protégées dans la liste des colonnes CTE 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 règle pas 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. La confidentialité différentielle d'AWS Clean Rooms ne garantit pas la confidentialité différentielle lorsqu'une requête SQL peut entraîner un débordement ou des erreurs de diffusion non valides au moment de l'exécution en raison de l'utilisation de certaines constructions SQL. Le tableau suivant répertorie certaines constructions SQL, mais pas toutes, susceptibles de générer des erreurs d'exécution et qui doivent 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 constructions SQL suivantes sont vulnérables aux erreurs de débordement :

- Fonctions d'agrégation : AVG, LISTAVG, 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\_MONTHS, DATEADD, DATEDIFF
- Fonctions mathématiques - +, -, \*,/, POWER
- Fonctions de chaîne - ||, CONCAT, REPEAT, REPLICATE
- Fonctions de fenêtre : AVG, LISTAGG, PERCENTILE\_COUNT, PERCENTILE\_DISC, RATIO\_TO\_REPORT, SUM

La fonction de formatage du type de données CAST est vulnérable aux erreurs de conversion non valides.



# 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. La seconde partie introduit ensuite ses données de départ AWS Clean Rooms et génère un segment similaire qui ressemble aux données d'entraînement.

Pour une explication plus détaillée de son fonctionnement, voir [Emplois 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. 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.

Lors de l'utilisation de l'API, le terme modèle d'audience est utilisé de la même manière que modèle similaire. Par exemple, vous utilisez l'[CreateAudienceModel](#) API pour créer un modèle similaire.

- Segment similaire : sous-ensemble des données d'entraînement qui ressemble le plus aux données de départ.

Lorsque vous utilisez l'API, vous créez un segment similaire avec l'[StartAudienceGenerationJob](#) API.

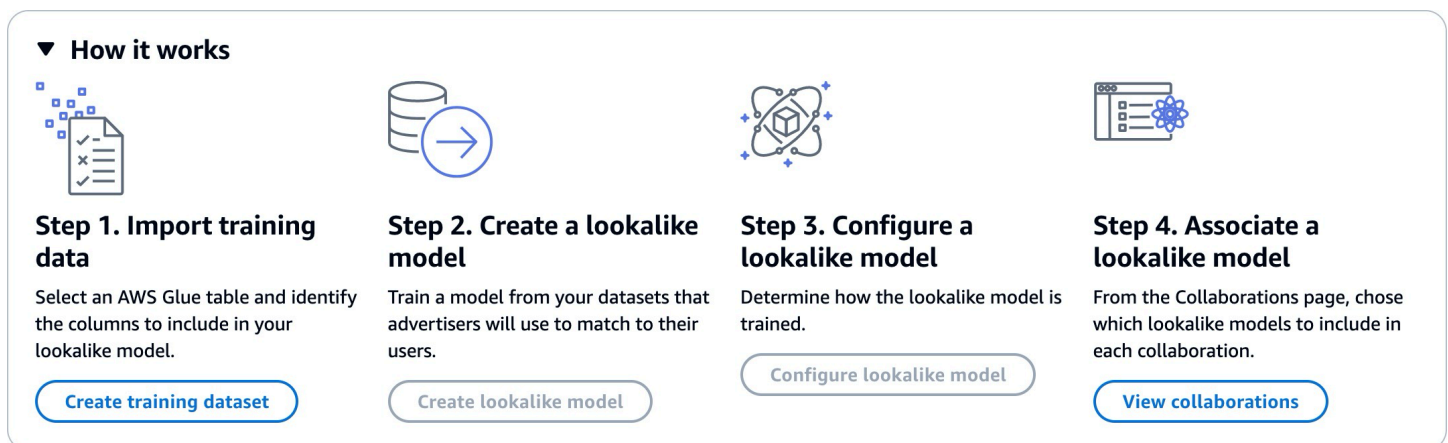
Les données du fournisseur de données de formation ne sont jamais partagées avec le fournisseur de données de départ et les données du fournisseur de données de départ ne sont jamais partagées avec le fournisseur de données de formation. La sortie du segment similaire est partagée avec le fournisseur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

Voici le flux de travail que le fournisseur de données de départ doit effectuer ensuite :

1. Les données du fournisseur de données de base doivent être stockées dans un compartiment Amazon S3.
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 démarrage n'observent pas directement les résultats de Clean Rooms ML et les fournisseurs de données de formation ne peuvent jamais observer les données d'amorçage. 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 au public initial. 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.

## 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 vont de 0 à 1, les valeurs les 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. Ainsi, lorsque la taille du segment augmente, il peut être moins similaire aux données de départ. 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, car ils sont influencés par de multiples facteurs complexes en plus de la pertinence, tels que la qualité des stocks, le type d'inventaire, le calendrier des publicités, etc.

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 le mois dernier. 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 \(fournisseur de données de départ\)](#)
- [Étapes suivantes](#)

## 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. Entrez un nom et une description facultative.
5. Pour Source de données, choisissez votre AWS Glue table :
  - a. Choisissez la base de données que vous souhaitez configurer dans la liste déroulante.
  - b. 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 vos données. 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.

7. Dans **Accès au service**, vous devez spécifier un rôle de service qui peut accéder à vos données et indiquer si vos données 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 chiffrées, entrez votre clé KMS dans le **AWS KMS keychamp** ou cliquez sur **Créer une AWS KMS key** pour générer une nouvelle clé KMS.

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

Pour l'action d'API correspondante, consultez [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.

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. Pour **Créer un modèle similaire**, pour les détails du modèle similaire :
  - a. Entrez un nom et une description facultative.
  - b. Choisissez le jeu de données d'entraînement que vous souhaitez modéliser dans la liste déroulante.
  - c. Entrez une fenêtre d'entraînement facultative.
5. Si vous souhaitez activer les paramètres de chiffrement personnalisés pour le modèle similaire, choisissez **Personnaliser les paramètres de chiffrement**, puis entrez la clé KMS.

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.

Pour l'action d'API correspondante, consultez [CreateAudienceModel](#).

## Configuration d'un modèle similaire

Une fois que vous avez 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. Pour Configurer le modèle similaire, pour les détails du modèle similaire configuré :
  - a. Entrez un nom et une 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.
7. Pour l'accès au service, choisissez le nom du rôle de service existant qui sera utilisé pour accéder à cette table.
8. Choisissez Configurer le modèle similaire.
9. Si vous souhaitez activer les balises pour la ressource de table configurée, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.



Pour l'action d'API correspondante, consultez [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, choisissez Associate lookalike model.
5. Pour le modèle similaire configuré par Associate, pour les détails du modèle similaire Associate :
  - 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'action d'API correspondante, consultez [CreateConfiguredAudienceModelAssociation](#).

## 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. Pour Créer un segment similaire, pour les détails du segment similaire, entrez un nom et une description facultative.
6. Pour les profils de départ, choisissez la source d'entrée Amazon S3 dans laquelle vos données de départ sont stockées.
7. Pour l'accès au service, choisissez le nom du rôle de service existant qui sera utilisé pour accéder à cette table.
8. Si vous souhaitez activer les balises pour le jeu de données d'entraînement, choisissez Ajouter une nouvelle balise, puis entrez la paire clé/valeur.
9. Choisissez Créer un segment similaire.

Pour l'action d'API correspondante, consultez [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, 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'action d'API correspondante, consultez [StartAudienceExportJob](#).

## Étapes suivantes

Maintenant que vous avez créé un modèle similaire et exporté un segment de départ, vous êtes prêt à :

- [Gérer AWS Clean Rooms](#)

# Informatique cryptographique pour Clean Rooms

Informatique cryptographique pour Clean Rooms (C3R) est une capacité dans AWS Clean Rooms qui peut être utilisée en complément de [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 [crypter](#) vos données à utiliser avec AWS Clean Rooms. Lorsque vous utilisez le client de chiffrement C3R, les données restent protégées cryptographiquement lorsqu'elles sont utilisées dans un AWS Clean Rooms collaboration. Comme un habitué AWS Clean Rooms collaboration, 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 langage SQL `JOIN` et `SELECT` déclarations 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 :

- Colonne protégées par cryptographie pour une utilisation dans `JOIN` les déclarations sont appelées `fingerprint` colonnes.
- Colonne protégées par cryptographie pour une utilisation dans `SELECT` les déclarations sont appelées `sealed` colonnes.
- Colonne qui ne sont pas protégées par cryptographie pour être utilisées dans `JOIN` ou `SELECT` les déclarations sont appelées `clear text` colonnes.

Dans certains cas, `GROUP BY` les déclarations sont prises en charge sur `fingerprint` colonnes. Pour plus d'informations, veuillez consulter [Fingerprint colonnes](#). Actuellement, C3R ne prend pas en charge l'utilisation d'autres constructions SQL sur des données chiffrées, telles que `WHERE` des clauses ou des fonctions agrégées telles que `SUM` et `AVERAGE`, même s'ils seraient autrement autorisés 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 pendant que le

contenu est utilisé dans AWS Clean Rooms. C3R utilise le cryptage AES-GCM standard pour tous les données et une fonction pseudo-aléatoire standard de l'industrie, connue sous le nom de code d'authentification de message utilisant hash (HMAC) pour protéger les données.

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 cryptées 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 C3R, consultez les rubriques suivantes.

#### Rubriques

- [Considérations relatives à l'utilisation de l'informatique cryptographique pour Clean Rooms](#)
- [Types de fichiers et de données pris en charge dans Cryptographic Computing pour Clean Rooms](#)
- [Noms de colonnes dans Cryptographic Computing pour Clean Rooms](#)
- [Types de colonnes dans le calcul cryptographique pour Clean Rooms](#)
- [Paramètres de calcul cryptographique](#)
- [Indicateurs facultatifs dans l'informatique cryptographique pour Clean Rooms](#)
- [Requêtes avec informatique cryptographique pour Clean Rooms](#)
- [Directives relatives au client de chiffrement C3R](#)

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

L'informatique cryptographique pour Clean Rooms (C3R) vise à optimiser la protection des données. Toutefois, certains cas d'utilisation peuvent bénéficier de niveaux de protection des données inférieurs 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 mélangéescleartext et cryptées dans vos tableaux](#)
- [Autoriser les valeurs répétées dansfingerprint les colonnes](#)
- [Assouplissement des restrictions relatives au nom desfingerprint colonnes](#)
- [Déterminer commentNULL les valeurs sont représentées](#)

Pour de plus amples informations sur la configuration des paramètres pour ces scénarios, consultez[Paramètres de calcul cryptographique](#).

## Autoriser les données mélangéescleartext et cryptées dans vos tableaux

Le chiffrement de toutes les données côté client garantit une protection maximale des données. Toutefois, cela limite certains types de requêtes (par exemple, la fonction d'SUMagrégation). Le risque lié à l'autorisation descleartext 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 sur les donnéescleartext et les données associées.

Par exemple, imaginez que vous aviez les colonnes deCity etState. LaCity colonne est cryptéecleartext et laState colonne est cryptée. Lorsque vous voyez la valeurChicago dans laCity colonne, cela vous aide à déterminer avec une forte probabilité que la valeurState estIllinois. En revanche, si une colonne l'estCity et l'autre l'estEmailAddress, ilcleartextCity est peu probable que a révèle quoi que ce soit sur une colonne cryptéeEmailAddress.

Pour de plus amples informations sur le paramètre de ce scénario, consultez[Paramètre Autorisercleartext les colonnes](#).

## Autoriser les valeurs répétées dansfingerprint les colonnes

Pour l'approche la plus sûre, nous supposons que chaquefingerprint colonne contient exactement une instance de variable. Aucun élément ne peut être répété dans unefingerprint colonne. Le client de chiffrement C3R mappe cescleartext valeurs en valeurs uniques impossibles à distinguer des valeurs aléatoires. Par conséquent, il est impossible de déduire des informations sur lecleartext à partir de ces valeurs aléatoires.

Le risque de valeurs répétées dans une fingerprint colonne est que des valeurs répétées se traduisent par des valeurs aléatoires répétées. Ainsi, toute personne ayant accès aux tables cryptées pourrait, en théorie, effectuer une analyse statistique des fingerprint colonnes susceptible de révéler des informations sur le texte des 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` très probable. Cette inférence est possible car `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 de plus amples informations sur le paramètre de ce scénario, consultez [Paramètre Autoriser les doublons](#).

## Assouplissement des restrictions relatives au nom des fingerprint colonnes

Par défaut, nous supposons que lorsque deux tables sont jointes à l'aide de fingerprint colonnes cryptées, 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 crypter 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 avec des noms de colonne différents, nous dérivons des clés différentes et nous ne pouvons pas calculer de jointure valide.

Pour résoudre ce problème, vous pouvez désactiver la fonctionnalité qui dérive 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 susceptible de révéler des informations puisse être effectué.

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

Pour de plus amples informations sur le paramètre de ce scénario, consultez [Paramètre Autorisation JOIN 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 n'importe quelle autre valeur. Si vous ne traitez pas NULL les valeurs comme n'importe quelle autre valeur, des informations peuvent être révélées.

Par exemple, supposons que NULL la Middle Name colonne du cleartext indique des personnes sans deuxième prénom. Si vous ne cryptez pas ces valeurs, vous divulguez les lignes de la table cryptée qui sont utilisées pour les personnes sans deuxième prénom. Cette information peut constituer un signal d'identification pour certaines personnes de certaines populations. Mais si vous traitez des NULL valeurs de manière cryptographique, certaines requêtes SQL agissent différemment. Par exemple, GROUP BY les clauses ne regroupent pas fingerprint NULL les valeurs dans fingerprint des colonnes.

Pour de plus amples informations sur le paramètre de ce scénario, consultez [Paramètre de préservation 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
- Parquet fichiers

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](#)
- [Parquet fichiers](#)
- [Chiffrement de valeurs autres que des chaînes](#)



## fichiers CSV

Un fichier avec 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`.

### NULL Encodage 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 en utilisant 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.

<b>&lt;csv-input-null&gt;</b>	<b>&lt;csv-output-null&gt;</b>	Entrée d'entrée	Entrée de sortie
None	None	,AnyProduct,	,AnyProduct,
None	None	, AnyProduct ,	,AnyProduct,
None	None	,"AnyProduct",	,AnyProduct,
None	None	, "AnyProdu ct" ,	,AnyProduct,
None	None	,,	,,
None	None	, ,	,,
None	None	, "",	,,
None	None	, " ",	, " ",
None	None	, " " ,	, " ",
"AnyProduct"	« NUL »	,AnyProduct,	, NUL,
"AnyProduct"	« NUL »	, AnyProduct ,	, NUL,
"AnyProduct"	« NUL »	,"AnyProduct",	, NUL,
"AnyProduct"	« NUL »	, "AnyProdu ct" ,	, NUL,
None	« NUL »	,,	, NUL,

<b>&lt;csv-input-null&gt;</b>	<b>&lt;csv-output-null&gt;</b>	Entrée d'entrée	Entrée de sortie
None	« NUL »	, ,	, NUL,
None	« NUL »	, "",	, NUL,
None	« NUL »	, " ",	, " ",
None	« NUL »	, " " ,	, " " ,
""	« NUL »	,,	, NUL,
""	« NUL »	, ,	, NUL,
""	« NUL »	, "",	, "",
""	« NUL »	, " ",	, " ",
""	« NUL »	, " " ,	, " " ,
"\""	« NUL »	,,	,,
"\""	« NUL »	, ,	,,
"\""	« NUL »	, "",	, NUL,
"\""	« NUL »	, " ",	, " ",
"\""	« NUL »	, " " ,	, " " ,

## Fichier CSV sans en-têtes

Le fichier .csv source n'a pas besoin d'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, consultez [Schémas 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 :

- Binarytype 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)
- Booleantype de données primitif sans annotation logique (type de BOOLEAN données)
- Doubletype 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)
- Floattype de données primitif sans annotation logique (type de FLOAT données)
- Int32type 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)
- Int64type 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 SMALLINT, ouBIGINT. De plus, la INTEGRAL valeur ne 0 correspondra jamais à la BOOLEAN valeur FALSE (qui est représentée par la valeur0).

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 le calcul cryptographique pour Clean Rooms.

Si la valeur du paramètre `AutoriserJOINde colonnes` portant des noms différents est faux, les noms de colonnes sont utilisés lors du chiffrement de fingerprint colonnes. C'est pourquoi, par défaut, les collaborateurs doivent se coordonner à l'avance et utiliser les mêmes noms de colonne cible pour les données qui utiliseront JOIN déclarations dans les requêtes. Par défaut, les colonnes sont cryptées pour JOIN avec des noms différents ne fonctionnent pas JOIN sur n'importe quelle valeur.

Si la valeur du paramètre `AutoriserJOINde colonnes` portant des noms différents est vrai, JOIN déclarations sur plusieurs colonnes cryptées en tant que fingerprint les colonnes se succèdent. Le chiffrement des données à l'aide de ce paramètre peut permettre de déduire cleartext valeurs. Par exemple, si une ligne possède la même valeur de code d'authentification des messages basé sur le hachage (HMAC) dans les deux `City` colonne et `State` colonne, la valeur peut être `New York`.

## Normalisation des noms d'en-têtes de colonne

Les noms des en-têtes de colonne sont normalisés par le client de chiffrement C3R. Tous les espaces blancs de début et de fin sont supprimés et le nom de 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 for Clean Rooms.

### Rubriques

- [Fingerprint colonnes](#)
- [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 du cleartext. 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 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 souhaitez 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 informatiques cryptographiques 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 laAWS Clean Rooms console ou de l'opérationCreateCollaboration API. Dans la console, vous pouvez définir des valeurs pour les paramètres dans Paramètres de calcul cryptographique après avoir activé l'option Prise en Support du calcul cryptographique. Pour plus d'informations, consultez les rubriques suivantes.

### Rubriques

- [Paramètre Autorisercleartext les colonnes](#)
- [Paramètre Autoriser les doublons](#)
- [Paramètre AutorisationJOIN des colonnes avec des noms différents](#)
- [Paramètre de préservationNULL des valeurs](#)

## Paramètre Autorisercleartext les colonnes

Dans la console, vous pouvez définir le paramètre Autoriser lescleartext colonnes lors de la [création d'une collaboration](#) afin de spécifier si cleartext les données sont autorisées dans une table contenant des données cryptées.

Le tableau suivant décrit les valeurs du paramètre cleartextAllow columns.

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
	<p>Cleartextles colonnes ne sont pas protégées par cryptographie et sont incluses en tant quecleartext. Vous devez prendre note de ce que lescleartext données de vos lignes peuvent révéler à propos des autres données du tableau.</p> <p>Pour fonctionnerSUM ouAVG sur des colonnes spécifiques, les colonnes doivent se trouver danscleartext.</p>

À l'aide de l'opération d'CreateCollaborationAPI, pour ledataEncryptionMetadata paramètre, vous pouvez définir la valeurallowCleartext de true ou false. Pour de plus amples informations sur les opérations de l'[AWS Clean RoomsAPI](#), consultez [Référence d'API](#).

Cleartextles colonnes correspondent aux colonnes qui sont classées seloncleartext le schéma spécifique 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 que ne le permet unesealed colonne ou unefingerprint 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 cryptées pour lesJOIN requêtes peuvent contenir desNULL non-valeurs dupliquées.

### Important

Les paramètres Autoriser les doublons, [AutoriserJOIN les colonnes portant des noms différents](#) et [Préserver lesNULL 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 fingerprint colonne doivent être uniques.
Oui	<p>Les valeurs répétées sont autorisées dans une fingerprint colonne.</p> <p>Si vous devez joindre des colonnes contenant des valeurs répétées, définissez cette valeur sur Oui. Lorsque ce paramètre est défini sur Oui, les modèles de fréquence apparaissant dans les fingerprint colonnes du tableau C3R ou des résultats peuvent impliquer des informations supplémentaires sur la structure des données.</p>

À l'aide de l'opération `CreateCollaborationAPI`, vous pouvez définir la valeur du paramètre `allowDuplicates` à `true` ou `false`. Pour de plus amples informations sur les opérations de l'[AWS Clean Rooms API](#), consultez [Référence d'API](#).


Par défaut, si des données cryptées 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 cryptées dans des JOIN requêtes sans craindre les doublons, le paramètre Autoriser les doublons peut désactiver cette vérification prudente.

## Paramètre Autorisation JOIN 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 de plus amples informations, consultez [Normalisation des noms d'en-têtes de colonne](#).

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

Valeur de paramètre	Description
Non	<p>Les jointures defingerprint colonnes portant des noms différents ne sont pas prises en charge. JOIN les instructions fournissent des résultats précis uniquement sur les colonnes portant le même nom.</p> <div data-bbox="609 472 1507 1071" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> <b>Important</b></p><p>La valeur Non renforce la sécurité des informations mais nécessite que les participants à la collaboration se mettent d'accord au préalable sur les noms des colonnes. Si deux colonnes ont des noms différents lorsqu'elles sont cryptées en tant que fingerprint colonnes et que JOIN l'option Autoriser les colonnes portant des noms différents est définie sur Non, JOIN les instructions relatives à ces colonnes ne produisent aucun résultat. Cela est dû au fait qu'aucune valeur n'est partagée entre eux après le chiffrement.</p></div>
Oui	<p>Les jointures defingerprint 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 leur nom de colonne.</p> <p>Si ce paramètre est défini sur Oui, le client de chiffrement C3R ne prend pas en compte le nom de la colonne lors de la protection fingerprint des colonnes. Par conséquent, des valeurs communes aux différentes fingerprint colonnes sont observables dans la table C3R.</p> <p>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 c'est le cas New York.</p>

À l'aide de l'opération `CreateCollaborationAPI`, pour le paramètre `dataEncryptionMetadata`, vous pouvez définir la valeur `allowJoinsOnColumnsWithDifferentNames` de `true` ou `false`. Pour de plus amples informations sur les opérations de l'[AWS Clean Rooms API](#), consultez [Référence d'API](#).

Par défaut, le chiffrement des colonnes est affecté par le paramètre `targetHeader` pour cette colonne, défini dans [Étape 4 : générer un schéma de chiffrement pour un fichier tabulaire](#). Par conséquent, la même valeur possède des représentations cryptées différentes dans chaque colonne pour laquelle elle est chiffrée.

Ce paramètre peut être utile pour empêcher l'inférence de valeurs dans certains cas. Par exemple, le fait de voir la même valeur cryptée dans les colonnes `City` et `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 aient des noms communs.

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

## Paramètre de préservation NULL des valeurs

Dans la console, vous pouvez définir le paramètre `PreserveNULL` les valeurs lors de la [création d'une collaboration](#) afin d'indiquer qu'aucune valeur n'est présente pour cette colonne.

Le tableau suivant décrit les valeurs du paramètre `PreserveNULL values`.

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

Valeur de paramètre	Description
	soit cryptée ou non et quel que soit le paramètre défini pour Autoriser les doublons.

À l'aide de l'opération `CreateCollaborationAPI`, pour le paramètre `dataEncryptionMetadata`, vous pouvez définir la valeur `preserveNulls` sur `true` ou `false`. Pour de plus amples informations sur les opérations de l'[AWS Clean Rooms API](#), consultez [Référence d'API](#).

Lorsque le paramètre `PreserveNULL values` est défini sur `Non` pour la collaboration :

1. Les entrées dans les colonnes `clearText` restent inchangées.
2. Les entrées des colonnes `fingerprint` cryptées sont cryptées sous forme de valeurs aléatoires afin de masquer leur contenu. La jointure d'une colonne cryptée avec des entrées `NULL` dans la colonne `clearText` ne produit aucune correspondance pour aucune des entrées `NULL`. Aucune correspondance n'est établie car chacun reçoit son propre contenu aléatoire unique.
3. Les entrées des colonnes cryptées `sealed` sont cryptées.

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

Le paramètre `Préserver les valeurs NULL` est utile dans des scénarios tels que l'enrichissement de données, dans lesquels vous souhaitez partager un manque d'informations exprimé sous forme de `NULL`. Le paramètre `PreserveNULL values` est également utile au format `fingerprint HMAC` si vous avez des valeurs `NULL` dans la colonne que vous souhaitez `JOIN` ou `GROUP BY`.

Si la valeur des paramètres `Autoriser les doublons` et `Préserver les valeurs NULL` est définie sur `Non`, la présence de plusieurs entrées `NULL` dans une colonne `fingerprint` 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.

## Indicateurs facultatifs dans l'informatique cryptographique pour Clean Rooms

Les sections suivantes décrivent les indicateurs facultatifs que vous pouvez définir lorsque vous [chiffrez des données](#) à l'aide du client de chiffrement C3R à des fins de personnalisation et de test de fichiers tabulaires.

## Rubriques

- [--csvInputNULLValuedrapeau](#)
- [--csvOutputNULLValuedrapeau](#)
- [--enableStackTracesdrapeau](#)
- [--dryRundrapeau](#)
- [--tempDir](#)

### -- csvInputNULLValuedrapeau

Vous pouvez utiliser l'`--csvInputNULLValue`indicateur pour spécifier des codages personnalisés pour lesNULL entrées des 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 pourNULL les entrées des données d'entrée.	Codage desNULL valeurs spécifié par l'utilisateur dans le fichier CSV d'entrée

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

### -- csvOutputNULLValuedrapeau

Vous pouvez utiliser l'`--csvOutputNULLValue`indicateur pour spécifier des codages personnalisés pour lesNULL entrées des 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 codages personnalisés dans le fichier de sortie généré pour les NULL entrées.	Codage des NULL valeurs spécifié par l'utilisateur dans le fichier CSV de sortie

Une NULL entrée est une entrée considérée comme dépourvue de contenu, en particulier dans le contexte d'un format tabulaire plus riche tel qu'un tableau SQL. Bien que le fichier .csv ne prenne pas explicitement en charge cette caractérisation pour des raisons historiques, il est courant de considérer qu'une entrée vide ne contenant que 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.

## --enableStackTracesdrapeau

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 la trace de pile pour la résoudre vous-même ou envoyez la trace de pile 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 pour le signalement d'erreurs lorsque le client de chiffrement C3R rencontre une erreur.	Aucune

## --dryRun drapeau

Les commandes client de [chiffrement](#) et de déchiffrement C3R incluent un `--dryRun` indicateur facultatif. L'indicateur prend tous les arguments fournis par l'utilisateur et en vérifie la validité et la cohérence.



Vous pouvez utiliser l'option `--dryRun` 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. Permet au client de chiffrement C3R d'analyser les paramètres et de vérifier les fichiers, mais n'effectue aucun chiffrement ni déchiffrement.	Aucune

## `--tempDir` drapeau

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

Lorsque vous [chiffrez des données](#) à l'aide de C3R, utilisez l'option `--tempDir` 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.	La valeur par défaut est le répertoire temporaire du système.

## Requêtes avec informatique cryptographique pour Clean Rooms

Cette rubrique fournit des informations sur l'écriture de requêtes utilisant des tables de données chiffrées à l'aide du chiffrement pour Clean Rooms.

### Rubriques

- [Requêtes qui se ramifient sur NULL](#)
- [Mappage d'une colonne source à plusieurs colonnes cibles](#)

- [Utiliser les mêmes données pour JOIN les deux SELECT requêtes](#)

## Requêtes qui se ramifient sur NULL

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

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

Les requêtes peuvent se baser sur NULL des instructions contenues dans un fingerprint des colonnes et des colonnes uniquement lorsque la valeur du paramètre `Preserve NULL values` (`preserveNulls`) est définie sur `true`.

Les requêtes qui ne respectent pas ces contraintes peuvent donner des résultats incorrects.

## Mappage d'une colonne source à plusieurs colonnes cibles

Une colonne source peut correspondre à plusieurs colonnes cibles. Par exemple, vous souhaitez peut-être les deux `JOIN` et `SELECT` sur une colonne.

Pour plus d'informations, veuillez consulter [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 en clair cible, ce qui permet de les utiliser à toutes fins.

Si les données d'une colonne sont sensibles et doivent être utilisées à la fois pour des `SELECT` requêtes `JOIN` et, mappez cette colonne source à deux colonnes cibles dans le fichier de sortie. Une colonne est cryptée avec le type en tant que fingerprint de colonne, et une colonne est cryptée avec le type en tant que colonne scellée. La génération de schémas interactifs du client de chiffrement C3R suggère des suffixes d'en-tête de `_fingerprint` et `_sealed`. Ces suffixes d'en-tête peuvent constituer une convention utile pour différencier rapidement de telles colonnes.

## Directives relatives au 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 conservant 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 différentes garanties cryptographiques. Les paramètres de collaboration sont les plus sécurisés par défaut. L'ajout de fonctionnalités supplémentaires lors de la création d'une collaboration affaiblit les garanties de confidentialité, permettant ainsi d'effectuer des activités telles que l'analyse des fréquences sur le texte chiffré. Pour plus d'informations sur la façon dont ces paramètres sont utilisés et leurs implications, consultez [Informatique cryptographique](#).

## Rubriques

- [Implications sur les performances pour les types de colonnes](#)
- [Résolution des problèmes liés à l'augmentation imprévue 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 et 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.

## Fingerprint colonnes

Fingerprintles colonnes sont destinées à être utilisées pour joindre des données entre 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 un impact variable sur la taille du fichier de sortie en fonction du texte contenu de l'entrée.

### Rubriques

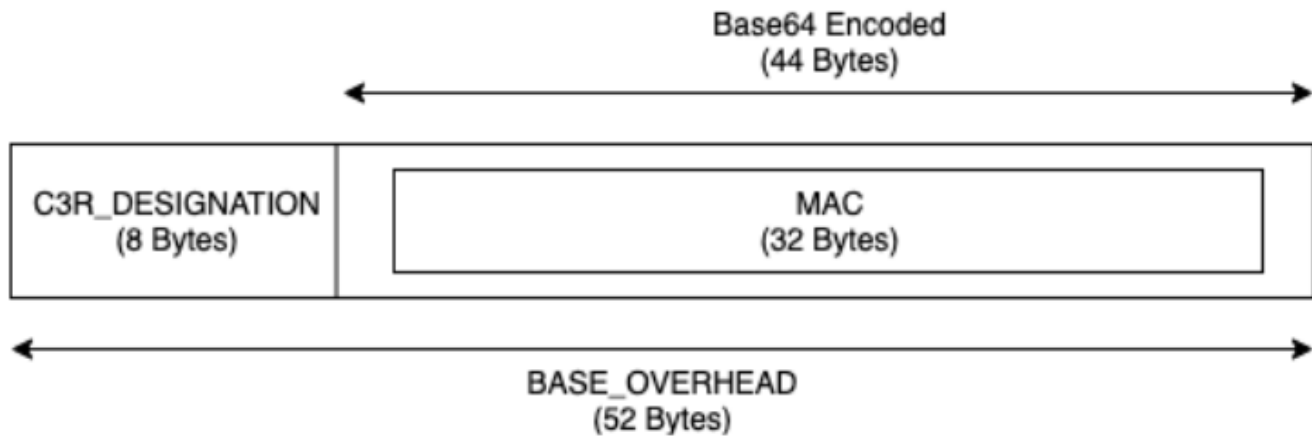
- [Surplomb de base pour les fingerprint colonnes](#)
- [Paramètres de collaboration pour les fingerprint colonnes](#)
- [Exemple de données pour une fingerprint colonne](#)
- [fingerprintColonnes de dépannage](#)

### Surplomb de base pour les fingerprint colonnes

Il existe un plafond de base pour les fingerprint colonnes. Cette surcharge est constante et ne dépend pas de la taille des octets.

Les données des fingerprint colonnes sont traitées de manière cryptographique par le biais d'une fonction HMAC (code d'authentification des messages basé sur le hachage), qui transforme les données en un code d'authentification des messages (MAC) de 32 octets. Ces données sont ensuite traitées par 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 auquel appartiennent les données et la version client qui les a produites. Le résultat final est de 52 octets. Ce résultat est ensuite multiplié par le nombre de lignes pour obtenir la surcharge de base totale (utilisez le nombre total de lignes non-valeurs si `preserveNulls` est défini sur `vrai`).

L'image suivante montre comment  $BASE\_OVERHEAD = C3R\_DESIGNATION + (MAC * 1.33)$



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

Paramètres de collaboration pour les fingerprint colonnes

### Paramètre `preserveNulls`

Lorsque le paramètre de niveau de collaboration `preserveNulls` est défini sur `false` (par défaut), chaque valeur est remplacée par 32 octets aléatoires uniques et traitée comme si ce n'était pas le cas. Il en résulte que chaque valeur est désormais de 52 octets. Cela peut ajouter des exigences de stockage importantes pour les tables contenant des données très éparpillées par rapport à ce qui se passe lorsque ce paramètre est défini sur `true` et que les valeurs sont transmises sous forme de `null`.

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

Exemple de données pour une fingerprint colonne

Voici un exemple d'ensemble de données d'entrée et de sortie pour une fingerprint colonne avec des paramètres à reproduire. Les autres paramètres de collaboration, tels que `allowClearText` les résultats, `allowDuplicates` n'ont aucune incidence sur les résultats et peuvent être définis au fur et à mesure de la reproduction locale.

Exemple de secret partagé :wJa1rXUtnFEMI/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 présentées dans les tableaux suivants.

#### Exemple 1

Entrée	null
<code>preserveNulls</code>	TRUE
Sortie	null
Déterministe	Yes
Octets d'entrée	0
Octets de sortie	0

#### Exemple 2

Entrée	null
<code>preserveNulls</code>	FALSE
Sortie	01:hmac:31kFjthvV3IUu6mMvFc1a+XAHwgw/E1m0q4p3Yg25kk=
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	abcdefghijklmnopqrstuvwxy
preserveNulls	-
Sortie	01: hmac: kU/IqwG7FMmzzshr0B9 scomE0UJUEE7j9keTctp1Gww=
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 `textclear` qui y est entré ?

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 celui de `clear` qui y est entré ?

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

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

Malheureusement, la réponse est que cela dépend. Au minimum, vous [the section called "Paramètres"](#) devez vérifier la manière dont le `preserveNulls` paramètre protège vos données. Nous vous recommandons toutefois de vous référer aux exigences de votre organisation en matière de traitement des données et à tout contrat applicable à la collaboration respective.

Pourquoi dois-je supporter la surcharge de Base64 ?

Pour assurer la compatibilité avec les formats de fichiers tabulaires tels que CSV, le codage en 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 pour 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

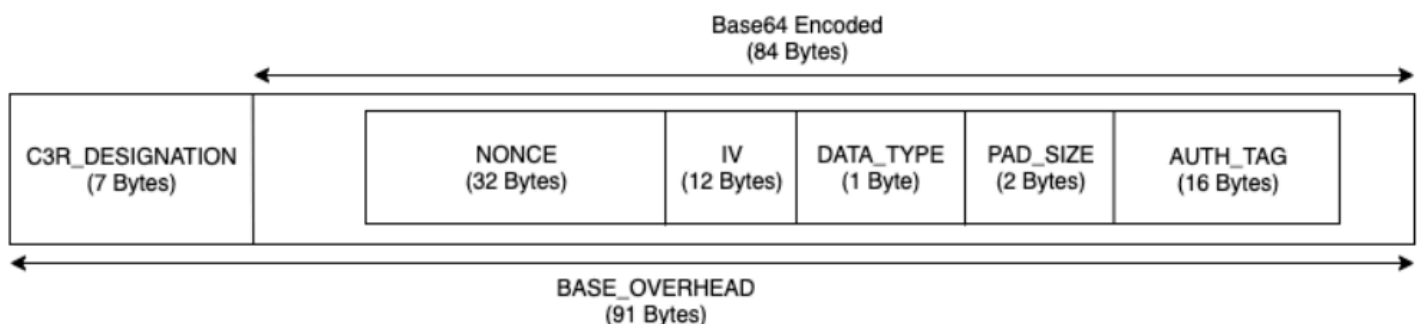
- [Surplomb de base pour lessealed colonnes](#)
- [Paramètres de collaboration pour lessealed colonnes](#)
- [sealedColonnes des paramètres du schéma : types de remplissage](#)
- [Exemple de données pour unesealed colonne](#)
- [sealedColonnes de dépannage](#)

## Surplomb de base pour lessealed colonnes

Il existe un plafond de base pour lessealed colonnes. Cette surcharge est constante et s'ajoute à la taille des octetsclartext et du remplissage (le cas échéant).

Avant tout chiffrement, les données dessealed colonnes sont précédées d'un caractère d'un octet désignant le type de données contenues. Si le remplissage 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 avecIV (12 octets),nonce (32 octets) etAuth Tag (16 octets). Ces données sont ensuite traitées par un encodeur base64, ce qui ajoute environ 33 % à la taille des octets. Les données sont précédées d'une désignation C3R à 7 octets pour désigner le type de colonne auquel les données appartiennent et la version client utilisée pour les produire. Le résultat est une surcharge de base finale de 91 octets. Ce résultat peut ensuite être multiplié par le nombre de lignes pour obtenir la surcharge de base totale (utilisez le nombre total de valeurs non nulles s'ilpreserveNulls est défini sur true).

L'image suivante vous montre comment le faire  $BASE\_OVERHEAD = C3R\_DESIGNATION + ((NONCE + IV + DATA\_TYPE + PAD\_SIZE + AUTH\_TAG) * 1.33)$



## Paramètres de collaboration pour lessealed colonnes

### Paramètre **preserveNulls**

Lorsque le paramètre de niveau de collaboration `preserveNulls` est défini sur `false` (par défaut), chaque `null` valeur est unique, aléatoire, de 32 octets et traitée comme si elle ne l'était pas `null`. Le résultat est que chaque `null` valeur est désormais de 91 octets (plus si elle est remplie). Cela peut ajouter des exigences de stockage importantes pour les tables contenant des données très éparses par rapport à ce qui se passe lorsque ce paramètre est défini `true` et que `null` les valeurs sont transmises sous forme de `null`.

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

sealedColonnes des paramètres du schéma : types de remplissage

### Rubriques

- [Type de tamponnone](#)
- [Type de tamponfixed](#)
- [Type de tamponmax](#)

### Type de tampon**none**

La sélection d'un type de coussin `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 ne fournit pas les mêmes garanties de confidentialité que `fixed` les types de `max` rembourrage. Cela est dû au fait que la taille du sous-jacent `cleartext` est discernable de la taille du texte chiffré.

### Type de tampon**fixed**

La sélection d'un type de `padfixed` est une mesure de préservation de la confidentialité qui permet de masquer la longueur des données contenues dans une colonne. Cela se fait en ajoutant tous les éléments `cleartext` fournis `pad_length` avant qu'ils ne soient cryptés. Toute donnée dépassant cette taille entraîne l'échec du client de chiffrement C3R.

Étant donné que le remplissage est ajouté avant d'être crypté, AES-GCM dispose d'un mappage 1 octet de texte clair à 1 octet de texte chiffré. L'encodage base64 ajoutera 33 %. La charge de stockage supplémentaire du rembourrage peut être calculée en soustrayant la longueur moyenne du texte clair de la valeur `pad_length` et en la multipliant par 1,33. Le résultat est la surcharge moyenne de remplissage par enregistrement. Ce résultat peut ensuite être multiplié par le nombre de lignes pour obtenir la surcharge totale de remplissage (utilisez le nombre total de lignes non-valeurs nulles si `preserveNulls` est défini 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 plus grande valeur 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'ajoute aucune surcharge de calcul significative.

### Type de tampon `max`

La sélection d'un type de `pad_max` est une mesure de préservation de la confidentialité qui permet de masquer la longueur des données contenues dans une colonne. Pour ce faire, ajoutez toutes les valeurs de texte clair à la valeur la plus élevée de la colonne, plus la valeur supplémentaire, `pad_length`, avant qu'elle ne soit cryptée. En général, le `max` remplissage fournit les mêmes garanties que le `fixed` remplissage pour un seul ensemble de données, tout en permettant de ne pas connaître la plus grande valeur de texte clair de la colonne. Toutefois, 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 différents ensembles de données peut être différente.

Nous vous recommandons de sélectionner une valeur supplémentaire `pad_length` de 0 lorsque vous utilisez le `max` rembourrage. Cette longueur complète toutes les valeurs de manière à ce qu'elles aient 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 valeur de texte clair la plus élevée est connue pour une colonne donnée, nous vous recommandons d'utiliser plutôt le type `fixed pad`. L'utilisation du `fixed` du remplissage crée une cohérence entre les ensembles de données mis à jour. L'utilisation du `max` remplissage permet de compléter chaque sous-ensemble de données à la valeur la plus élevée qui se trouvait dans le sous-ensemble.

## Exemple de données pour unesealed colonne

Voici un exemple d'ensemble de données d'entrée et de sortie pour unesealed colonne avec des paramètres à reproduire. Les autres paramètres de collaborationallowCleartext, tels que, etallowJoinsOnColumnsWithDifferentNames,allowDuplicates n'ont aucune incidence sur les résultats et peuvent être définis au fur et à mesure de la reproduction localetrue oufalse si vous essayez de le faire. Bien qu'il s'agisse des paramètres de base à reproduire, lasealed colonne n'est pas déterministe et les valeurs changent à chaque fois. L'objectif est de montrer les octets entrants par rapport aux octets sortants. Lespad\_length valeurs d'exemple ont été choisies intentionnellement. Ils montrent que lefixed rembourrage donne les mêmes valeurs que lemax rembourrage avec lepad\_length paramètres minimaux recommandés ou lorsqu'un rembourrage supplémentaire est souhaité.

Exemple de secret partagé :wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

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

## Rubriques

- [Type de tamponnone](#)
- [Type de tamponfixed \(exemple 1\)](#)
- [Type de tamponfixed \(exemple 2\)](#)
- [Type de tamponmax \(exemple 1\)](#)
- [Type de tamponmax \(exemple 2\)](#)

## Type de tamponnone

### Exemple 1

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

## Exemple 2

Entrée	<code>null</code>
<code>preserveNulls</code>	<code>FALSE</code>
Sortie	<code>01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSPbNIJfG3iXmu6cbCUrizuV</code>
Déterministe	<code>No</code>
Octets d'entrée	<code>0</code>
Octets de sortie	<code>91</code>

## Exemple 3

Entrée	<code>empty string</code>
<code>preserveNulls</code>	<code>-</code>
Sortie	<code>01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSPeM6qR8DWC2PB2GMlX41YK</code>
Déterministe	<code>No</code>
Octets d'entrée	<code>0</code>
Octets de sortie	<code>91</code>

## Exemple 4

Entrée	<code>abcdefghijklmnopqrstuvwxy</code>
<code>preserveNulls</code>	<code>-</code>

Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstEE1GKEPiRzyh0 h7t60mWMLTWcV02ckr6pkx9sGL5 VLDQeHzh6DmPpyWNuI=
Déterministe	No
Octets d'entrée	26
Octets de sortie	127

## Exemple 5

Entrée	abcdefghijklmnopqrstuvwxyza BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstEE1GKEPiRzyh0 h7t60mWMLTWcV02ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqdP4/ QOQ3cXb/pbvPcnohrHIGSX54ua+1/ JfcVjc=
Déterministe	No
Octets d'entrée	62
Octets de sortie	175

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

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

## Exemple 1

Entrée	<code>null</code>
<code>preserveNulls</code>	<code>TRUE</code>
Sortie	<code>null</code>
Déterministe	<code>Yes</code>
Octets d'entrée	<code>0</code>
Octets de sortie	<code>0</code>

## Exemple 2

Entrée	<code>null</code>
<code>preserveNulls</code>	<code>FALSE</code>
Sortie	<code>01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKL0hK1+7r75Tk+Mx9jy48Fcg1y0PvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=</code>
Déterministe	<code>No</code>
Octets d'entrée	<code>0</code>
Octets de sortie	<code>175</code>

## Exemple 3

Entrée	<code>empty string</code>
<code>preserveNulls</code>	<code>-</code>

Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKL0hK1+7r75Tk+Mx9jy48Fcg1y0PvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsircolB53l07VZpA60wkuXu29CA=
Déterministe	No
Octets d'entrée	0
Octets de sortie	175

## Exemple 4

Entrée	abcdefghijklmnopqrstuvwxy
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t60mWMLTWCv02ckr6pkx9jy48Fcg1y0PvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsircutBAc0+Mb9tuU2KIH31AWg=
Déterministe	No
Octets d'entrée	26
Octets de sortie	175



## Exemple 5

Entrée	abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstEE1GKEPiRzyh0 h7t60mWMLTWcV02ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqdP4/ Q0Q3cXb/pbvPcnnohrHIGSX54ua+1/ JfcVjc=
Déterministe	No
Octets d'entrée	62
Octets de sortie	175

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

Dans cet exemple, la valeur `pad_length` est de 162 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:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKL0hK1+7r75Tk+Mx9jy48Fcg1y0PvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsircnkB0xbLWD7zNdAqQGR0rXoSESdW0I0vpNoGcBfv4cJbG0A3h1DvtkSSVc2B8000GppzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn+8o4WtG/ClipNcjDXvXVtK4vfCohcCA6uwrmwv/xAySX+xcntotL703aBTBb
Déterministe	No
Octets d'entrée	0
Octets de sortie	307

## Exemple 3

Entrée	empty string
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKL0hK1+7r75Tk+Mx9jy48Fcg1y0PvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsircnkB0xbLWD7zNdAqQGR0rXoSESdW0I0vpNoGcBfv4cJbG0A3h1DvtkSSVc2B8000Gp

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

## Exemple 4

Entrée	abcdefghijklmnopqrstuvwxy
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t60mWMLTWCv02ckr6pkx9jy48 Fcg1y0PvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B8000Gp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwvX5Hn1+Wyf06ks3QMaRDGSf
Déterministe	No
Octets d'entrée	26
Octets de sortie	307

## Exemple 5

Entrée	abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstEE1GKEPiRzyh0 h7t60mWMLTWcV02ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/Q0Q3cXb/pbvPcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B8000Gp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrnwjkJXQZ0gPdeFX9Yr/8a1V5i
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	<pre> 01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4 0TBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKL0hK1+7r75Tk+Mx9jy48 Fcg1y0PvBqRSZ7oqy1V3UKfYTLEZb/ hCz7oaIneVsrcoNpATs0GzbnLkor4L+/ aSuA= </pre>
Déterministe	No
Octets d'entrée	0
Octets de sortie	175

## Exemple 3

Entrée	empty string
preserveNulls	-
Sortie	<pre> 01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4 0TBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKL0hK1+7r75Tk+Mx9jy48 Fcg1y0PvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcoLB53l07VZp A60wkuXu29CA= </pre>

Déterministe	No
Octets d'entrée	0
Octets de sortie	175

## Exemple 4

Entrée	abcdefghijklmnopqrstuvwxy
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstEE1GKEPiRzyh0h7t60mWMLTWCv02ckr6pkx9jy48Fcg1y0PvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAc0+Mb9tuU2KIIHH31AWg=
Déterministe	No
Octets d'entrée	26
Octets de sortie	175

## Exemple 5

Entrée	abcdefghijklmnopqrstuvwxyza BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstEE1GKEPiRzyh0h7t60mWMLTWCv02ckr6plwtH/8t

	RFnn2rF91bcB9G4+n8GiRfJNmqdP4/ Q0Q3cXb/pbvPcnnohrHIGSX54ua+1/ JfcVjc=
Déterministe	No
Octets d'entrée	62
Octets de sortie	175

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

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

#### Exemple 1

Entrée	null
<code>preserveNulls</code>	TRUE
Sortie	null
Déterministe	Yes
Octets d'entrée	0
Octets de sortie	0

#### Exemple 2

Entrée	null
<code>preserveNulls</code>	FALSE
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKL0hK1+7r75Tk+Mx9jy48 Fcg1y0PvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsircnkB0xbLWD7z

	NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B8000Gp 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 MX2s3JKL0hK1+7r75Tk+Mx9jy48 Fcg1y0PvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B8000Gp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv841VaT9Yd+6oQx65/+gdVT
Déterministe	No
Octets d'entrée	0
Octets de sortie	307



## Exemple 4

Entrée	abcdefghijklmnopqrstuvwxy
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstEE1GKEPiRzyh0 h7t60mWMLTWcV02ckr6pkx9jy48 Fcg1y0PvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B8000Gp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmtX5Hn1+Wyf06ks3QMaRDGSf
Déterministe	No
Octets d'entrée	26
Octets de sortie	307

## Exemple 5

Entrée	abcdefghijklmnopqrstuvwxyza BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
Sortie	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstEE1GKEPiRzyh0 h7t60mWMLTWcV02ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/Q0Q3cXb/pbvPcnkB0xbLWD7z

```
NdAqQGR0rXoSESdW0I0vpNoGcBf
v4cJbG0A3h1DvtkSSVc2B8000Gp
pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn
+8o4WtG/ClipNcjDXvXVtK4vfCohcCA6
uwrmwjkJXQZ0gPdeFX9Yr/8a1V5i
```

Déterministe	No
Octets d'entrée	62
Octets de sortie	307

### sealedColonnes de dépannage

Pourquoi le texte chiffré de messealed colonnes est-il plusieurs fois supérieur à la taille du textecleartext qui y est entré ?

Cela dépend de plusieurs facteurs. D'une part, le texte chiffré dans uneCleartext 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 avezpreserveNulls défini un grand nombre de valeursfalse et que vos données d'entrée contenaient un grand nombre denu11null valeurs, chacune de ces valeurs aura été transformée en 91 octets de texte chiffré. Enfin, si vous utilisez le remplissage, par définition, des octets sont ajoutés auxcleartext données avant qu'elles ne soient cryptées.

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

Nous ne vous recommandons pas de supprimer les valeurs de grande taille et de les déconseillons de les traiter séparément. Cela modifie les garanties de confidentialité fournies par le client de cryptage C3R. En tant que modèle de menace, supposons qu'un observateur puisse voir les deux ensembles de données cryptés. Si l'observateur constate que la colonne d'un sous-ensemble de données est nettement 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'unefullName 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 jeu de données contient le nom le plus long du monde (747 octets).

Dois-je fournir un rembourrage supplémentaire lorsque j'utilise le type **demax** rembourrage ?

Non. Lorsque vous utilisez lemax remplissage, nous recommandons de définir lepad\_length, également appelé remplissage supplémentaire au-delà de la plus grande valeur de la colonne, sur 0.

Puis-je simplement choisir une valeur plus grande pad\_length lorsque j'utilise unfixed rembourrage pour ne pas me demander si la plus grande valeur convient ?

Oui, mais la grande longueur du bloc-notes est inefficace et utilise plus d'espace de stockage que nécessaire. Nous vous recommandons de vérifier la taille de la valeur la plus élevée et de pad\_length définir le sur cette valeur.

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

Malheureusement, la réponse est que cela dépend. Au minimum, vous [Informatique cryptographique pour Clean Rooms](#) devez vérifier la manière dont le preserveNulls paramètre protège vos données. Nous vous recommandons toutefois de vous référer aux exigences de votre organisation en matière de traitement des données et à tout contrat applicable à la collaboration respective.

Pourquoi dois-je supporter la surcharge de Base64 ?

Pour assurer 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 pour garantir des résultats de requête corrects.

## Résolution des problèmes liés à l'augmentation imprévue de la taille du texte chiffré

Supposons que vous ayez chiffré vos données et que la taille des données qui en résultent 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.

### Identifier l'endroit où l'augmentation de taille s'est produite

Avant de déterminer pourquoi vos données chiffrées sont nettement plus volumineuses que vos clear text données, vous devez d'abord identifier l'origine de l'augmentation de taille. Clear text les colonnes peuvent être ignorées en toute sécurité car elles restent inchangées. Examinez les sealed colonnes restantes fingerprint et choisissez-en une qui semble significative.

## Identifier la raison de l'augmentation de taille

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 ?](#)
- [L'augmentation de taille provient-elle d'une `sealed` colonne ?](#)

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

Si la colonne qui contribue le plus à l'augmentation de la capacité de 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 pour résoudre ce problème sur une `column-by-column` base. Pour plus d'informations, consultez la section [Surplomb de base pour les `fingerprint` colonnes](#) pour en savoir plus sur cette colonne, y compris son impact sur les exigences de stockage.

L'autre cause possible d'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 le `preserveNulls` paramètre et sur l'impact de son activation sur les garanties de confidentialité de vos données, consultez [Informatique cryptographique](#).

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

Si la colonne qui contribue le plus à l'augmentation de la capacité de 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, consultez la section [Surplomb de base pour les `sealed` colonnes](#) pour en savoir plus sur cette colonne, y compris son impact sur les exigences de stockage.

La deuxième cause principale de l'augmentation de la capacité de stockage dans les `sealed` colonnes est le rembourrage. Le remplissage ajoute des octets supplémentaires `cleartext` avant qu'il ne soit crypté afin de masquer la taille des valeurs individuelles d'un ensemble de données.

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

La dernière cause possible d'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 le fonctionnement de ce paramètre et sur l'impact de son activation sur les garanties de confidentialité de vos données, consultez [Informatique cryptographique](#).

# Journalisation des requêtes

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).
- `eventID`— Identifiant unique de la requête exécutée. Après le 31 août 2023, l'identifiant unique est le même que `protectedQueryID`.
- `eventTimestamp`— Durée d'exécution de la requête.
- `parameters.parameterValue`— Les valeurs des paramètres (apparaissent en fonction du texte de la requête).
- `queryText`— Définition SQL 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.

## 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 du code SQL non pris en charge et pris en charge dans AWS Clean Rooms. Pour plus de détails, consultez la [référence AWS Clean Rooms SQL](#).

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 pour un code SQL incorrect dans AWS Clean Rooms.

Les journaux de requêtes n'indiquent pas qu'une requête a réussi et que le résultat de la requête a été fourni. 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 du code SQL pris en charge AWS Clean Rooms et fait référence aux tables configurées associées à la collaboration.

### Exemple

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, consultez [Création d'une collaboration dans AWS Clean Rooms](#).

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 l'affichage des 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 l'affichage des 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](#)
- [Configurer les rôles de service pour AWS Clean Rooms](#)
- [Configuration des rôles de service pour le AWS Clean Rooms ML](#)

## Inscrivez-vous pour AWS

Avant de pouvoir en utiliser Service AWS, 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 <https://portal.aws.amazon.com/billing/signup>.
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 Services AWS 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

- [Création d'un utilisateur administrateur](#)
- [Création d'un rôle IAM pour un membre de la collaboration](#)
- [Création d'un rôle de service pour lire les données](#)

- [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 bonnes pratiques, veuillez consulter <a href="#">Security best practices in IAM</a> (français non garanti) dans le Guide de l'utilisateur IAM.	Suivre les instructions de la section <a href="#">Mise en route</a> dans le AWS IAM Identity Center Guide de l'utilisateur.	Configurez l'accès par programmation en <a href="#">configurant le AWS CLI à utiliser AWS IAM Identity Center</a> dans le guide de l'AWS Command Line Interface utilisateur.
Dans IAM	Utiliser des identifiants à long terme pour accéder à AWS.	Suivre les instructions relatives à la <a href="#">Création de votre premier groupe utilisateur administrateur</a>	Configuration de l'accès par programmation via la <a href="#">Gestion des clés d'accès pour les</a>

Choisissez un moyen de gérer votre administrateur	Pour	Par	Vous pouvez également
(Non recommandé)		<a href="#">et utilisateur IAM</a> dans le Guide de l'utilisateur IAM.	<a href="#">utilisateurs IAM</a> dans le Guide de l'utilisateur IAM.

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

Un membre est un AWS client participant à une collaboration.

Pour créer un rôle IAM pour un membre de la collaboration

1. Suivez la procédure [Création d'un rôle pour déléguer des autorisations à un utilisateur IAM](#) dans le Guide de l'AWS Identity and Access Management utilisateur.
2. Pour l'étape Créer une politique, sélectionnez l'onglet JSON 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	<a href="#">AWS politique gérée : AWSCleanRoomsReadOnlyAccess</a>
Requête	<a href="#">AWS politique gérée : AWSCleanRoomsFullAccess</a>
Interrogez et recevez des résultats	<a href="#">AWS politique gérée : AWSCleanRoomsFullAccess</a>

Si vous voulez...	Ensuite, utilisez...
Gérez les ressources de collaboration sans poser de questions	<a href="#">AWS politique gérée : AWSCleanRoomsFullAccessNoQuerying</a>

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 autorisations IAM nécessaires pour créer un rôle de service	Utilisez la AWS Clean Rooms console pour créer un rôle de service.
Vous n'en avez pas <code>iam:CreateRole</code> , <code>iam:CreatePolicy</code> et <code>iam:AttachRolePolicy</code> les autorisations or Vous souhaitez créer les rôles IAM manuellement	Effectuez l'une des actions suivantes : <ul style="list-style-type: none"> <li>Utilisez la procédure suivante pour créer un rôle de service.</li> <li>Demandez à votre administrateur de créer le rôle de service en suivant la procédure suivante.</li> </ul>

## Pour créer un rôle de service permettant de lire des données

### Note

Vous ou votre administrateur IAM 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 plus d'informations, consultez [Prévention du cas de figure de l'adjoint désorienté 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 clé KMS 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 chaque *espace réservé* par 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 autorisations IAM nécessaires pour créer un rôle de service	Utilisez la AWS Clean Rooms console pour créer un rôle de service.
Vous n'en avez pas <code>iam:CreateRole</code> , <code>iam:CreatePolicy</code> et <code>iam:AttachRolePolicy</code> les autorisations  or  Vous souhaitez créer les rôles IAM manuellement	Effectuez l'une des actions suivantes : <ul style="list-style-type: none"> <li>Utilisez la procédure suivante pour créer un rôle de service.</li> <li>Demandez à votre administrateur de créer le rôle de service en suivant la procédure suivante.</li> </ul>



## Pour créer un rôle de service afin de recevoir des résultats

### Note

Vous ou votre administrateur IAM 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": [
```



```

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

```

4. Remplacez chaque *espace réservé* par 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 une requête. 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-1:5555555555555555:Membership/A1B2C3D4-5678-90AB-CDEF-Example11111* — L'ARN d'adhésion unique du membre qui peut effectuer une requête. L'ARN d'adhésion 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 ressource Amazon (ARN) se trouve dans l'onglet Propriétés du compartiment dans Amazon S3.
  - *AccountID* — Compte AWS L'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 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 autorisations IAM 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 console IAM (<https://console.aws.amazon.com/iam/>) avec votre compte administrateur.
2. Sous Access Management (Gestion des accès), choisissez Politiques (politiques).
3. Choisissez Créer une stratégie.
4. Dans l'éditeur de stratégie, sélectionnez l'onglet JSON, 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 clé KMS pour 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:catalog",
    "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 clé KMS 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 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'éditeur JSON.

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

SourceAccountC'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 l'ARN du jeu de données d'entraînement, 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-en 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 autorisations IAM 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 console IAM (<https://console.aws.amazon.com/iam/>) avec votre compte administrateur.
2. Sous Access Management (Gestion des accès), choisissez Politiques (politiques).
3. Choisissez Créer une stratégie.



4. Dans l'éditeur de stratégie, sélectionnez l'onglet JSON, 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 clé KMS pour 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 clé KMS 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 clé KMS 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 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'éditeur JSON.

```

{
  "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 l'ARN du jeu de données d'entraînement, 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-en 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 autorisations IAM 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 de lire les données de départ

1. Connectez-vous à la console IAM (<https://console.aws.amazon.com/iam/>) avec votre compte administrateur.
2. Sous Access Management (Gestion des accès), choisissez Politiques (politiques).
3. Choisissez Créer une stratégie.
4. Dans l'éditeur de stratégie, sélectionnez l'onglet JSON, 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 clé KMS pour 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"
                ]
            }
        }
    }
]
}

```

Si vous devez utiliser une clé KMS 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 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'éditeur JSON.

```


{
  "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/*"
        }
      }
    }
  ]
}

```

```
    }  
  ]  
}
```

SourceAccountC'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 l'ARN du jeu de données d'entraînement, 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-en si nécessaire.
  - d. Sélectionnez Créer un rôle.
15. Le rôle de service pour AWS Clean Rooms a été créé.



# Création d'une collaboration dans AWS Clean Rooms

Une collaboration est une limite logique sécurisée AWS Clean Rooms dans laquelle les membres peuvent effectuer des requêtes SQL 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 AWS des SDK, consultez la [référence des AWS Clean Rooms API](#).

## Rubriques

- [Créez une collaboration](#)
- [Étapes suivantes](#)

## Créez une collaboration

Avant de commencer, assurez-vous d'avoir rempli les conditions préalables suivantes :

- Vous avez le nom et l'Identifiant AWS de chaque membre que vous souhaitez inviter à rejoindre la collaboration.
- Vous êtes autorisé à partager le nom et l'Identifiant AWS 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 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 Roomsconsole](#) 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 qui sont 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 AWSidentifiant de membre.

- ii. Pour Membre 2, entrez le nom d'affichage du membre et l'Compte AWSID du membre que vous souhaitez inviter à rejoindre la collaboration.

Le nom d'affichage et l'Compte AWSidentifiant 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, elles ne sont plus modifiables.

 Note

Vous devez informer le membre de la collaboration que son Compte AWSidentifiant 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 AWSidentifiant de membre pour

chaque membre susceptible de fournir les données que vous souhaitez inviter à la collaboration.

c. Pour les capacités des membres, choisissez l'une des options suivantes :

Si vous voulez...	Alors...
Interrogez les données de la collaboration et recevez les résultats	<ol style="list-style-type: none"> <li>1. Choisissez-vous comme membre autorisé à exécuter des requêtes.</li> <li>2. Laissez le paramètre par défaut du membre autorisé à recevoir des résultats identique à celui du membre qui exécute les requêtes.</li> </ol>
Interrogez les données de la collaboration et désignez un autre membre pour recevoir les résultats	<ol style="list-style-type: none"> <li>1. Choisissez-vous comme membre autorisé à exécuter des requêtes.</li> <li>2. Sélectionnez le membre qui peut recevoir les résultats dans la liste déroulante.</li> </ol>
Recevez les résultats de la requête dans la collaboration et désignez un autre membre pour interroger les données	<ol style="list-style-type: none"> <li>1. Sélectionnez le membre autorisé à exécuter des requêtes dans la liste déroulante.</li> <li>2. Choisissez vous-même en tant que membre qui peut recevoir les résultats dans la liste déroulante.</li> </ol>
Créez et gérez la collaboration, assignez un autre membre pour interroger les données et affectez un autre membre pour recevoir les résultats	<ol style="list-style-type: none"> <li>1. Sélectionnez le membre autorisé à exécuter des requêtes dans la liste déroulante.</li> <li>2. Sélectionnez le membre qui peut recevoir les résultats dans la liste déroulante.</li> </ol>

d. Pour la configuration du paiement, choisissez l'une des options suivantes :

Si vous voulez...	Alors...
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.

- JOIN Autorisation 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. NULL les valeurs n'apparaîtront pas comme NULL dans une table cryptée.

Choisissez Oui si vous souhaitez conserver NULL les valeurs. NULL les valeurs apparaîtront comme NULL dans une table cryptée.

Pour plus d'informations sur les paramètres de calcul cryptographique, consultez [Paramètres de calcul cryptographique](#).

Pour plus d'informations sur la façon de chiffrer vos données pour les utiliser dans AWS Clean Rooms, consultez [Préparation 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 :

Si vous choisissez...	Alors...
Oui, inscrivez-vous en créant un abonnement dès maintenant	La collaboration et votre adhésion sont créées.  Votre statut dans la collaboration est actif.


Si vous choisissez...	Alors...
Non, je créerai un abonnement ultérieur	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 :

Si tu...	Alors...
Conservez la case Définir les paramètres par défaut maintenant cochée. (Il est sélectionné par défaut.)	<ol style="list-style-type: none"> <li>1. Pour la destination des résultats dans Amazon S3, entrez la destination Amazon S3.</li> <li>2. Pour le format du résultat de la requête, choisissez CSV ou PARQUET.</li> </ol>
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 :

Si vous choisissez...	Alors...
Allumez	<p>Les journaux de requêtes qui vous concernent sont stockés dans Amazon CloudWatch Logs.</p> <p>Chaque membre ne peut recevoir que les journaux des requêtes qu'il a initiées ou qui contiennent ses données.</p> <p>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.</p>
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, consultez [Tarification de 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 rubrique [Création d'un compte Amazon SNS pour les notifications budgétaires](#) dans le guide de l'AWS Cost Management 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. Sélectionnez l'une des méthodes suivantes :

Si vous avez choisi de...	Choisissez ensuite...
Créez un abonnement avec la collaboration (Oui, inscrivez-vous en créant un abonnement maintenant)	Créez une collaboration et une 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.

## Étapes suivantes

Vous êtes maintenant prêt à :

- [Préparez votre tableau de données à interroger. AWS Clean Rooms](#) (Facultatif si vous souhaitez interroger vos propres données.)
- [Associez le tableau configuré à votre collaboration.](#) (Facultatif si vous souhaitez interroger vos propres données.)
- [Configurez une règle d'analyse pour la table configurée.](#) (Facultatif si vous souhaitez interroger vos propres données.)
- [Créez un abonnement et rejoignez une collaboration.](#)
- [Gérez votre collaboration.](#)

# Création d'un abonnement et participation à une collaboration dans AWS Clean Rooms

Une adhésion 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 AWS des SDK, consultez la [référence des AWS Clean Rooms API](#).

## Rubriques

- [Créez un abonnement et rejoignez une collaboration](#)
- [Étapes suivantes](#)

## Créez un abonnement et rejoignez une 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 les Compte AWS identifiants 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	<p>Les journaux de requêtes qui vous concernent sont stockés dans Amazon CloudWatch Logs.</p> <p>Chaque membre ne peut recevoir que les journaux des requêtes qu'il a initiées ou qui contiennent ses données.</p> <p>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.</p>
Éteindre	<p>Les journaux de requêtes qui vous concernent ne sont pas stockés dans votre compte Amazon CloudWatch Logs.</p>

 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.

Exemple


Par exemple : **s3://bucket/prefix**

- ii. Choisissez le format du résultat (CSV ou 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 plus d'informations, consultez [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, consultez [Tarification de 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 rubrique [Création d'un compte Amazon SNS pour les notifications budgétaires](#) dans le guide de l'AWS Cost Management 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 identifiants des autres membres.

Pour plus d'informations sur la façon de quitter une collaboration, consultez [Quitter une collaboration](#).

## Étapes suivantes

Vous êtes maintenant prêt à :

- [Préparez votre tableau de données à interroger. AWS Clean Rooms](#) (Facultatif si vous souhaitez interroger vos propres données.)
- [Associez le tableau configuré à votre collaboration.](#)
- [Configurez une règle d'analyse pour la table configurée.](#)

# 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 vos tables de données sont déjà cataloguées AWS Glue, passez à [Création 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](#)
- [Étapes suivantes](#)

Pour plus d'informations sur les formats de données que vous pouvez utiliser pour les requêtes, consultez [Formats 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 ensembles de données doivent être enregistrés 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 plus d'informations, consultez [Création d'une collaboration dans AWS Clean Rooms](#).
- 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 dans [Préparation 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 plus d'informations, consultez

## [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/](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, consultez [Types 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 clés KMS 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.

## Étapes suivantes

Maintenant que vous avez préparé vos tableaux de données, vous êtes prêt à :

- [Création d'une table configurée](#)
- [Création d'un modèle ML](#)

## Formats de données pour AWS Clean Rooms

Les ensembles de données que vous utilisez pour les requêtes dans AWS Clean Rooms sont généralement les mêmes types de jeux de données que ceux que vous utilisez pour d'autres applications. Il est par exemple du même type de jeu de données utilisé avec Amazon Athena, Amazon EMR, Amazon Redshift, Spectrum et Amazon QuickSight. Il est possible d'interroger les données dans leur format d'origine directement depuis Amazon Simple Storage Service (Amazon S3).


Pour interroger des données, les ensembles de données doivent être dans un format qui AWS Clean Rooms soutient. Il s'agit du compartiment Amazon S3 contenant les ensembles de données et de AWS Clean Rooms le cluster doit être dans la même Région AWS.

## Formats de données pris en charge

AWS Clean Rooms est compatible avec les formats structurés suivants :

- [Tables Apache Iceberg](#)
- Parquet
- RCFile
- TextFile
- SequenceFile
- RegexSerde

- OpenCSV
- AVRO
- JSON

 Note

UNtimestamp a valeur d'un fichier texte doit être au format `yyyy-MM-dd HH:mm:ss.SSSSSS`. Il est par exemple `:2017-05-01 11:30:59.000000`.

Nous vous recommandons d'utiliser un format de fichier de stockage en colonnes, tel que Apache 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 avec AWS Clean Rooms, toutes vos données doivent être cataloguées dans AWS Glue. Il est recommandé de consulter la section intitulée [Démarrage avec le plugin AWS Glue Data Catalog](#) dans le AWS Glue Guide du développeur.

AWS Clean Rooms prend en charge les éléments suivants AWS Glue Data Catalog types de données :

- 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

Il est vivement recommandé de compresser vos ensembles de données afin de réduire l'espace de stockage, d'améliorer les performances et de diminuer les coûts.

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. Il est vivement recommandé de compresser les formats de colonnes au niveau du fichier.

## 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-KM— Chiffrement côté serveur avec des clés gérées par AWS Key Management Service

Il est recommandé d'utiliser le SSE-S3 AWS Clean Rooms le rôle de service utilisé pour associer la table configurée à la collaboration doit disposer des autorisations KMS-Decrypt. Il est également recommandé d'utiliser le SSE-KMS, la politique de clé KMS doit également autoriser AWS Clean Rooms rôle de service à déchiffrer.

AWS Clean Rooms n'est pas compatible avec le chiffrement côté client d'Amazon S3. Il est recommandé de plus d'informations sur le chiffrement côté serveur [Protection des données à l'aide d'un chiffrement côté serveur](#) dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

## En utilisant Apache Iceberg tables en AWS Clean Rooms (aperçu)

Il s'agit de documentation au niveau des versions préliminaires pour le support de Apache Iceberg tables, qui est en version préliminaire. La documentation et la fonction sont toutes deux sujettes à modification. Nous vous recommandons d'utiliser cette fonction uniquement dans des environnements de test et non dans des environnements de production. Pour un aperçu des conditions générales, voir Bêtas et aperçus dans le [AWS Termes de service](#).

Apache Iceberg est un format de table open source pour les lacs de données. AWS Clean Rooms peut utiliser les statistiques stockées dans Apache Iceberg des métadonnées pour optimiser les plans de requêtes et réduire le nombre de fichiers au niveau des tables lors du traitement de requêtes en salle blanche. Pour de plus amples informations, veuillez consulter le [Iceberg Apache](#) documentation.

Tenez compte des points suivants lors de l'utilisation AWS Clean Rooms avec tables Iceberg :

- tables au niveau des AWS Glue Data Catalog seulement— Apache Iceberg tables au niveau des tables AWS Glue Data Catalog sur la base de [implémentation d'un catalogue de colle open source](#).
- Format de fichier Parquet— AWS Clean Rooms ne prend en charge que les tables Iceberg au format de fichier de données Parquet.

- Compression GZIP et Snappy—AWS Clean Rooms supporte le parquet avec GZIP et Snappy compression.
- Versions Iceberg—AWS Clean Rooms prend en charge l'exécution de requêtes sur les tables Iceberg des versions 1 et 2.
- Cloisons— Vous n'avez pas besoin d'ajouter manuellement des partitions pour Apache Iceberg tables en AWS Glue. AWS Clean Rooms détecte les nouvelles partitions dans Apache Iceberg tables automatiquement 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 régulières dans AWS Clean Rooms schéma de table et non séparément en tant que clé de partition dans le schéma de table configuré.
- Limites
  - tables New Iceberg uniquement

Apache Iceberg tables converties à partir de Apache Parquet tables non prises en charge.
  - Requêtes Time Travel

AWS Clean Rooms ne prend pas en charge les demandes de voyage dans le temps avec Apache Iceberg tables.
  - Version 2 du moteur Athena

Iceberg tables créées avec la version 2 du moteur Athena ne sont pas prises en charge.
  - Formats de fichier

Avro et les formats de fichier ORC (Optimized Row Columnar) ne sont pas pris en charge.
  - Compression

Zstandard (Zstd) compression pour Parquet n'est pas pris en charge.

## Types de données pris en charge pour les tables Iceberg

AWS Clean Rooms peut interroger Iceberg tables au niveau des 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 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](#)
- [Étape 2 : Téléchargez le client de chiffrement C3R](#)
- [\(Facultatif\) Étape 3 : Afficher les commandes disponibles dans le client de chiffrement C3R](#)
- [Étape 4 : générer un schéma de chiffrement pour un fichier tabulaire](#)
- [Étape 5 : Création d'une clé secrète partagée](#)
- [Étape 6 : Stocker la clé secrète partagée dans une variable d'environnement](#)
- [Étape 7 : Chiffrer les données](#)
- [Étape 8 : vérifier le chiffrement des données](#)
- [\(Facultatif\) Créez un schéma \(utilisateurs avancés\)](#)

## 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 appels d'API 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 recommandée Java Runtime Environment, Amazon Corretto 11 ou version ultérieure, peut être téléchargée sur https://aws.amazon.com/corretto.](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 dans AWS Clean Rooms.](#)
- Le créateur de la collaboration vous a envoyé l'identifiant de collaboration en tant que participant à la collaboration. Le nom de ressource Amazon (ARN) de la collaboration est inclus dans l'invitation envoyée, qui contient l'ID 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 : https://github.com/aws/c3r](https://github.com/aws/c3r)
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](#).

## (Facultatif) Étape 3 : 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 fichier CSV 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 requêtes SQL 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

**i 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 soient garnies de la même longueur.

Lorsque vous déterminez la longueur `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 remboursement : [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 ( <code>_fingerprint</code> ) 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 ( <code>_sealed</code> ) ou entrezn.	Choisissez le type de remboursement.  Pour de plus amples informations, veuillez consulter

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 remboursement : [n] un, [f] fixe ou [m] max <default 'max'>
					<a href="#">(Facultatif) Créez un schéma (utilisateurs avancés).</a>
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 remboursement (pour les sealed colonnes uniquement).  Pour de plus amples informations, veuillez consulter <a href="#">(Facultatif) Créez un schéma (utilisateurs avancés).</a>

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 et ad\_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 ou Unix/Linux) ou dir si vous utilisez Windows).
  - 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 de la CLI, 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 courir `java --jar PATH/T0/c3r-cli.jar`. Ou, si vous l'avez ajoutée `PATH/T0/c3r-cli.jar` à votre variable d'environnement `CLASSPATH`, vous pouvez également exécuter le nom de la classe. Le client de chiffrement

C3R regardera le CLASSPATH pour le trouver (par exemple,). `java com.amazon.psion.cli.Main`

- L'`--interactive`indicateur sélectionne le mode interactif pour développer le schéma. Cela guide l'utilisateur à travers un assistant de création du schéma. Les utilisateurs ayant des 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 Services AWS 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 on macOS.

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, pour `sales.csv`, il y a trois colonnes : `usernamepurchased`, et `product`. 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 ou Unix/Linux) ou `dir` si vous utilisez Windows).
  - 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 de la CLI, 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'`--interactive`indicateur 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-têtes de colonne, consultez l'`--noHeaders`indicateur de la commande de schéma disponible dans la 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'utilisation de 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'utilisation PowerShell

Pour PowerShell une application de terminal disponible sur Windows, 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 Services AWS 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 Service AWS 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'utilisation PowerShell, 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 ou macOS, 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 dans [Étape 6 : Stocker la clé secrète partagée dans une variable d'environnement](#).
2. À partir de 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. Pour `<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](#) et [Indicateurs facultatifs dans l'informatique 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 spécifions 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 `allowRepeatedFingerprintValue` est `false`. 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 schéma JSON 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 schéma JSON 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 `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 objets JSON 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` 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 `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.

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,C00,9,""
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 `none`. 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/WR2J0/To2dTxD73aDEe2ZUXeSHy3Tv
+1Mk=,01:enc:FQ3n3Ahv9BQQNWQGcugeHzHYzEZE1vapHa2Uu4SRgSAtZ3q0bjPA4TcsHt
+B0kMKBcnHWI13BeGG/SBqmj7vKpI=
Paulo,Santos,01:hmac:CHF4eIrtTNgAooU9v4h9Qjc
+txBnMidQTjdjWuaDTTA=,01:enc:KZ5n5GtaXACco65AXk48BQ02durDNR2ULc4YxmMC8NaZZKKJiksU1IwFadAvV4iBQ1
Mateo,Jackson,01:hmac:iIRnjfNBzryusIJ1w35lgNzeY1RQ1bSfq6PDHW8Xrbk=,01:enc:mLKpS5HIOSgphdEsrzhd
eN9nB02gAbIygt40Fn4LalYn9Xyj/XUWXlmn8zFe2T4kyDTD8kG0vpQEUGxAUFk=
Diego,Ramirez,01:hmac:UK8s8Cn/WR2J0/To2dTxD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:rmZhT98Zm
+IIGw1UTjMIJP4IrW/AA1tBLMXcHvnYfRgmWP623VFQ6aUnhsb2MDqEw4G5Uwg5rKKZepUxx5uKbfbk=
Jorge,Souza,01:hmac:3BxJdXiFFyZ8HbBYNqqEhBVqhN0d7s2ZiKUe7QiTy08=,01:enc:vVaqWC1VRbhvkf8gnuR7q0z
Terry,Whitlock01:hmac:UK8s8Cn/WR2J0/To2dTxD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:3c9VEWb0D0/
xbQjdGuccLvI7oZTBdPU+SyrJIyr2kudfAxbuMQ2uRdU/q7rbgyJjxZS8M2U35ILJf/lDgTyg7cM=
Jane,Doe,01:hmac:UK8s8Cn/WR2J0/To2dTxD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:9RWv46YLveykeNZ/
G0Nd1YFg+AVd0nu05hHyAYTQkPLHnyX+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 des objets JSON 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 `casealed`. 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,C00, 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 entêtes cibles spécifiés.

```
givenname,surname,state_fingerprint,state
Mateo,Jackson,01:hmac:iIRnjfNBzryusIJ1w35lgNzeY1RQ1bSfq6PDHW8Xrbk=,01:enc:ENS6QD3cMV19vQEGfe9MM
Q8m/Y5SA89dJwKpT5rGpp8e36h6klwDoslpFzGvU0=
Jorge,Souza,01:hmac:3BxJdXiFFyZ8HBbYNqqEhBVqhN0d7s2ZiKUe7QiTy08=,01:enc:LKo0zirq2+
+XEIIIMNRjAsGMdyWUDwYaum0B+IFP+rUf1BNeZDJjtFe1Z+zbZfXQWwJy52Rt7HqvAb2WIK1oMmk=
Paulo,Santos,01:hmac:CHF4eIrtTNgAooU9v4h9Qjc
+txBnMidQTjdjWuaDTTA=,01:enc:MyQKyWxJ9kvK1xDQQtX1UNwv3F+y1BRr0xrUY/1BGg5KFg0n9pK+MZ7g
+ZNqZEPcPz4lht1u0t/wbTaqz0CLXFQ=
Jane,Doe,01:hmac:UK8s8Cn/WR2J0/To2dTxD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:Pd8sbITBfb0/
ttUB4svVsgoYkDfnDvgkvxzeci0Yxq54rLSwccy1o3/B50C3cpkkn56dovCwzgmPNwrmCmYtb4=
Terry,Whitlock01:hmac:UK8s8Cn/WR2J0/To2dTxD73aDEe2ZUXeSHy3Tv
+1Mk=,01:enc:Qmtzu3B3GAXKh2KkRYTiEAaMopYedsSdF2e/
ADUiBQ9kv2CxKPzWyYTD3ztmKPMka19dHre5VhUHNp030+j1AQ8=
Diego,Ramirez,01:hmac:UK8s8Cn/WR2J0/To2dTxD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:ysdg
+GHKdeZrS/geBIoo0EPLHG68MsWpx1dh3xjb+fG51mFmqUcJLNuuYBHhHA1xchM2WVeV1fmHkBX3mvZNVkc=
John,Doe,01:hmac:UK8s8Cn/WR2J0/To2dTxD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:9uX0wZu07kAPAx
+Hf6uvQownkWqFSKtWS7gQIJSe5aXFquKWCK6yZN0X5Ea2N3bn03Uj1kh0agDwoiP9FRZGJA4=
```

# 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 interrogées dans AWS Clean Rooms. Les tables configurées peuvent être associées à une ou plusieurs collaborations.

Pour plus d'informations sur AWS Glue, consultez le [manuel du développeur AWS Glue](#).

## Création d'une table configurée

Au cours de cette étape, vous créez un tableau configuré en vue dans AWS Clean Rooms de l'utiliser dans la collaboration.

Pour créer une table configurée dans AWS Clean Rooms

1. Connectez-vous à l'AWS Management Console et ouvrez la [AWS Clean Rooms console](#) avec votre compte AWS (si ce n'est pas déjà fait).
2. Dans le panneau de navigation de gauche, choisissez 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 qu'il s'agit du tableau 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, choisissez Toutes les colonnes ou Liste personnalisée.



Si tu choisis...	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 du tableau configuré,

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 et valeur.

7. Choisissez Configurer une nouvelle table.

## Étapes suivantes

Maintenant que vous avez créé une table configurée, vous êtes prêt à :

- [Configuration d'une règle d'analyse dans la table configurée](#)
- [Associer la table configurée à une collaboration](#)

# Configuration d'une règle d'analyse sur une table configurée

Les sections suivantes décrivent comment configurer une règle d'analyse pour 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 : [agrégation](#), [liste](#) et [personnalisée](#).

Il ne peut y avoir qu'une seule règle d'analyse par table configurée.

## 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).

Pour mieux comprendre les types de règles d'analyse disponibles dans AWS Clean Rooms, voir [Règles d'analyse dans AWS Clean Rooms](#).

Pour plus d'informations sur la règle d'analyse d'agrégation, consultez [Règle d'analyse d'agrégation](#).

Pour plus d'informations sur la règle d'analyse de liste, consultez [Règle d'analyse des listes](#).

Pour plus d'informations sur la règle d'analyse personnalisée, consultez [Règle d'analyse personnalisée dans AWS Clean Rooms](#).

Après avoir lu et compris ces sections, vous pouvez effectuer les procédures suivantes :

## Rubriques

- [Configuration d'une règle d'analyse d'agrégation pour une table \(flux guidé\)](#)
- [Configuration d'une règle d'analyse de liste pour une table \(flux guidé\)](#)
- [Configuration d'une règle d'analyse personnalisée pour une table \(flux guidé\)](#)
- [Configuration d'une règle d'analyse pour une table \(éditeur JSON\)](#)

- [Étapes suivantes](#)


## Configuration d'une règle d'analyse d'agrégation pour 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 Roomsconsole 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 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 :
    - COMPTER
    - DÉCOMPTE DISTINCT
    - SUM
    - SOMME DISTINCTE
    - 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...
ET	Vous pouvez inclure AND dans le INNER JOIN match des conditions permettant de joindre une colonne à une autre colonne entre les tables.
OU	Vous pouvez inclure OR dans les conditions de INNER JOIN correspondance pour combiner plusieurs correspondances de

Si vous choisissez...	Alors...
	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'instruction SELECT, 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	<p>Vous autorisez toutes les fonctions scalaires actuellement prises en charge par AWS Clean Rooms.</p> <ul style="list-style-type: none"> <li>• Vous pouvez choisir Afficher la liste pour voir la liste complète des fonctions scalaires prises en charge dans AWS Clean Rooms.</li> </ul>
Une liste personnalisée	<p>Vous pouvez personnaliser les fonctions scalaires à autoriser.</p> <ul style="list-style-type: none"> <li>• Choisissez une ou plusieurs options dans la liste déroulante Spécifier les fonctions scalaires autorisées.</li> </ul>
Aucun	Vous ne souhaitez autoriser aucune fonction scalaire.

Pour en savoir plus, consultez [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. Choisissez Suivant.
14. 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.

## Configuration d'une règle d'analyse de liste pour une table (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, choisissez 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...
ET	Vous pouvez inclure AND dans le INNER JOIN match des conditions permettant de joindre une colonne à une autre colonne entre les tables.
OU	Vous pouvez inclure OR dans les conditions 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 le menu déroulant 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 : 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.

## Configuration d'une règle d'analyse personnalisée pour une table (flux guidé)

La règle d'analyse personnalisée active les requêtes SQL personnalisées sur une table configurée. La règle d'analyse personnalisée est requise si vous utilisez des [modèles d'analyse](#) ou une [confidentialité différentielle](#).

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 Roomsconsole 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 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 au niveau de l'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	Éteindre



Si tu...	Ensuite, choisissez...
protection contre les tentatives de réidentification	

- b. Si vous avez choisi d'activer la confidentialité différentielle, sélectionnez la colonne Identifiant utilisateur qui contient l'identifiant unique de vos utilisateurs, telle que `user_id` la colonne, dont vous souhaitez protéger la confidentialité. Si vous souhaitez 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 le type de commande :

Si vous voulez...	Ensuite, choisissez...
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

Si tu as choisi...	Alors...
	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 AWSID approprié .

9. Choisissez Suivant.
10. 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 personnalisée pour la table.

## Configuration d'une règle d'analyse pour une table (éditeur JSON)

La procédure suivante montre comment ajouter une règle d'analyse à une table à l'aide de l'option de l'éditeur JSON dans la AWS Clean Rooms console.

Pour configurer une agrégation, une liste ou une règle d'analyse personnalisée pour une table (éditeur JSON)

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 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 l'éditeur JSON, 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	<ol style="list-style-type: none"> <li>1. Spécifiez les paramètres de la règle d'analyse sélectionnée dans la définition de la règle d'analyse.</li> <li>2. Vous pouvez appuyer sur Ctrl + barre d'espace pour activer la saisie automatique.</li> </ol> <p>Pour plus d'informations sur les paramètres des règles d'analyse d'agrégation, consultez <a href="#">Règle d'analyse d'agrégation : contrôles des requêtes</a>.</p> <p>Pour plus d'informations sur les paramètres des règles d'analyse de liste, consultez <a href="#">Règle d'analyse des listes : contrôles des requêtes</a>.</p>
Importer depuis un fichier	<ol style="list-style-type: none"> <li>1. Sélectionnez votre fichier JSON sur votre disque local.</li> <li>2. Choisissez Open.</li> </ol> <p>La définition de la règle d'analyse affiche la règle d'analyse du fichier chargé.</p>

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.

## 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/](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 qui est soutenue par un ensemble de données Amazon S3 AWS KMS chiffré, vous devez autoriser le rôle à utiliser la clé KMS 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

- [Associer une table configurée depuis la page détaillée de la table configurée](#)
- [Associer une table configurée depuis la page détaillée de la collaboration](#)
- [Étapes suivantes](#)

Pour plus d'informations sur la façon d'associer vos tables configurées à la collaboration à l'aide AWS des SDK, consultez la [référence des AWS Clean Rooms API](#).

## 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	<ul style="list-style-type: none"> <li>• AWS Clean Rooms crée un rôle de service avec la politique requise pour cette table.</li> <li>• Le nom du rôle de service par défaut est <code>cleanrooms-&lt;timestamp&gt;</code></li> </ul>

Si vous choisissez...	Alors...
	<ul style="list-style-type: none"><li data-bbox="862 212 1442 338">• Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques.</li><li data-bbox="862 365 1453 632">• Si vos données d'entrée sont cryptées, vous pouvez sélectionner Ces données sont cryptées avec une clé KMS, puis saisir une clé AWS KMS key qui sera utilisée pour déchiffrer vos données saisies.</li></ul>

Si vous choisissez...	Alors...
Utiliser un rôle de service existant	<ol style="list-style-type: none"><li data-bbox="862 226 1503 661">1. Choisissez un nom de 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.</li><li data-bbox="862 682 1503 955">2. Affichez le rôle de service en choisissant le lien externe 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.</li><li data-bbox="862 1186 1503 1501">3. (Facultatif) Cochez la case Ajouter une politique préconfigurée avec les autorisations nécessaires à ce rôle pour ajouter attacher les autorisations nécessaires au rôle. Vous devez disposer des autorisations nécessaires pour modifier les rôles et créer des politiques.</li></ol>

 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, voir [AWS 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 du tableau.

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	<ul style="list-style-type: none"> <li>• AWS Clean Rooms crée un rôle de service avec la politique requise pour cette table.</li> <li>• Le nom du rôle de service par défaut est <code>cleanrooms-&lt;timestamp&gt;</code>.</li> <li>• Vous devez disposer des autorisations nécessaires pour créer des rôles et associer des politiques.</li> <li>• Si vos données d'entrée sont cryptées, vous pouvez sélectionner Ces données sont cryptées avec une clé KMS, puis saisir une clé AWS KMS key qui sera utilisée pour déchiffrer vos données saisies.</li> </ul>
Utiliser un rôle de service existant	<ol style="list-style-type: none"> <li>1. Choisissez un nom de rôle de service existant dans la liste déroulante.</li> </ol> <p>La liste des rôles s'affiche si vous êtes autorisé à répertorier les rôles.</p> <p>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.</p>

Si vous choisissez...	Alors...
	<p>2. Affichez le rôle de service en choisissant le lien externe <b>Afficher</b> dans IAM.</p> <p>S'il n'existe aucun rôle de service existant, l'option <b>Utiliser un rôle de service existant</b> n'est pas disponible.</p> <p>Par défaut, AWS Clean Rooms ne tente pas de mettre à jour la politique de rôle existante pour ajouter les autorisations nécessaires.</p> <p>3. (Facultatif) Cochez la case <b>Ajouter une politique préconfigurée</b> avec les autorisations nécessaires à ce rôle pour ajouter attacher les autorisations nécessaires au rôle. Vous devez disposer des autorisations nécessaires pour modifier les rôles et créer des politiques.</p>

 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, voir [AWS 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.

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 :

- [Modifiez la collaboration](#), si vous en êtes le créateur
- [Interroger les tables de données](#) (en tant que membre pouvant effectuer des requêtes)

# Configuration d'une politique de confidentialité différentielle

## Rubriques

- [Configuration d'une politique de confidentialité différentielle \(flux guidé\)](#)
- [Étapes suivantes](#)

## Configuration d'une politique de confidentialité différentielle (flux guidé)

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.

## Étapes suivantes

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)

# Utilisation de modèles d'analyse

Les modèles d'analyse fonctionnent avec [Règle 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 AWS des SDK, consultez la [référence des AWS Clean Rooms API](#).

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'éditeur SQL 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. Choisissez 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 être saisi dans une requête dans 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

En tant que [membre habilité à effectuer une requête](#), vous pouvez effectuer l'une des opérations suivantes :

- Créez une requête SQL manuellement à l'aide de l'éditeur de code SQL.
- Utilisez l'interface utilisateur du générateur d'analyse pour créer une requête sans avoir à écrire de code SQL.
- Utilisez un [modèle d'analyse](#) approuvé.

Lorsque le membre habilité à effectuer une requête exécute une requête SQL 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.

AWS Clean Rooms prend en charge les requêtes SQL qui peuvent être différentes des autres moteurs de requêtes. Pour les spécifications, consultez la [référence AWS Clean Rooms SQL](#). 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 opérations SQL 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.

Les rubriques suivantes expliquent comment interroger des données dans le cadre d'une collaboration à l'aide de la AWS Clean Rooms console.

## Rubriques

- [Utilisation de l'éditeur de code SQL](#)

- [Utilisation du générateur d'analyse](#)
- [Interrogation de données avec 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'opération d' AWS Clean Rooms `StartProtectedQueryAPI` ou en utilisant AWS les SDK, consultez la [référence des AWS Clean Rooms API](#).

Pour plus d'informations sur la journalisation des requêtes, consultez [Journalisation des requêtes](#).

#### 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, consultez [Réception des résultats de requêtes](#).

## Utilisation de l'éditeur de code SQL

En tant que membre habilité à effectuer des requêtes, vous pouvez créer une requête manuellement en écrivant du code SQL dans l'éditeur de code SQL. L'éditeur de code SQL se trouve dans la section Analyse de l'onglet Requêtes de la AWS Clean Rooms console.

L'éditeur de code SQL s'affiche par défaut. Si vous souhaitez utiliser le générateur d'analyse pour créer des requêtes, consultez [Utilisation du générateur d'analyse](#).

#### Important

Si vous commencez à écrire une requête SQL 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 commandes, fonctions et conditions SQL. Pour plus d'informations, consultez la [référence AWS Clean Rooms SQL](#).

**i** 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 créer la requête manuellement à l'aide de l'éditeur de code SQL

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.

**i** 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).

**i** 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 code SQL.

(Facultatif) Si vous souhaitez utiliser un exemple de requête

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.

L'exemple de requête apparaît.

Toutes les tables répertoriées sous Tables sont incluses dans la requête.

3. Modifiez les valeurs d'espace réservé dans la requête.

(Facultatif) Si vous souhaitez insérer des noms de colonnes ou des fonctions

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 (par exemple INNER JOIN SUMDISTINCT, SUM ou COUNT).
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-vous que la colonne de partition est étiquetée comme colonne de partition dans la AWS

(Facultatif) Si vous souhaitez utiliser un exemple de requête

(Facultatif) Si vous souhaitez insérer des noms de colonnes ou des fonctions

Glue table sous-jacente à la table configurée.


5. Modifiez les valeurs d'espace réservé dans la requête.

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 de AWS Clean Rooms](#).

## Utilisation du générateur d'analyse

Vous pouvez utiliser le générateur d'analyse pour créer des requêtes sans avoir à écrire de code SQL. Avec le générateur d'analyse, vous pouvez créer une requête pour une collaboration qui possède les caractéristiques suivantes :

- Une table unique qui utilise la [règle d'analyse d'agrégation](#) sans qu'aucun JOIN ne soit requis
- 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 requêtes SQL manuellement, consultez [Utilisation de l'éditeur de code SQL](#).

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 BY n'est pas pris en charge pour les requêtes d'agrégation.  
Seul l'AND opérateur 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 code SQL d'aperçu.
    - a. Affichez le code SQL généré à partir du générateur d'analyse.
    - b. Pour copier le code SQL, choisissez Copier.
    - c. Pour modifier le code SQL, choisissez Modifier dans l'éditeur de code SQL.
  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 de 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 Choisir les métriques, passez en revue les métriques agrégées qui ont été présélectionnées par défaut et	1. Pour Choisir les attributs, passez en revue les attributs de liste présélectionnés par

### Si les deux tables utilisent la règle d'analyse d'agrégation

supprimez toute métrique si nécessaire.

2. Pour Match records, sélectionnez un ou plusieurs enregistrements.

#### 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

### Si les deux tables utilisent la règle d'analyse de liste

défaut et supprimez toute métrique si nécessaire.

2. Pour Match records, sélectionnez un ou plusieurs enregistrements.

#### 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

LIMIT n'est pas pris en charge pour les requêtes de liste.

### Si les deux tables utilisent la règle d'analyse d'agrégation

z 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 BY n'est pas pris en charge pour les requêtes d'agrégation. Seul l'AND opérateur 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.

### Si les deux tables utilisent la règle d'analyse de liste

Seul l'AND opérateur est pris en charge dans les filtres.

4. (Facultatif) Pour Ajouter une description — facultatif, entrez une description pour aider à identifier la requête dans la liste des requêtes récentes.

7. Développez le code SQL d'aperçu.
  - a. Affichez le code SQL généré à partir du générateur d'analyse.
  - b. Pour copier le code SQL, choisissez Copier.
  - c. Pour modifier le code SQL, choisissez Modifier dans l'éditeur de code SQL.
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 de AWS Clean Rooms](#).

## Interrogation de données avec 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 si le budget de confidentialité restant est insuffisant. 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 texte SQL 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.



# Réception des résultats de requêtes

En tant que [membre qui peut recevoir les résultats](#), vous pouvez recevoir le résultat de la requête depuis AWS Clean Rooms dans le compartiment Amazon S3 que vous avez spécifié lorsque vous avez activé la collaboration.

Les rubriques suivantes expliquent comment recevoir les résultats d'une requête à l'aide de AWS Clean Rooms console.

## Rubriques

- [Recevoir les résultats d'une requête](#)
- [Modifier les valeurs par défaut pour les paramètres des résultats de requête](#)
- [Utilisation du résultat de la requête dans d'autres Services AWS](#)

Pour plus d'informations sur la façon d'interroger des données ou d'afficher des requêtes en appelant le AWS Clean Rooms API directement ou en utilisant le AWS SDK, voir le [AWS Clean Rooms Référence d'API](#).

Pour plus d'informations sur la journalisation des requêtes, voir [Journalisation des requêtes](#).

### Note

Si vous exécutez une requête sur des tables de données chiffrées, les résultats des colonnes chiffrées sont chiffrés.

## Recevoir les résultats d'une requête

Les résultats de la requête apparaîtront dans le Paramètres par défaut des résultats de requêtes section et le Requête section de la Requête onglet dans l'AWS Clean Rooms console.

Pour recevoir les résultats d'une requête

1. Connectez-vous au AWS Management Console et ouvrez le [AWS Clean Rooms console](#) avec votre Compte AWS (si vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, choisissez Collaborations.
3. Choisissez la collaboration qui a Les capacités de vos membres statut de Recevez les résultats.

4. Pour recevoir les résultats de la requête directement depuis AWS Clean Rooms, sur le Requête onglet, sous Requête, en vertu du ID de requête protégé colonne, sélectionnez la requête.
5. Sur le Détails de la requête page, sous Résultats, effectuez l'une des opérations suivantes :

Si tu veux...	Ensuite, choisissez...
Copiez les résultats.	Copy
Téléchargez les résultats.	Download <div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>Par défaut, le nom du fichier téléchargé est le nom correspondant <code>Query id</code> qui était affiché lors de l'exécution de la requête dans AWS Clean Rooms.</p> </div>
Il est possible de voir les résultats apparaître dans Amazon S3.	Afficher dans Amazon S3  La console Amazon S3 apparaîtront dans un onglet séparé.

6. Si vous avez activé vos données cryptées, vous pouvez désormais [déchiffrer](#) les tableaux de données.

Pour plus d'informations, veuillez consulter [Déchiffrer des tables de données avec le client de chiffrement C3R](#).

## Modifier les 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 le AWS Clean Rooms console.

## Pour modifier les valeurs par défaut des paramètres des résultats de requête

1. Connectez-vous à l'[AWS Management Console](#) et ouvrez le [AWS Clean Rooms console](#) avec votre compte AWS (si vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, choisissez **Collaborations**.
3. Choisissez la collaboration qui a les capacités de vos membres et recevez les résultats.
4. Sur le onglet **Requêtes**, sous **Paramètres des résultats de la requête**, choisissez **Modifier**.
5. Sur le 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 la requête**, modifiez la **Destination des résultats** dans **Amazon S3** ou le **Format de résultat**.
  - b. Sous **Accès au service**, modifiez la **Méthode d'autorisation AWS Clean Rooms** d'écrire dans le compartiment **Amazon S3** et le format que vous avez spécifiés.

Le mis à jour **Paramètres des résultats de la requête** apparaît sur la page détaillée de la collaboration.

## Utilisation du résultat de la requête dans d'autres Services AWS

Résultat de la requête de **AWS Clean Rooms** est disponible sur la console (si la console est utilisée pour exécuter des requêtes) et téléchargé dans un compartiment **Amazon S3** spécifié. À partir de là, vous pouvez utiliser le résultat de la requête dans d'autres **Services AWS**, comme **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**, voir le [Amazon QuickSight Documentation](#).

Pour plus d'informations sur **Amazon SageMaker**, voir le [Amazon SageMaker Documentation](#).

# Déchiffrer des tables de données avec le client de chiffrement C3R

Suivez cette procédure pour les collaborations qui utilisent l'informatique cryptographique pour Clean Roomset le client de chiffrement C3R pour chiffrer les tables de données. Utilisez cette procédure après avoir [données demandées 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 Roomsles 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) [Afficher les commandes disponibles dans le client de chiffrement C3R](#).
2. (Facultatif) Accédez au répertoire souhaité et exécutez `ls` (macOS) ou `dir` (Windows).
  - Vérifiez que `c3r-cli.jar` le 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 le AWS Clean Rooms interface de console, ils se trouvent probablement dans le Téléchargements dossier pour votre compte d'utilisateur. (Par exemple, le Téléchargements dossier de votre répertoire utilisateur sur Windows et macOS.) Nous vous recommandons de déplacer le fichier des résultats de la requête dans le même dossier que le `c3r-cli.jar`.

3. Stockez la clé secrète partagée dans le `C3R_SHARED_SECRET` variable d'environnement. Pour plus d'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 chacune *espace réservé à la saisie par l'utilisateur* avec vos propres informations :

- a. Pour `id=`, entrez l'ID de collaboration.
- b. Pour `output=`, spécifiez le nom du fichier de sortie (par exemple, `results-decrypted.csv`).

Si vous ne spécifiez aucun nom de sortie, un nom par défaut s'affiche dans le terminal.

- c. Affichez les données déchiffrées dans le fichier de sortie spécifié à l'aide de votre CSV préféré ou Parquet application de visualisation (telle que Microsoft Excel, un éditeur de texte ou une autre application).

# Gestion d'AWS Clean Rooms

Les rubriques suivantes décrivent comment gérer une collaboration, les membres et les tables configurées à AWS Clean Rooms l'aide de la AWS Clean Rooms console.

Pour plus d'informations sur la gestion de AWS Clean Rooms l'utilisation AWS des SDK, consultez la [référence AWS Clean Rooms d'API](#).

## Rubriques

- [Gérer les collaborations dans AWS Clean Rooms](#)
- [Gestion des tables configurées dans AWS Clean Rooms](#)

## 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 AWS des SDK, consultez la [référence des AWS Clean Rooms API](#).

## Rubriques

- [Collaborations d'édition](#)
- [Supprimer des collaborations](#)
- [Afficher les collaborations](#)
- [Afficher les tables et les règles d'analyse](#)
- [Afficher les journaux d'utilisation différentiels de confidentialité](#)
- [Surveillance du statut des membres](#)
- [Supprimer un membre d'une collaboration](#)
- [Quitter une collaboration](#)
- [Modification des associations de tables configurées](#)
- [Dissociation des tables configurées](#)
- [Modifier une politique de confidentialité différentielle](#)

- [Supprimer une politique de confidentialité différentielle](#)
- [Affichage des paramètres de confidentialité différentiels calculés](#)

## 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 Roomsconsole 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. 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 Roomsconsole 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. 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 Roomsconsole 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. 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 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 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 Roomsconsole 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. 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 Roomsconsole 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 qui contient 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 fournir 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 Roomsconsole 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 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 Roomsconsole 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 N'est plus disponible, consultez la liste des collaborations supprimées et des adhésions pour les collaborations qui ne sont plus disponibles (adhésions supprimées).

## 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 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. 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.

## 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 Roomsconsole 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.

## Surveillance du statut 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 Roomsconsole 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. Consultez le statut de membre de chaque membre.

## 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 Roomsconsole 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. 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 ».

## 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 Roomsconsole 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. 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 Roomsconsole 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. 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.

## 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 Roomsconsole 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 Roomsconsole 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 requête SQL. 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 valeur UCL calculée et exclut les impressions restantes de cet utilisateur lors de l'exécution de la requête. La valeur UCL 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 `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 `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 l'aide de la console AWS Clean Rooms.

Pour plus d'informations sur la gestion des tables configurées à l'aide des SDK AWS, consultez la [référence des AWS Clean Rooms API](#).

### Rubriques

- [Modification des détails d'une table configurée](#)
- [Modification des balises de tableau configurées](#)
- [Modification d'une règle d'analyse de table configurée](#)

- [Suppression d'une règle d'analyse de table configurée](#)

## 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 Roomsconsole 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 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 Roomsconsole 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 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 Roomsconsole 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 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'éditeur JSON.
    - 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 vous ne l'avez pas encore fait).
2. Dans le volet de navigation de gauche, choisissez 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.

# Résolution des problèmes de AWS Clean Rooms

Cette section décrit certains problèmes courants pouvant survenir lors de l'utilisation AWS Clean Roomset comment y remédier.

## Problèmes

- [Une ou plusieurs tables référencées par la requête ne sont pas accessibles par leur rôle de service associé. Le propriétaire de la table/du rôle doit accorder au rôle de service l'accès à la table.](#)
- [Le format de fichier de l'un des ensembles de données sous-jacents n'est pas pris en charge.](#)
- [Les résultats des requêtes ne correspondent pas aux attentes lors de l'utilisation du calcul cryptographique pour Clean Rooms.](#)

Une ou plusieurs tables référencées par la requête ne sont pas accessibles par leur rôle de service associé. Le propriétaire de la table/du rôle doit accorder au rôle de service l'accès à la table.

- Vérifiez que les autorisations pour le rôle de service sont configurées selon les besoins. Pour plus d'informations, voir [Con AWS Clean Rooms figuration](#).

Le format de fichier de l'un des ensembles de données sous-jacents n'est pas pris en charge.

- Assurez-vous que votre jeu 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, veuillez consulter [Formats de données pour AWS Clean Rooms](#).

## Les résultats des requêtes ne correspondent pas aux attentes lors de l'utilisation du calcul cryptographique pour Clean Rooms.

Si vous utilisez le calcul cryptographique pour Clean Rooms (C3R), vérifiez que votre requête utilise correctement les colonnes cryptées :

- Les colonnes scellées ne sont utilisées que dans les clauses `SELECT`.
- Les colonnes d'empreinte ne sont utilisées que dans les clauses `JOIN` (et les clauses `GROUP BY` sous certaines conditions).
- Que tu es seulement `JOIN` les colonnes d'empreinte 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 conformité. Pour en savoir plus sur les programmes de conformité applicables à AWS Clean Rooms, consultez la section [Services AWS concernés par programme de conformité](#) .
- 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](#)
- [Conservation des données dans AWS Clean Rooms](#)
- [Bonnes pratiques en matière de collaboration de données dans AWS Clean Rooms](#)
- [Identity and Access Management pour AWS Clean Rooms](#)
- [Validation de conformité pour AWS Clean Rooms](#)
- [Résilience dans AWS Clean Rooms](#)
- [Sécurité de l'infrastructure dans AWS Clean Rooms](#)
- [Accès AWS Clean Rooms ou AWS Clean Rooms ML à l'aide d'un point de terminaison d'interface \(AWS PrivateLink\)](#)

# 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 Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez [Questions fréquentes \(FAQ\) sur la confidentialité des données](#). Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog [Modèle de responsabilité partagée AWS et RGPD \(Règlement général sur la protection des données\)](#) sur le Blog de sécuritéAWS .

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) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la 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 Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez [Federal Information Processing Standard \(FIPS\) 140-2](#) (Normes de traitement de l'information fédérale).

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 Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI 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 une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à 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 clé KMS, le contenu de vos modèles similaires et de vos tâches de génération de segments similaires est chiffré au repos avec votre clé KMS.

### 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.

## Chiffrement en transit

AWS Clean Rooms utilise le protocole TLS (Transport Layer Security) et le chiffrement côté client pour le chiffrement en transit. La communication se AWS Clean Rooms fait toujours via HTTPS, de 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, consultez [Informatique 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 Les requêtes SQL 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 vous souhaitez supprimer votre modèle de similarité ou les données de travail de génération de segments similaires, utilisez l'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 l'API. 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 dans l'API et que 3 jours se sont écoulés, toutes les données associées au modèle ou à la tâche sont définitivement supprimées.

## Bonnes pratiques en matière de collaboration 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 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](#)
- [Bonnes pratiques d'utilisation des règles d'analyse dans AWS Clean Rooms](#)

## 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 prémunir 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 souhaitez 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 non approuvées.
- 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 non approuvées.

## Identity and Access Management pour AWS Clean Rooms

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS Clean Rooms les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

### Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [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 cas de figure de l'adjoint désorienté entre services](#)
- [Comportements IAM pour le ML AWS Clean Rooms](#)

## 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 soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec AWS Clean Rooms, voir [Comment AWS Clean Rooms fonctionne avec IAM](#).

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaitez peut-être en savoir plus sur la façon d'écrire 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 dans IAM, 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 qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

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 (IAM Identity Center) ou l'authentification unique de votre entreprise sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section [Comment vous connecter à votre compte Compte AWS dans](#) le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer 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 l'utilisateur AWS IAM Identity Center et [Utilisation de l'authentification multifactorielle \(MFA\) dans l'interface AWS](#) dans le Guide de l'utilisateur IAM.

### Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée 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 les [Utilisateur racine d'un compte AWS informations d'identification et les identités IAM](#) 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 Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez [Qu'est-ce que IAM Identity Center ?](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

## Utilisateurs et groupes IAM

Un [utilisateur IAM](#) 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 utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification](#) dans le Guide de l'utilisateur IAM.

Un [groupe IAM](#) est une identité qui concerne un ensemble d'utilisateurs IAM. 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 avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez [Quand créer un utilisateur IAM \(au lieu d'un rôle\)](#) dans le Guide de l'utilisateur IAM.

## Rôles IAM

Un [rôle IAM](#) est une identité au sein de votre Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console [changeant de rôle](#). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez [Utilisation de rôles IAM](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- 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 obtenir des informations sur les rôles pour la fédération, consultez [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. 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 d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez [Différence entre les rôles IAM et les politiques basées sur les ressources](#) dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM 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. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez [Sessions de transmission d'accès](#).
- Rôle de service : il s'agit d'un [rôle IAM](#) attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de 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 qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez [Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2](#) dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez [Quand créer un rôle IAM \(au lieu d'un utilisateur\)](#) dans le Guide de l'utilisateur IAM.

## 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 documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions, ainsi que les ressources sur lesquelles il peut le faire et dans quelles conditions.

Chaque entité IAM (utilisateur ou rôle) démarre sans 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.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

### Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM.

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 découvrir comment choisir entre une politique gérée et une politique en ligne, consultez [Choix entre les politiques gérées et les politiques en ligne](#) dans le Guide de l'utilisateur IAM.

## politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une 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.

- **Limite d'autorisations** : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). 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, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.
- **Politiques de contrôle des services (SCP)** — Les SCP sont des politiques JSON 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 les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez [Fonctionnement des SCP](#) dans le Guide de l'utilisateur AWS Organizations .

- **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 [politiques de séance](#) dans le Guide de l'utilisateur IAM.

## 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 l'utilisateur IAM.

## Comment AWS Clean Rooms fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Clean Rooms, découvrez les fonctionnalités IAM disponibles. AWS Clean Rooms

Fonctionnalités IAM que vous pouvez utiliser avec AWS Clean Rooms

Fonction IAM	AWS Clean Rooms soutien
<a href="#">Politiques basées sur l'identité</a>	Oui
<a href="#">Politiques basées sur les ressources</a>	Partielle
<a href="#">Actions de politique</a>	Oui

Fonction IAM	AWS Clean Rooms soutien
<a href="#">Ressources de politique</a>	Oui
<a href="#">Clés de condition de politique (spécifiques au service)</a>	Partielle
<a href="#">ACL</a>	Non
<a href="#">ABAC (étiquettes dans les politiques)</a>	Oui
<a href="#">Informations d'identification temporaires</a>	Oui
<a href="#">Transmission des sessions d'accès (FAS)</a>	Oui
<a href="#">Fonctions de service</a>	Oui
<a href="#">Rôles liés à un service</a>	Non

Pour obtenir une vue d'ensemble du fonctionnement de la plupart des fonctionnalités IAM AWS Clean Rooms et des autres Services AWS fonctionnalités, consultez le [Services AWS guide de l'utilisateur IAM](#) consacré à leur utilisation.

## 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 des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et 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 découvrir tous les éléments



que vous utilisez dans une politique JSON, consultez [Références des éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.

## 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      Partielle

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que 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 administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez [Différence entre les rôles IAM et les politiques basées sur une ressource](#) dans le Guide de l'utilisateur IAM.

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. [Comportements IAM pour le ML AWS Clean Rooms](#)

## Actions politiques pour AWS Clean Rooms

Prend en charge les actions de politique	Oui
--	-----

Les administrateurs peuvent utiliser les politiques AWS JSON 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 `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. 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, reportez-vous à la section [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 les politiques AWS JSON 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 de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de 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 de leurs ARN, voir [Ressources définies par AWS Clean Rooms](#) dans la référence d'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez [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	Partielle
---	-----------

Les administrateurs peuvent utiliser les politiques AWS JSON 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 accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez [Éléments d'une politique IAM : variables et identifications](#) dans le Guide de l'utilisateur IAM.

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 de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

Pour savoir comment le AWS Clean Rooms ML utilise les clés de condition de politique, consultez [Comportements IAM pour le ML AWS Clean Rooms](#).

## ACL dans AWS Clean Rooms

Prend en charge les listes ACL

Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

## ABAC avec AWS Clean Rooms

Prend en charge ABAC (étiquettes dans les politiques) Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas 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'informations sur l'ABAC, consultez [Qu'est-ce que le contrôle d'accès basé sur les attributs \(ABAC\) ?](#) dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez [Utilisation du contrôle d'accès par attributs \(ABAC\)](#) dans le Guide de l'utilisateur IAM.

## Utilisation d'informations d'identification temporaires avec AWS Clean Rooms

Prend en charge les informations d'identification temporaires Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation [d'IAM](#) dans le guide de l'utilisateur d'IAM.

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 [Changement de rôle \(console\)](#) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. 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 [Informations d'identification de sécurité temporaires dans IAM](#).

## Transférer les sessions d'accès pour AWS Clean Rooms

Prend en charge les sessions d'accès direct (FAS)	Oui
---	-----

Lorsque vous utilisez un utilisateur ou un rôle IAM 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. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez [Transmission des sessions d'accès](#).

## Fonctions du service pour AWS Clean Rooms

Prend en charge les fonctions du service	Oui
--	-----

Une fonction de service est un [rôle IAM](#) qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM.

Pour plus d'informations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le Guide de l'utilisateur IAM.

#### 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 êtes invité à le faire.

## 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 service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez [Services AWS qui fonctionnent 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 à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de l'API AWS. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez [Création de politiques dans l'onglet JSON](#) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS Clean Rooms, y compris le format des ARN 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 [politiques gérées par AWS](#) ou [politiques gérées par AWS pour les activités professionnelles](#) dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule 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 de IAM pour appliquer des autorisations, consultez [politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.



- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez [Validation de politique IAM Access Analyzer](#) dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez [Configuration de l'accès aux API protégé par MFA](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez [Bonnes pratiques de sécurité dans IAM](#) dans le Guide de l'utilisateur IAM.

## 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 l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API 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 [Ajout d'autorisations à un utilisateur](#) dans le Guide de l'utilisateur IAM.

## Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les

autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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 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 Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

## AWS politique gérée : **AWSCleanRoomsReadOnlyAccess**

Vous pouvez vous rattacher `AWSCleanRoomsReadOnlyAccess` à vos principaux IAM.

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 principaux IAM.

Cette politique accorde des autorisations administratives qui permettent un accès complet (lecture, écriture et mise à jour) aux ressources et aux métadonnées dans le cadre 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 (`PassedToServicecondition`) 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 dans IAM.
- `ListPoliciesToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dans IAM.
- `GetPolicyToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dans IAM.
- `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 votre IAM principaux.

Cette politique accorde des autorisations administratives qui permettent un accès complet (lecture, écriture et mise à jour) aux ressources et aux métadonnées dans le cadre 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 (`PassedToServicecondition`) 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 dans IAM.
- **ListPoliciesToInspectServiceRolePolicy**— Permet aux principaux de voir le rôle du service et la politique correspondante dans IAM.
- **GetPolicyToInspectServiceRolePolicy**— Permet aux principaux de voir le rôle du service et la politique correspondante dans IAM.
- **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.

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

```
{
  "Sid": "CleanRoomsAccess",
  "Effect": "Allow",
  "Action": [
    "cleanrooms:BatchGetCollaborationAnalysisTemplate",
    "cleanrooms:BatchGetSchema",
    "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 principaux IAM.

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 **AWSCleanRoomsMLFullAccess** à vos principaux IAM. 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 (`PassedToServicecondition`) 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 ; le SID de navigation dans la console n'est requis 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 dans IAM.
- `ListPoliciesToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dans IAM.
- `GetPolicyToInspectServiceRolePolicy`— Permet aux principaux de voir le rôle du service et la politique correspondante dans IAM.
- `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 flux RSS sur la page Historique du AWS Clean Rooms document.

Modification	Description	Date
<a href="#">AWSCleanRoomsFullAccess</a> – 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
<a href="#">AWSCleanRoomsMLReadOnlyAccess</a> : nouvelle politique  <a href="#">AWSCleanRoomsMLFullAccess</a> : nouvelle politique	Ajouté AWSCleanRoomsMLReadOnlyAccess et AWSCleanRoomsMLFullAccess pour prendre en charge le AWS Clean Rooms ML.	29 novembre 2023

Modification	Description	Date
<a href="#">AWSCleanRoomsFullAccessNoQuering</a> – Mise à jour de la politique existante	Ajout de cleanrooms:CreateAnalysisTemplate,cleanrooms:GetAnalysisTemplate,cleanrooms:UpdateAnalysisTemplate, cleanrooms:DeleteAnalysisTemplate,cleanrooms:ListAnalysisTemplates,cleanrooms:GetCollaborationAnalysisTemplate,cleanrooms:BatchGetCollaborationAnalysisTemplate, et cleanrooms:ListCollaborationAnalysisTemplates CleanRoomsAccess pour activer la nouvelle fonctionnalité de modèles d'analyse.	31 juillet 2023
<a href="#">AWSCleanRoomsFullAccessNoQuering</a> – 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 IAM.

### 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 quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource `my-example-widget` fictive, mais ne dispose pas des autorisations `cleanrooms:GetWidget` 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 services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans AWS Clean Rooms. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction 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, consultez [Comment AWS Clean Rooms fonctionne avec IAM](#).
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section [Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez](#) dans le Guide de l'utilisateur IAM.
- 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 l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez [Fournir un accès à des utilisateurs authentifiés en externe \(fédération d'identité\)](#) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des stratégies basées sur les ressources pour l'accès comptes multiples, consultez [Différence entre les rôles IAM et les stratégies basées sur les ressources](#) dans le Guide de l'utilisateur IAM.

## Prévention du cas de figure de l'adjoint désorienté 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 la confusion des 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 AWS Clean 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 député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Dans AWS Clean Rooms, vous devez également comparer avec la clé de `sts:ExternalId` condition.

La valeur de `aws:SourceArn` doit être définie sur l'ARN de l'appartenance au rôle assumé.

L'exemple suivant montre comment vous pouvez utiliser la clé de contexte de condition `aws:SourceArn` globale AWS Clean 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 AWS Clean Rooms utilisé pour accéder aux données des clients.

La valeur de *MembershipID* est votre identifiant de AWS Clean Rooms membre dans 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"
      }
    }
  }
]
```

## Comportements IAM pour le ML AWS Clean Rooms

### 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 situé dans Compte AWS A appelle `StartAudienceGenerationJob` une `ConfiguredAudienceModel` ressource appartenant à Compte AWS B, Clean Rooms ML crée deux ARN pour la tâche. Un ARN dans Compte AWS A et un autre dans Compte AWS B. Les ARN sont identiques à l'exception du leur. Compte AWS

Clean Rooms ML crée deux ARN pour la tâche afin de garantir que les deux comptes peuvent appliquer leurs propres politiques IAM 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 les `Export` API sur le tas en utilisant l'ARN avec leur propre Compte AWS identifiant.

Aucun des deux ne Compte AWS peut accéder à la tâche en utilisant un ARN avec l'autre Compte AWS ID.

Le nom de la tâche doit être unique dans 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 l'[API AWS Clean Rooms ML](#) pour créer un modèle similaire configuré avec `manageResourcePolicies` set 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 ressources IAM pour agir `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 marquage

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 [StartAudienceGenerationJob](#) demande. 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. Toutes les autres API de Clean Rooms ML ne peuvent être utilisées 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. 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 Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité](#) spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- [Guides de démarrage rapide sur la sécurité et la conformité](#) : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- [Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services](#) : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

### Note

Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le [HIPAA Eligible Services Reference](#).

- AWS Ressources de <https://aws.amazon.com/compliance/resources/> de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- [AWS Guides de conformité destinés aux clients](#) — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- [Évaluation des ressources à l'aide des règles](#) du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- [AWS Security Hub](#)— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez [Référence des contrôles Security Hub](#).
- [AWS Audit Manager](#)— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

## 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 des appels d'API AWS publiés pour accéder AWS Clean Rooms via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou 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 ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. 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 transit est signé par le protocole Amazon Signature Version 4 (SIGv4) et chiffré via HTTPS. Ce trafic est autorisé en fonction du rôle de service IAM 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 fonctionnent uniquement en HTTPS. Vous pouvez utiliser les points de terminaison Amazon Virtual Private Cloud (VPC) au cas où vous souhaiteriez vous connecter depuis AWS Clean Rooms votre VPC sans avoir de connexion Internet. Pour plus d'informations, consultez la section [Accès aux AWS services AWS PrivateLink](#) dans le AWS PrivateLink Guide.



Vous pouvez attribuer des politiques IAM à vos principaux IAM en utilisant les [clés de SourceVpce contexte aws](#) : pour empêcher votre principal IAM de ne pouvoir passer des appels que via AWS Clean Rooms un point de terminaison VPC 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, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou AWS Direct Connect de connexion. Les instances de votre VPC 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 Services AWS 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 actions d'API via le point de terminaison de l'interface.

Les politiques de point de terminaison VPC ne sont pas prises en charge pour le ML AWS Clean Rooms . AWS Clean Rooms 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 console Amazon VPC 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 DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à AWS Clean Rooms l'aide de son nom DNS 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 [Comportements IAM pour le ML AWS Clean Rooms](#).

- AWS CloudTrail capture 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 Rooms est intégré à AWS CloudTrail, un service qui enregistre les actions effectuées par un utilisateur, un rôle ou un Service AWS dans AWS Clean Rooms. CloudTrail capture les appels d'API vers AWS 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'événements CloudTrail à un compartiment Amazon S3, y compris des événements pour AWS 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 à AWS 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 de AWS CloudTrail l'utilisateur](#).

## AWS Clean Rooms informations dans CloudTrail

CloudTrail est activé dans votre Compte AWS lors de la création de ce dernier. Lorsqu'une activité a lieu dans AWS Clean Rooms, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS 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'autres Services AWS 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 les AWS Clean Rooms actions sont enregistrées CloudTrail et documentées dans la [référence de AWS 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 Service AWS.

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

[CreateTrainingDataset](#) dans 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 Service AWS. Sauf indication contraire, chaque quota est spécifique à un Région AWS. Vous pouvez demander des augmentations de 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 panneau de navigation, choisissez AWS services (Services AWS) et 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 Service Quotas, utilisez le [Formulaire d'augmentation de limite 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

Ressource	Par défaut	Description
Demandes continues simultanées par membre	5	Nombre maximum de requêtes en cours simultanées par membre
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.

### Limites des paramètres de ressources

Ressource	Par défaut	Description
Taille de la règle d'analyse	100 Ko	Taille maximale du JSON pour une règle d'analyse
Longueur du texte de la requête	90 Ko (8 Ko pour les requêtes de confidentialité différentes)	Longueur de texte maximale pour une instruction de requête SQL
Durée d'exécution de la requête	12 heures	Durée maximale pendant laquelle une requête est exécutée avant l'expiration du délai

Vous Compte AWS disposez des quotas de transaction API par seconde (TPS) suivants par compte et par point de terminaison.

#### Quotas de limitation de l'API

Ressource	Limite de débit	Description
Taux de BatchGetCollaborationAnalysisTemplate demandes	5 TPS	Nombre maximal d'appels d'BatchGetCollaborationAnalysisTemplate API par seconde
Taux de BatchGetSchema demandes	5 TPS	Nombre maximal d'appels d'BatchGetSchema API par seconde
Taux de CreateAnalysisTemplate demandes	5 TPS	Nombre maximal d'appels d>CreateAnalysisTemplate API par seconde
Taux de CreateCollaboration demandes	5 TPS	Nombre maximal d'appels d>CreateCollaboration API par seconde
Taux de CreateConfiguredAudienceModelAssociation demandes	5 TPS	Nombre maximal d'appels CreateConfiguredAudienceModelAssociation par seconde
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

Ressource	Limite de débit	Description
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 CreatePrivacyBudgetTemplate 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
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



Ressource	Limite de débit	Description
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
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

Ressource	Limite de débit	Description
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
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

Ressource	Limite de débit	Description
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
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

Ressource	Limite de débit	Description
Taux de <code>ListConfiguredTables</code> demandes	5 TPS	Nombre maximal d'appels <code>ListConfiguredTables</code> par seconde
Taux de <code>ListMembers</code> demandes	5 TPS	Nombre maximal d'appels <code>ListMembers</code> par seconde
Taux de <code>ListMemberships</code> demandes	5 TPS	Nombre maximal d'appels <code>ListMemberships</code> par seconde
Taux de <code>ListPrivacyBudgets</code> demandes	5 TPS	Nombre maximal d'appels <code>ListPrivacyBudgets</code> par seconde
Taux de <code>ListPrivacyBudgetTemplates</code> demandes	5 TPS	Nombre maximal d'appels <code>ListPrivacyBudgetTemplates</code> par seconde
Taux de <code>ListProtectedQueries</code> demandes	5 TPS	Nombre maximal d'appels <code>ListProtectedQueries</code> par seconde
Taux de <code>ListSchemas</code> demandes	5 TPS	Nombre maximal d'appels <code>ListSchemas</code> par seconde
Taux de <code>StartProtectedQuery</code> demandes	5 TPS	Nombre maximal d'appels <code>StartProtectedQuery</code> par seconde
Taux de <code>UpdateAnalysisTemplate</code> demandes	5 TPS	Nombre maximal d'appels <code>UpdateAnalysisTemplate</code> par seconde
Taux de <code>UpdateCollaboration</code> demandes	5 TPS	Nombre maximal d'appels <code>UpdateCollaboration</code> par seconde

Ressource	Limite de débit	Description
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 de limitation de l'API ML

Ressource	Limite de débit	Description
Taux de CreateAudienceModel demandes	Taux de 1 TPS, rafale de 3 TPS	Nombre maximal d'appels d>CreateAudienceModel API par seconde
Taux de CreateConfiguredAudienceModel demandes	10 TPS	Nombre maximal d'appels d>CreateConfiguredAudienceModel API par seconde

Ressource	Limite de débit	Description
Taux de CreateTrainingDataset demandes	10 TPS	Nombre maximal d'appels d>CreateTrainingDataset API par seconde
Taux de DeleteAudienceGenerationJob demandes	Débit de 2 TPS, rafale de 10 TPS	Nombre maximal d'appels d>DeleteAudienceGenerationJob API par seconde
Taux de DeleteAudienceModel demandes	Débit de 2 TPS, rafale de 10 TPS	Nombre maximal d'appels d>DeleteAudienceModel API par seconde
Taux de DeleteConfiguredAudienceModel demandes	10 TPS	Nombre maximal d'appels d>DeleteConfiguredAudienceModel API par seconde
Taux de DeleteConfiguredAudienceModelPolicy demandes	25 TPS	Nombre maximal d'appels d>DeleteConfiguredAudienceModelPolicy API par seconde
Taux de DeleteTrainingDataset demandes	10 TPS	Nombre maximal d'appels d>DeleteTrainingDataset API par seconde
Taux de GetAudienceGenerationJob demandes	50 TPS	Nombre maximal d'appels d'GetAudienceGenerationJob API par seconde
Taux de GetAudienceModel demandes	50 TPS	Nombre maximal d'appels d'GetAudienceModel API par seconde

Ressource	Limite de débit	Description
Taux de <code>GetConfiguredAudienceModel</code> demandes	50 TPS	Nombre maximal d'appels d' <code>GetConfiguredAudienceModel</code> API par seconde
Taux de <code>GetConfiguredAudienceModelPolicy</code> demandes	50 TPS	Nombre maximal d'appels d' <code>GetConfiguredAudienceModelPolicy</code> API par seconde
Taux de <code>GetTrainingDataset</code> demandes	50 TPS	Nombre maximal d'appels d' <code>GetTrainingDataset</code> API par seconde
Taux de <code>ListAudienceExportJobs</code> demandes	50 TPS	Nombre maximal d'appels d' <code>ListAudienceExportJobs</code> API par seconde
Taux de <code>ListAudienceGenerationJobs</code> demandes	50 TPS	Nombre maximal d'appels d' <code>ListAudienceGenerationJobs</code> API par seconde
Taux de <code>ListAudienceModels</code> demandes	50 TPS	Nombre maximal d'appels d' <code>ListAudienceModels</code> API par seconde
Taux de <code>ListConfiguredAudienceModels</code> demandes	50 TPS	Nombre maximal d'appels d' <code>ListConfiguredAudienceModels</code> API par seconde
Taux de <code>ListTagsForResource</code> demandes	50 TPS	Nombre maximal d'appels d' <code>ListTagsForResource</code> API par seconde

Ressource	Limite de débit	Description
Taux de ListTrainingDatasets demandes	50 TPS	Nombre maximal d'appels d>ListTrainingDatasets API par seconde
Taux de PutConfiguredAudienceModelPolicy demandes	25 TPS	Nombre maximal d'appels d'PutConfiguredAudienceModelPolicy API par seconde
Taux de StartAudienceExportJob demandes	Taux de 1 TPS, rafale de 3 TPS	Nombre maximal d'appels d'StartAudienceExportJob API par seconde
Taux de StartAudienceGenerationJob demandes	Débit de 1 TPS, rafale de 5 TPS	Nombre maximal d'appels d'StartAudienceGenerationJob API par seconde
Taux de TagResource demandes	10 TPS	Nombre maximal d'appels d'TagResource API par seconde
Taux de UntagResource demandes	50 TPS	Nombre maximal d'appels d'UntagResource API par seconde
Taux de UpdateConfiguredAudienceModel demandes	10 TPS	Nombre maximal d'appels d'UpdateConfiguredAudienceModel API par seconde

Nom	Par défaut	Ajusté	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



Nom	Par défaut	Ajusté	Description
			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	<a href="#">Oui</a>	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	<a href="#">Oui</a>	Le nombre maximum de tâches de formation sur les modèles d'audience en attente ou en cours par client

### Quotas ML pour Clean Rooms

Ressource	Par défaut	Description
Ensembles de données	par tâche	
Nombre maximum d'interactions	20 milliards	Nombre maximum d'interactions autorisées dans les données d'entraînement. Les entrées plus importantes sont échantillonnées vers le bas.
Nombre minimal d'interactions	1 million	
Nombre maximum d'utilisateurs distincts pour la formation sur les modèles similaires	100 000	Si d'autres sont inclus, seuls les 100 millions les plus populaires sont utilisés,

Ressource	Par défaut	Description
		classés en fonction du nombre d'interactions.
Nombre minimal d'utilisateurs distincts pour la formation sur les modèles similaires	1 million	
Nombre maximum d'utilisateurs pour la tâche d'exportation portant sur un segment similaire (audience)	10 000	
Nombre maximum d'éléments distincts utilisés pour l'entraînement des modèles.	1 million	Vous pouvez inclure jusqu'à 50 millions d'articles, mais seul le million le plus populaire est utilisé.
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.
API	par client	

Ressource	Par défaut	Description
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	
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.
Pourcentage minimum pour une classe de taille de segment (audience)	1 %	
Pourcentage maximal pour un groupe de taille de segment (audience)	20 %	

Ressource	Par défaut	Description
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 recevoir les notifications sur les mises à jour de cette documentation, vous pouvez vous abonner au Flux RSS. Pour vous abonner aux mises à jour RSS, un plug-in RSS doit être activé pour le navigateur que vous utilisez.

Modification	Description	Date
<a href="#">AWS Clean Rooms ML est désormais entièrement disponible</a>	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
<a href="#">Mise à jour de la politique existante</a>	L'ID de déclaration dans la politique <code>AWSCleanRoomsFullAccess</code> gérée a été mis à jour de <code>ConsolePickQueryResultsBucket</code> à <code>SetQueryResultsBucket</code> pour mieux représenter les autorisations depuis les autorisations.	21 mars 2024
<a href="#">Nouvelles politiques gérées pour le machine AWS Clean Rooms learning</a>	Deux nouvelles politiques gérées ont été ajoutées : <code>AWSCleanRoomsMLReadOnlyAccess</code> et <code>AWSCleanRoomsMLFullAccess</code> .	29 novembre 2023

---

<a href="#">AWS Clean Rooms ML (aperçu)</a>	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
<a href="#">AWS Clean Rooms Confidentialité différentielle (version préliminaire)</a>	Les clients peuvent désormais utiliser la confidentialité AWS Clean Rooms différentielle pour protéger la vie privée de leurs utilisateurs.	29 novembre 2023
<a href="#">Configuration du paiement</a>	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
<a href="#">Durée d'exécution de la requête - mise à jour</a>	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 Protected QueryOutputConfiguration  
AWS::CleanRooms::Membership ProtectedQueryResultConfiguration ,  
etAWS::CleanRooms::Membership Protected QueryS3OutputConfiguration .

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

<a href="#">AWS Clean Rooms Glossaire</a>	Mise à jour portant uniquement sur la documentation pour ajouter un glossaire des termes. AWS Clean Rooms	30 août 2023
<a href="#">Support pour les Apache Iceberg tableaux (version préliminaire)</a>	AWS Clean Rooms prend désormais en charge Apache Iceberg les tableaux (aperçu).	25 août 2023
<a href="#">Mise à jour des quotas</a>	La <a href="#">section Quotas</a> a été mise à jour pour refléter le nouveau quota par défaut d'abonnements par compte.	9 août 2023
<a href="#">Mise à jour de la politique existante</a>	Les nouvelles autorisations suivantes ont été ajoutées à la politique AWSCleanRoomsFullAccessNoQuering gérée : cleanrooms:CreateAnalysisTemplate , cleanrooms:GetAnalysisTemplate , cleanrooms:UpdateAnalysisTemplate , cleanrooms>DeleteAnalysisTemplate , cleanrooms>ListAnalysisTemplates , cleanrooms:GetCollaborationAnalysisTemplate , cleanrooms:BatchGetCollaborationAnalysisTemplate , et cleanrooms>ListCollaborationAnalysisTemplates .	31 juillet 2023



<a href="#">Modèles d'analyse et règle d'analyse personnalisée</a>	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 requête SQL personnalisée à utiliser dans le cadre de la collaboration. Avec la règle d'analyse personnalisée, le propriétaire de la table peut approuver des requêtes SQL personnalisées sur ses tables configurées.	31 juillet 2023
<a href="#">Les règles d'analyse prennent en charge la condition OR logique</a>	AWS Clean Rooms les règles d'analyse prennent désormais en charge la condition OR logique de la JOIN clause.	29 juin 2023
<a href="#">CloudFormation intégration</a>	AWS Clean Rooms s'intègre désormais à AWS CloudFormation.	15 juin 2023
<a href="#">Générateur d'analyses</a>	Les membres autorisés à effectuer des requêtes et à recevoir des résultats peuvent désormais exécuter des requêtes sur certaines tables sans écrire de code SQL à l'aide de l'interface utilisateur du générateur d'analyse.	15 juin 2023
<a href="#">fonctions SQL</a>	Mise à jour uniquement destinée à la documentation pour clarifier les fonctions SQL prises en charge.	5 mai 2023

<a href="#">Dépannage</a>	Mise à jour basée uniquement sur la documentation pour ajouter une section de résolution des problèmes courants.	27 avril 2023
<a href="#">Types de données pris en charge pour AWS Clean Rooms</a>	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
<a href="#">Exemples d' AWS CloudTrail événements</a>	Mise à jour de documentation uniquement pour ajouter des exemples d' CloudTrail événements pour StartProtectedQuery (réussite) et StartProtectedQuery (échec).	20 avril 2023
<a href="#">Mise à jour de la politique existante</a>	Les nouvelles autorisations suivantes ont été ajoutées à la politique AWSCleanRoomsFullAccessNoQuerying gérée :cleanrooms:ListTagsForResource ,cleanrooms:UntagResource , etcleanrooms:TagResource . Pour plus d'informations, consultez la section <a href="#">Politiques AWS gérées</a> .	21 mars 2023
<a href="#">Disponibilité générale</a>	AWS Clean Rooms est désormais disponible pour tous.	21 mars 2023

[Version préliminaire](#)

Version préliminaire du guide  
de AWS Clean Rooms l'utilisa  
teur

12 janvier 2023

# Glossaire AWS Clean Rooms

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 des analyses utilisant COUNT ou AVG fonctionnant selon des dimensions facultatives. SUM 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 requêtes SQL personnalisées prises en charge dans AWS Clean Rooms.

Peut contenir des paramètres là où une valeur littérale peut généralement apparaître dans une requête SQL. Pour plus d'informations sur les types de paramètres pris en charge, consultez la section [Types de données](#) de la référence AWS Clean Rooms SQL.

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 SDK de chiffrement côté client doté d'une interface en ligne de commande.

## Colonne en texte clair

Colonne qui n'est pas protégée cryptographiquement pour une construction JOIN ou une construction SELECT SQL.

Les colonnes en texte clair peuvent être utilisées dans n'importe quelle partie de la requête SQL.

## Collaboration

Limite logique sécurisée AWS Clean Rooms dans laquelle les membres peuvent effectuer des requêtes SQL 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 sur AWS Glue, consultez le [Manuel du développeur AWS Glue](#).

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.

## 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 construction JOIN SQL.

## 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.

## 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 principaux IAM (tels que les utilisateurs ou les rôles) peut interroger des données dans le cadre de la collaboration. Pour en savoir plus, consultez [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 construction SELECT SQL.



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.