Manual do usuário

AWS Clean Rooms

AWS Clean Rooms: Manual do usuário

Table of Contents

O que é AWS Clean Rooms?

AWS Clean Rooms ajuda você e seus parceiros a analisar e colaborar em seus conjuntos de dados coletivos para obter novos insights sem revelar dados subjacentes uns aos outros. Você pode usar AWS Clean Rooms um espaço de trabalho de colaboração seguro para criar suas próprias salas limpas em minutos e começar a analisar seus conjuntos de dados coletivos com apenas algumas etapas. É possível escolher os parceiros com os quais deseja colaborar, selecionar seus conjuntos de dados e configurar restrições para os participantes.

Com AWS Clean Rooms, você pode colaborar com milhares de empresas que já usam AWS. A colaboração não exige que os dados sejam retirados AWS ou carregados em outra plataforma. Quando você executa consultas, AWS Clean Rooms lê os dados de seu local original e aplica regras de análise integradas para ajudá-lo a manter o controle sobre seus dados.

AWS Clean Rooms fornece controles integrados de acesso a dados e controles de suporte de auditoria que você pode configurar. Os controles incluem:

- Regras de análise para restringir consultas SQL e fornecer restrições de saída
- Computação criptográfica para o Clean Rooms manter os dados criptografados, mesmo quando as consultas são processadas, para cumprir políticas rigorosas de tratamento de dados
- Logs de consulta para revisar consultas e ajudar a apoiar auditorias
- Privacidade diferencial para proteção contra tentativas de identificação do usuário. AWS Clean Rooms A Privacidade Diferencial é um recurso totalmente gerenciado que protege a privacidade de seus usuários com técnicas baseadas em matemática e controles intuitivos que você pode aplicar em alguns cliques.
- AWS Clean Rooms ML para permitir que duas partes identifiquem usuários semelhantes em seus dados sem a necessidade de compartilhar seus dados entre si. A primeira parte cria e configura um modelo de semelhanças com base nos dados de treinamento. A segunda parte traz os dados de seed para uma colaboração e cria um segmento de semelhanças aos dados de treinamento.

O vídeo a seguir explica mais sobre AWS Clean Rooms.

AWS Clean Rooms

Você é um AWS Clean Rooms usuário iniciante?

Se você é usuário iniciante do AWS Clean Rooms, recomendamos que comece lendo as seguintes seções:

- Como AWS Clean Rooms funciona
- Acessando AWS Clean Rooms
- Conf AWS Clean Rooms iguração
- AWS Clean Rooms Glossário

Como AWS Clean Rooms funciona

O fluxo de trabalho a seguir pressupõe que:

- O membro da colaboração já fez o upload de suas tabelas de dados para o Amazon S3 e criou uma AWS Glue tabela.
- (Opcional) Somente para tabelas de dados criptografadas, o membro da colaboração já preparou tabelas de dados criptografadas usando o cliente de criptografia C3R.

Em resumo, o fluxo de trabalho para AWS Clean Rooms é o seguinte:

1. O criador da colaboração executa as seguintes tarefas:
   - Cria uma colaboração.
   - Convida um ou mais membros para a colaboração.
   - Atribui habilidades aos membros, como o membro que pode consultar e o membro que pode receber resultados.

     Se o criador da colaboração também for o membro que pode receber os resultados, ele especificará o destino e o formato dos resultados de consulta. Eles também fornecem um perfil de serviço nome do recurso da Amazon (ARN) para gravar os resultados no destino dos resultados de consulta.
   - Configura qual membro é responsável por pagar pelos custos de computação da consulta na colaboração.
2. O membro convidado se junta à colaboração criando um recurso de associação.

Se o membro convidado for o membro que pode receber os resultados, ele especificará o destino e o formato dos resultados de consulta. Eles também fornecem um perfil de serviço ARN para gravar no destino dos resultados de consulta.

Se o membro convidado for o membro responsável por pagar pelos custos de computação da consulta, ele aceitará suas responsabilidades de pagamento antes de ingressar na colaboração.

3. O membro configura uma AWS Glue tabela existente para uso em AWS Clean Rooms. (Essa etapa pode ser realizada antes ou depois de ingressar em uma colaboração, a menos que seja usada a Computação Criptográfica para o Clean Rooms.)

> **Note**
>
> AWS Clean Rooms suporta AWS Glue tabelas. Para obter mais informações sobre como obter os dados no AWS Glue, consulte Etapa 3: Carregar seu backup no Amazon S3.

1. O membro nomeia a tabela configurada e escolhe quais colunas usar na colaboração.
2. O membro configura uma das seguintes regras de análise na tabela configurada:
   - Regra de análise de agregação ou regra de análise de lista – Para controlar o tipo de análise que pode ser executada na tabela.
   - Regra de análise personalizada – Para permitir um conjunto específico de consultas pré-aprovadas ou um conjunto específico de contas que possam fornecer consultas que usem seus dados. Permite que o membro ative a privacidade diferencial para se proteger contra tentativas de identificação do usuário.

> **Note**
>
> O membro pode configurar a regra de análise a qualquer momento antes de associar suas tabelas configuradas à colaboração.

4. O membro associa suas tabelas configuradas à colaboração e atribui AWS Clean Rooms uma função de serviço para acessar suas AWS Glue tabelas.

> **Note**
>
> Esse perfil de serviço tem permissões para as tabelas. A função de serviço só pode ser assumida AWS Clean Rooms executando consultas permitidas em nome do membro

que pode consultar. Nenhum membro da colaboração (exceto o proprietário dos dados) tem acesso às tabelas subjacentes na colaboração. O proprietário dos dados pode ativar a privacidade diferencial para disponibilizar suas tabelas para consulta por outros membros.

5. O membro que pode consultar executa consultas SQL nas tabelas configuradas.

   As consultas só podem ser executadas se o membro responsável por pagar pelos custos de computação da consulta tiver ingressado na colaboração como membro ativo.

   As regras de análise e as restrições de saída são aplicadas automaticamente. AWS Clean Rooms retorna somente os resultados que estão em conformidade com as regras de análise definidas na Etapa 3.b.

   Para consultas sobre dados criptografados, o membro que pode receber os resultados recebe a saída criptografada AWS Clean Rooms que deve ser descriptografada (consulte a Etapa 8).

6. O membro que pode receber os resultados analisa os resultados no AWS Clean Rooms console ou no bucket do Amazon S3 que ele especificou.
7. O membro que paga pelos custos de computação da consulta é cobrado pelas consultas executadas na colaboração.
8. (Opcional) Somente para tabelas de dados criptografadas, o membro que pode receber os resultados descriptografa os resultados de consulta executando o cliente de criptografia C3R no modo de descriptografia.

Serviços relacionados

Os itens a seguir Serviços da AWS estão relacionados a AWS Clean Rooms:

- Amazon S3

  Os membros da colaboração podem armazenar dados que eles trazem para AWS Clean Rooms o Amazon S3.

  Para obter mais informações, consulte os tópicos a seguir.

  Preparando tabelas de dados para consultas no AWS Clean Rooms

  O que é o Amazon S3? no Guia do usuário do Amazon Simple Storage Service

- AWS Glue

  Os membros da colaboração podem criar AWS Glue tabelas a partir de seus dados no Amazon S3 para uso em. AWS Clean Rooms

  Para obter mais informações, consulte os tópicos a seguir.

  Preparando tabelas de dados para consultas no AWS Clean Rooms

  O que é o AWS Glue? no Guia do desenvolvedor do AWS Glue

- AWS CloudFormation

  Crie os seguintes recursos em AWS CloudFormation: colaborações, tabelas configuradas, associações de tabelas configuradas e associações

  Para ter mais informações, consulte Criando AWS Clean Rooms recursos com AWS CloudFormation.

- AWS CloudTrail

  Use AWS Clean Rooms com CloudTrail registros para aprimorar sua análise da AWS service (Serviço da AWS) atividade.

  Para ter mais informações, consulte Registrar em log chamadas de API do AWS Clean Rooms usando o AWS CloudTrail.

Acessando AWS Clean Rooms

Você pode acessar AWS Clean Rooms por meio das seguintes opções:

- Diretamente pelo AWS Clean Rooms console em https://console.aws.amazon.com/cleanrooms/.
- Programaticamente por meio da API. AWS Clean Rooms Para obter mais informações, consulte a Referência da API do AWS Clean Rooms .

Preços para AWS Clean Rooms

Para obter informações sobre a definição de preço, consulte Definição de preço do AWS Clean Rooms.

Faturamento para AWS Clean Rooms

AWS Clean Rooms dá ao criador da colaboração a capacidade de configurar qual membro está pagando pelos custos de computação da consulta na colaboração.

Na maioria dos casos, o membro que pode consultar e o membro que paga pelos custos de computação da consulta são os mesmos. No entanto, se o membro que pode consultar e o membro que paga pelos custos de computação da consulta forem diferentes, então, quando o membro que pode consultar executa consultas em seu próprio recurso de associação, o recurso de associação do membro que paga pelos custos de computação da consulta é cobrado.

O membro que paga pelos custos de computação da consulta não vê nenhum evento para consultas sendo executadas em seu histórico de CloudTrail eventos porque o pagador não é quem está executando as consultas nem o proprietário do recurso no qual as consultas são executadas. No entanto, o pagador vê as contas geradas em seu recurso de associação para todas as consultas executadas pelo membro que pode executar consultas na colaboração.

Para obter mais informações sobre como criar uma colaboração e configurar o membro que pague pelos custos de computação da consulta, consulte Crie uma colaboração.

Regras de análise em AWS Clean Rooms

Como parte da habilitação de uma tabela para uso na AWS Clean Rooms análise de colaboração, o membro da colaboração deve configurar uma regra de análise.

Uma regra de análise é um controle de aprimoramento de privacidade que cada proprietário de dados configura em uma tabela configurada. Uma regra de análise determina como a tabela configurada pode ser analisada.

A regra de análise é um controle em nível de conta na tabela configurada (um recurso em nível de conta) e é aplicada em qualquer colaboração em que a tabela configurada esteja associada. Se não houver uma regra de análise configurada, a tabela configurada poderá ser associada às colaborações, mas não poderá ser consultada. As consultas só podem fazer referência a tabelas configuradas com o mesmo tipo de regra de análise.

Para configurar uma regra de análise, primeiro você seleciona um tipo de análise e depois especifica a regra de análise. Em ambas as etapas, você deve considerar o caso de uso que deseja habilitar e como deseja proteger seus dados subjacentes.

AWS Clean Rooms impõe os controles mais restritivos em todas as tabelas configuradas referenciadas em uma consulta.

Os exemplos a seguir ilustram os controles restritivos.

Example Controle restritivo: restrição de saída

- O colaborador A tem uma restrição de saída na coluna identificadora de 100.
- O colaborador B tem uma restrição de saída na coluna identificadora de 150.

  Uma consulta de agregação que faz referência às duas tabelas configuradas requer pelo menos 150 valores distintos de identificador em uma linha de saída para que seja exibida na saída da consulta. A saída da consulta não indica que os resultados foram removidos devido à restrição de saída.

Example Controle restritivo: modelo de análise não aprovado

- O Colaborador A permitiu um modelo de análise com uma consulta que faz referência às tabelas configuradas do Colaborador A e do Colaborador B em sua regra de análise personalizada.
- O colaborador B não permitiu o modelo de análise.

Como o Colaborador B não permitiu o modelo de análise, o membro que pode consultar não pode executar esse modelo de análise.

Tipos de regras de análise

Há três tipos de regras de análise: agregação, lista e personalizada. As tabelas a seguir comparam os tipos de regras de análise. Cada tipo tem uma seção separada que descreve a especificação da regra de análise.

As tabelas a seguir mostram um resumo comparativo dos tipos de regras de análise.

Casos de uso compatíveis

As tabelas a seguir mostram um resumo comparativo dos casos de uso compatíveis para cada tipo de regra de análise.

Caso de uso	Agregação	Lista	Custom (Personalizado)
Análises suportadas	Consultas que agregam estatísticas usando as funções COUNT, SUM e AVG em dimensões opcionais	Consultas que geram listas em nível de linha da sobreposição entre várias tabelas	Qualquer análise personalizada, desde que o modelo de análise ou o criador da análise tenham sido revisados e permitidos
Casos de uso comuns	Análise, mensuração e	Enriquecimento, construçã	Atribuição no primeiro toque,

Caso de uso	Agregação	Lista	Custom (Personalizado)
	atribuição de segmentos	o de segmentos	análises incrementais, descoberta de público
Estruturas de SQL	• Declarações JOIN: INNER JOIN • Funções agregadas: COUNT/ COUNT DISTINCT, SUM/ SUM DISTINCT e AVG • Funções escalares: subconjunto limitado	• Declarações JOIN: INNER JOIN • Funções escalares: nenhuma	A maioria das funções SQL e construções SQL disponíveis com o comando SELECT
Subconsultas e expressões de tabela comuns (CTEs)	Não	Não	Sim

Caso de uso	Agregação	Lista	Custom (Personalizado)
Modelos de análise	Não	Não	Sim

Controles compatíveis

As tabelas a seguir mostram um resumo comparativo de como cada tipo de regra de análise protege seus dados subjacentes.

Controle	Agregação	Lista	Custom (Personalizado)
Mecanismo de controle	Controle como os dados na tabela podem ser usados em uma consulta (Por exemplo, permita COUNT e SUM da coluna hashed_email.)	Controle como os dados na tabela podem ser usados em uma consulta (Por exemplo, permita o uso da coluna hashed_email somente para junção.)	Controle quais consultas podem ser executadas na tabela (Por exemplo, permita somente consultas definidas nos modelos de análise “Consulta personalizada 1".)

Controle	Agregação	Lista	Custom (Personalizado)
Técnicas de aprimoramento de privacidade integradas	• Correspondência às cegas • Agregação necessária • Limite mínimo de agregação >= • 2 Estrutura de consulta predefinida	• Correspondência às cegas • Sobreposição necessária • Estrutura de consulta predefinida	Privacidade diferencial
Revise a consulta antes que ela possa ser executada	Não	Não	Sim, usando modelos de análise

Para obter mais informações sobre as regras de análise disponíveis em AWS Clean Rooms, consulte os tópicos a seguir.

- Regra de análise de agregação
- Regra de análise de lista
- Regra de análise personalizada em AWS Clean Rooms

Regra de análise de agregação

Em AWS Clean Rooms, uma regra de análise de agregação gera estatísticas agregadas usando as funções COUNT, SUM e/ou AVG junto com dimensões opcionais. Quando a regra de análise de agregação é adicionada a uma tabela configurada, ela permite que o membro que pode consultar execute consultas na tabela configurada.

A regra de análise de agregação oferece suporte a casos de uso como planejamento de campanhas, alcance de mídia, medição de frequência e atribuição.

A estrutura e a sintaxe de consulta suportadas são definidas em Estrutura e sintaxe da consulta de agregação.

Os parâmetros da regra de análise, definidos em Regra de análise de agregação - controles de consulta, incluem controles de consulta e controles de resultados de consulta. Seus controles de consulta incluem a capacidade de exigir que uma tabela configurada seja unida a pelo menos uma tabela configurada de propriedade do membro que pode consultar, direta ou transitivamente. Esse requisito permite garantir que a consulta seja executada na interseção (INNER JOIN) da sua tabela com a deles.

Estrutura e sintaxe da consulta de agregação

As consultas em tabelas que têm uma regra de análise de agregação devem seguir a sintaxe a seguir.

```
    --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}]] [,...]]
```

A tabela a seguir explica cada expressão listada na sintaxe anterior.

Expressão	Definição	Exemplos
select_aggregate_function_expression	Uma lista separada por vírgulas contendo as seguintes expressões: • select_aggregation_function_expression • select_aggregate_expression **Note** Deve haver pelo menos um select_aggregation_function_expression no select_aggregate_expression .	SELECT SUM(PRICE), user_segment
select_aggregation_function_expression	Uma ou mais funções de agregação suportadas aplicadas a uma ou mais	AVG(PRICE)

Expressão	Definição	Exemplos
	colunas. Somente colunas são permitidas como argumentos das funções de agregação. **Note** Deve haver pelo menos um `select_aggregation_function_expression` no `select_aggregate_expression` .	`COUNT(DISTINCT user_id)`

Expressão	Definição	Exemplos
select_grouping_column_expression	Uma expressão que pode conter qualquer expressão usando o seguinte: • Nomes de colunas da tabela • Funções escalares aceitas • Literais de string • Literais numéricos **Note** select_aggregate_expression pode criar um alias para colunas com ou sem o parâmetro AS. Para obter mais informações, consulte a SQL Reference AWS Clean Rooms.	TRUNC(timestampColumn) UPPER(campaignName)

Expressão	Definição	Exemplos
table_expression	Uma tabela, ou junção de tabelas, conectando expressões condicionais de junção com `join_condition` . `join_condition` retorna um Booleano. O `table_expression` oferece suporte a: • Um tipo específico JOIN (INNER JOIN) • A condição de comparação de igualdade dentro de um `join_condition` (=) • Operadores lógicos (`AND`, `OR`).	`FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2`

Expressão	Definição	Exemplos

where_expression	Uma expressão condicional que retorna um booliano. Pode ser composto do seguinte:
	• Nomes de colunas da tabela
	• Funções escalares aceitas
	• Operadores matemáticos
	• Literais de string
	• Literais numéricos
	
	As condições de comparação suportadas são (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Os operadores lógicos suportados são (`AND, OR`).
	
	`where_expression` é opcional.
		`WHERE where_condition`
		
		`WHERE price > 100`
		
		`WHERE TRUNC(timestampColumn) = '1/1/2022'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

group_by_expression	Uma lista separada por vírgulas de expressões que atendem aos requisitos do `select_grouping_column_expression` .	`GROUP BY TRUNC(timestampColumn), UPPER(campaignName), segment`

Expressão	Definição	Exemplos
having_expression	Uma expressão condicional que retorna um booleano. Eles têm uma função de agregação compatível aplicada a uma única coluna (por exemplo, `SUM(price)`) e são comparados a um literal numérico. As condições suportadas são (`=, >, <, <=, >=, <>, !=`). Os operadores lógicos suportados são (`AND, OR`). `having_expression` é opcional.	`HAVING SUM(SALES) > 500`

Expressão	Definição	Exemplos
order_by_expression	Uma lista de expressões separadas por vírgulas que é compatível com os mesmos requisitos `select_aggregate_expression` definidos anteriormente. `order_by_expression` é opcional. **Note** `order_by_expression` permite os parâmetros `ASC` e `DESC`. Para obter mais informações, consulte Parâmetros ASC DESC na SQL Reference AWS Clean Rooms.	`ORDER BY SUM(SALES), UPPER(campaignName)`

Para a estrutura e a sintaxe da consulta de agregação, lembre-se de que:

- Comandos SQL diferentes SELECT dos não são suportados.
- Não há suporte para subconsultas e expressões de tabela comuns (por exemplo, WITH).
- Operadores que combinam várias consultas (por exemplo, UNION) não são compatíveis.
- Os parâmetros TOP, LIMIT e OFFSET não têm suporte.

Regra de análise de agregação - controles de consulta

Com os controles de consulta de agregação, você pode controlar como as colunas em sua tabela são usadas para consultar a tabela. Por exemplo, você pode controlar qual coluna é usada para unir, qual coluna pode ser contada ou qual coluna pode ser usada em declarações WHERE.

As seções a seguir explicam cada controle.

Tópicos

Controles de agregação

Ao usar controles de agregação, você pode definir quais funções de agregação permitir e em quais colunas elas devem ser aplicadas. As funções de agregação podem ser usadas nas expressões SELECT, HAVING, ORDER e BY.

Controle	Definição	Uso
`aggregateColumns`	Colunas de colunas de tabela configuradas que você permite usar nas funções de agregação.	`aggregateColumns` pode ser usado dentro de uma função de agregação nas expressões SELECT, HAVING, ORDER e BY. Alguns `aggregateColumns` também podem ser categoriz ados como `joinColumn` (definidos posteriormente). Considerando que `aggregateColumn` também não pode ser categoriz ado como um `dimension`

Controle	Definição	Uso
		`Column` (definido posterior mente).
`function`	As funções COUNT, SUM e AVG que você permite usar em cima do `aggregate Columns` .	`function` pode ser aplicado a um `aggregateColumns` que esteja associado a ele.

Controles de junção

Uma cláusula `JOIN` é usada para combinar linhas de duas ou mais tabelas, com base em uma coluna relacionada entre elas.

Você pode usar os controles de união para controlar como sua tabela pode ser unida a outras tabelas no `table_expression`. AWS Clean Rooms só suporta INNER JOIN. As instruções INNER JOIN só podem usar colunas que tenham sido explicitamente categorizadas como `joinColumn` em sua regra de análise, sujeitas aos controles que você define.

INNER JOIN devem operar em uma `joinColumn` da sua tabela configurada e em outra `joinColumn` tabela configurada na colaboração. Você decide quais colunas da sua tabela podem ser usadas como `joinColumn`.

Cada condição de correspondência dentro da cláusula ON deve usar a condição de comparação de igualdade (=) entre duas colunas.

Várias condições de correspondência dentro de qualquer ON cláusula podem ser:

- Combinado usando o operador lógico `AND`
- Separado usando o operador lógico `OR`

> **Note**
>
> Todas as condições de correspondência JOIN devem corresponder a uma linha de cada lado do JOIN. Todas as condicionais conectadas por um `OR` ou um operador lógico `AND` ou devem atender a este requisito também.

Veja a seguir um exemplo de uma consulta com um operador lógico AND.

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

Veja a seguir um exemplo de uma consulta com um operador lógico OR.

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

Controle	Definição	Uso
`joinColumns`	As colunas (se houver) que você deseja permitir que o membro que pode consultar use na instrução INNER JOIN.	Um `joinColumn` específico também pode ser classificado como `aggregateColumn` (consulte Controles de agregação). A mesma coluna não pode ser usada como `joinColumn` e `dimensionColumns` (confira mais adiante). A menos que também tenha sido categorizado como um `aggregateColumn`, um `joinColumn` não pode ser usado em nenhuma outra parte da consulta além de INNER JOIN.
`joinRequired`	Controle se você precisa de um INNER JOIN com uma tabela configurada do membro que pode consultar.	Se você ativar esse parâmetro, será necessário um INNER JOIN. Se você não habilitar

Controle	Definição	Uso
		esse parâmetro, an INNER JOIN é opcional. Supondo que você habilite esse parâmetro, o membro que pode consultar deverá incluir uma tabela de sua propriedade no INNER JOIN. Eles devem unir JOIN sua mesa à deles, direta ou transitivamente (ou seja, unir sua mesa a outra mesa, que por sua vez está unida à sua mesa).

A seguir está um exemplo de transitividade.

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

> **Note**
>
> O membro que pode consultar também pode usar o parâmetro `joinRequired`. Nesse caso, a consulta deve unir sua tabela a pelo menos uma outra tabela.

Controles de dimensão

Os controles de dimensão controlam a coluna na qual as colunas de agregação podem ser filtradas, agrupadas ou agregadas.

Controle	Definição	Uso
`dimensionColumns`	As colunas (se houver) que você permite que o membro que pode consultar use em SELECT, WHERE, GROUP BY e ORDER BY.	A `dimensionColumn` pode ser usado em SELECT (`select_grouping_column_expression`), WHERE, GROUP BY e ORDER BY. A mesma coluna não pode ser ao mesmo tempo um `dimensionColumn` , um `joinColumn` e/ou um `aggregateColumn` .

Funções escalares

As funções escalares controlam quais funções escalares podem ser usadas em colunas de dimensão.

Controle	Definição	Uso
`scalarFunctions`	As funções escalares que podem ser usadas em `dimensionColumns` na consulta.	Especifica as funções escalares (se houver) nas quais você permite (por exemplo, CAST) que sejam aplicadas a `dimensionColumns` . As funções escalares não podem ser usadas em cima de outras funções ou dentro de outras funções. Os argumentos das funções escalares podem ser colunas, literais de string ou literais numéricos.

As seguintes funções escalares são suportadas:

- Funções matemáticas — ABS, CEILING, FLOOR, LOG, LN, ROUND, SQRT
- Funções de formatação de tipo de dados – CAST, CONVERT, TO_CHAR, TO_DATE, TO_NUMBER, TO_TIMESTAMP
- Funções de string — LOWER, UPPER, TRIM, RTRIM, SUBSTRING
  - Para RTRIM, conjuntos de caracteres personalizados para cortar não são permitidos.
- Expressões condicionais – COALESCE
- Funções de data — EXTRACT, GETDATE, CURRENT_DATE, DATEADD
- Outras funções – TRUNC

Para obter mais detalhes, consulte a SQL Reference AWS Clean Rooms.

Regra de análise de agregação - controles de resultados da consulta

Com os controles de resultados da consulta de agregação, você pode controlar quais resultados são retornados especificando uma ou mais condições que cada linha de saída deve atender para que seja retornada. AWS Clean Rooms suporta restrições de agregação na forma de `COUNT (DISTINCT column) >= X`. Esse formulário exige que cada linha agregue pelo menos X valores distintos de uma escolha da tabela configurada (por exemplo, um número mínimo de `user_id` valores distintos). Esse limite mínimo é aplicado automaticamente, mesmo que a consulta enviada em si não use a coluna especificada. Elas são aplicadas coletivamente em cada tabela configurada na consulta a partir das tabelas configuradas de cada membro na colaboração.

Cada tabela configurada deve ter pelo menos uma restrição de agregação em sua regra de análise. Os proprietários de tabelas configuradas podem adicionar várias `columnName` e associadas `minimum` e elas são aplicadas coletivamente.

Restrições de agregação

As restrições de agregação controlam quais linhas nos resultados da consulta são retornadas. Para ser retornada, uma linha deve atender ao número mínimo especificado de valores distintos em cada coluna especificada na restrição de agregação. Esse requisito se aplica mesmo que a coluna não seja mencionada explicitamente na consulta ou em outras partes da regra de análise.

Controle	Definição	Uso
`columnName`	O `aggregateColumn` que é usado na condição que cada linha de saída deve atender.	Pode ser qualquer coluna na tabela configurada.
`minimum`	O número mínimo de valores distintos associados `aggregateColumn` que a linha de saída deve ter (por exemplo, COUNT DISTINCT) para que ela seja retornada nos resultados da consulta.	O `minimum` deve ter pelo menos um valor de 2.

Estrutura de regras de análise de agregação

O exemplo a seguir mostra uma estrutura predefinida para uma regra de análise de agregação.

No exemplo a seguir, *`MyTable`* refere-se à sua tabela de dados. Você pode substituir cada *`espaço reservado de entrada do usuário`* por suas próprias informações.

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

Regra de análise de agregação - exemplo

O exemplo a seguir demonstra como duas empresas podem colaborar em AWS Clean Rooms usando da análise de agregação.

A empresa A tem dados de clientes e vendas. A empresa A está interessada em entender a atividade de devolução de produtos. A empresa B é uma das varejistas da empresa A e tem dados de devoluções. A empresa B também tem atributos de segmento de clientes que são úteis para a empresa A (por exemplo, comprou produtos relacionados, usa o atendimento ao cliente do varejista). A empresa B não quer fornecer dados de retorno de clientes em nível de linha e informações de atributos. A empresa B deseja apenas habilitar um conjunto de consultas para que a empresa A obtenha estatísticas agregadas sobre clientes sobrepostos em um limite mínimo de agregação.

A empresa A e a empresa B decidem colaborar para que a empresa A possa entender a atividade de devolução de produtos e oferecer produtos melhores na empresa B e em outros canais.

Para criar a colaboração e executar uma análise de agregação, as empresas fazem o seguinte:

1. A empresa A cria uma colaboração e cria uma associação. A colaboração tem a Empresa B como outro membro da colaboração. A empresa A permite o registro de consultas na colaboração e permite o registro de consultas em sua conta.
2. A empresa B cria uma associação na colaboração. Ele permite o registro de consultas em sua conta.
3. A empresa A cria uma tabela configurada de vendas.
4. A empresa A adiciona a seguinte regra de análise de agregação à tabela configurada de vendas.

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

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

`aggregateColumns` – A empresa A quer contar o número de clientes únicos na sobreposição entre dados de vendas e dados de devoluções. A empresa A também deseja somar o número de `purchases` feitos para comparar com o número de `returns`.

`joinColumns` – A empresa A deseja usar para combinar clientes `identifier` a partir de dados de vendas com clientes a partir de dados de devoluções. Isso ajudará a empresa A Match a retornar às compras certas. Também ajuda a Empresa A a segmentar clientes sobrepostos.

`dimensionColumns` – A empresa A usa `dimensionColumns` para filtrar por produto específico, comparar compras e devoluções em um determinado período de tempo, garantir que a data de devolução seja posterior à data do produto e ajudar a segmentar clientes sobrepostos.

`scalarFunctions` – A empresa A seleciona a função escalar `CAST` para ajudar a atualizar os formatos do tipo de dados, se necessário, com base na tabela configurada que a empresa A associa à colaboração. Ele também adiciona funções escalares para ajudar a formatar colunas, se necessário.

`outputConstraints` – A empresa A define restrições mínimas de produção. Não é necessário restringir os resultados porque o analista pode ver dados em nível de linha em sua tabela de vendas

> **Note**
>
> A empresa A não inclui `joinRequired` na regra de análise. Ele fornece flexibilidade para o analista consultar a tabela de vendas sozinho.

5. A empresa B cria uma tabela configurada de devoluções.
6. A empresa B adiciona a seguinte regra de análise de agregação à tabela configurada de devoluções.

```
{
  "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` – A empresa B permite que a empresa A faça uma soma `returns` para comparar com o número de compras. Eles têm pelo menos uma coluna agregada porque estão habilitando uma consulta agregada.

`joinColumns` – A empresa B permite que a empresa A se junte `identifier` para combinar clientes a partir dos dados de devolução com os clientes a partir dos dados de vendas. Os dados `identifier` são particularmente confidenciais e tê-los como garantia `joinColumn` de que os dados nunca serão gerados em uma consulta.

`joinRequired` – A empresa B exige que as consultas sobre os dados de devolução sejam sobrepostas aos dados de vendas. Eles não querem permitir que a Empresa A consulte todas as pessoas em seu conjunto de dados. Eles também concordaram com essa restrição em seu acordo de colaboração.

`dimensionColumns` – A empresa B permite que a empresa A filtre e agrupe por `state`, `popularpurchases` e `customerserviceuser` que são atributos exclusivos que podem ajudar a fazer a análise para a empresa A. A empresa B permite que a empresa A use `returndate` para filtrar a saída `returndate` que ocorre depois de `purchasedate`. Com essa filtragem, a saída é mais precisa para avaliar o impacto da alteração do produto.

`scalarFunctions` – A empresa B permite o seguinte:

- TRUNC para datas
- LOWER e UPPER, caso o `producttype` seja inserido em um formato diferente em seus dados
- CAST se a empresa A precisar converter os tipos de dados em vendas para serem iguais aos tipos de dados em devoluções

A empresa A não habilita outras funções escalares porque não acredita que sejam necessárias para consultas.

`outputConstraints` – A empresa B define restrições mínimas de produção em `hashedemail` para ajudar a reduzir a capacidade de reidentificar clientes. Também adiciona uma restrição mínima de produção em `producttype` para reduzir a capacidade de reidentificar produtos específicos que foram devolvidos. Certos tipos de produtos podem ser mais dominantes com base nas dimensões da produção (por exemplo, `state`). Suas restrições de saída sempre serão aplicadas, independentemente das restrições de saída adicionadas pela Empresa A aos seus dados.

7. A empresa A cria uma associação de tabela de vendas à colaboração.
8. A empresa B cria uma associação de tabela de devoluções à colaboração.
9. A empresa A executa consultas, como o exemplo a seguir, para entender melhor a quantidade de devoluções na empresa B em comparação com o total de compras por local em 2022.

```
SELECT
  companyB.state,
  SUM(companyB.returns),
  COUNT(DISTINCT companyA.hashedemail)
FROM
```

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

10 A empresa A e a empresa B revisam os logs de consulta. A empresa B verifica se a consulta está alinhada com o que foi acordado no contrato de colaboração.

Solução de problemas de regras de análise de agregação

Use as informações aqui para ajudá-lo a diagnosticar e corrigir problemas comuns ao trabalhar com regras de análise de agregação.

Problemas

- Minha consulta não retornou nenhum resultado

Minha consulta não retornou nenhum resultado

Isso pode acontecer quando não há resultados correspondentes ou quando os resultados correspondentes não atendem a um ou mais limites mínimos de agregação.

Para obter mais informações sobre limites mínimos de agregação, consulte Regra de análise de agregação - exemplo.

Regra de análise de lista

Em AWS Clean Rooms, uma regra de análise de lista gera listas em nível de linha da sobreposição entre a tabela configurada à qual ela é adicionada e as tabelas configuradas do membro que pode consultar. O membro que pode consultar executa consultas que incluem uma regra de análise de lista.

O tipo de regra de análise de lista oferece suporte a casos de uso como enriquecimento e criação de público.

Para obter mais informações sobre a estrutura de consulta e a sintaxe predefinidas para essa regra de análise, consulte Estrutura predefinida da regra de análise de listas.

Os parâmetros da regra de análise de lista, definidos em Regra de análise de lista - controles de consulta, têm controles de consulta. Seus controles de consulta incluem a capacidade de selecionar as colunas que podem ser listadas na saída. É necessário que a consulta tenha pelo menos uma junção com uma tabela configurada do membro que pode consultar, direta ou transitivamente.

Não há controles de resultados de consulta como os da regra de análise de agregação.

As consultas de lista só podem usar operadores matemáticos. Eles não podem usar outras funções (como agregação ou escalar).

Tópicos

- Estrutura e sintaxe da consulta de lista
- Regra de análise de lista - controles de consulta
- Estrutura predefinida da regra de análise de listas
- Regra de análise de listas - exemplo

Estrutura e sintaxe da consulta de lista

As consultas em tabelas que têm uma regra de análise de lista devem seguir a sintaxe a seguir.

```
--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]
```

A tabela a seguir explica cada expressão listada na sintaxe anterior.

Expressão	Definição	Exemplos
select_list_expression	Uma lista separada por vírgulas contendo pelo menos um nome de coluna de tabela. Um parâmetro DISTINCT é obrigatório. **Note** select_list_expression pode criar um alias para colunas com ou sem o parâmetro AS. Ele também suporta o parâmetro TOP. Para obter mais informações, consulte AWS Clean Rooms SQL Reference.	SELECT DISTINCT segment
table_expression	Uma tabela, ou junção de tabelas, com join_condition para conectá-la a join_condition . join_condition retorna um Booleano. table_expression oferece suporte a: • Um tipo específico de JOIN (JOIN INNER)	FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2

Expressão	Definição	Exemplos
	• As condições de comparação de igualdade dentro de um `join_condition` (=) • Operadores lógicos (`AND`, `OR`).	

where_expression	Uma expressão condicional que retorna um Booleano. Pode ser composto pelo seguinte:
	• Nomes de colunas da tabela
	• Operadores matemáticos
	• Literais de string
	• Literais numéricos
	
	As condições de comparação suportadas são (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Os operadores lógicos suportados são (`AND, OR`).
	
	`where_expression` é opcional.
		`WHERE state + '_' + city = 'NY_NYC'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

limit_expression	Essa expressão deve ter um inteiro positivo. Também pode ser trocado por um parâmetro TOP. `limit_expression` é opcional.	`LIMIT 100`

Para a estrutura e a sintaxe de consulta de lista, lembre-se de que:

- Comandos SQL diferentes de SELECT não são suportados.
- Subconsultas e expressões de tabela comuns (por exemplo, WITH) não são suportadas
- As cláusulas HAVING, GROUP BY e ORDER BY não são suportadas
- O parâmetro OFFSET não é suportado

Regra de análise de lista - controles de consulta

Com os controles de consulta de lista, você pode controlar como as colunas em sua tabela são usadas para consultar a tabela. Por exemplo, você pode controlar qual coluna é usada para unir ou qual coluna pode ser usada na instrução e cláusula WHERE SELECT.

As seções a seguir explicam cada controle.

Tópicos

Controles de junção

Com os controles de junção, você pode controlar como sua tabela pode ser unida a outras tabelas na table_expression. AWS Clean Rooms suporta apenas JOIN INNER. Na regra de análise de lista, é necessário pelo menos uma JOIN INNER e o membro que pode consultar deve incluir uma tabela de sua propriedade no JOIN INNER. Isso significa que eles devem unir sua mesa à deles, direta ou transitivamente.

A seguir está um exemplo de transitividade.

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

As instruções JOIN INNER só podem usar colunas que tenham sido explicitamente categorizadas como `joinColumn` em sua regra de análise.

A JOIN INNER deve operar em uma tabela configurada `joinColumn` e em outra `joinColumn` tabela configurada na colaboração. Você decide quais colunas da sua tabela podem ser usadas como `joinColumn`.

Cada condição de correspondência dentro da cláusula ON deve usar a condição de comparação de igualdade (=) entre duas colunas.

Várias condições de correspondência em uma cláusula ON podem ser:

- Combinado usando o operador lógico `AND`
- Separado usando o operador lógico `OR`

> **Note**
>
> Todas as condições de correspondência JOIN devem corresponder a uma linha de cada lado do JOIN. Todas as condicionais conectadas por um `OR` ou um operador lógico `AND` ou devem atender a este requisito também.

Veja a seguir um exemplo de uma consulta com um operador lógico `AND`.

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

Veja a seguir um exemplo de uma consulta com um operador lógico `OR`.

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

Controle	Definição	Uso
`joinColumns`	As colunas que você deseja permitir que o membro	A mesma coluna não pode ser categorizada como

Controle	Definição	Uso
	que pode consultar use na instrução JOIN INNER.	`joinColumn` e `listColumn` (consulte Controles de lista). `joinColumn` não pode ser usado em nenhuma outra parte da consulta além de JOIN INNER.

Controles de lista

Os controles de lista controlam as colunas que podem ser listadas na saída da consulta (ou seja, usadas na instrução SELECT) ou usadas para filtrar resultados (ou seja, usadas na WHERE instrução).

Controle	Definição	Uso
`listColumns`	As colunas que você permite que o membro que pode consultar use no SELECT e WHERE	A `listColumn` pode ser usado em SELECT e WHERE. A mesma coluna não pode ser usada como a `listColumn` e `joinColumn` .

Estrutura predefinida da regra de análise de listas

O exemplo a seguir inclui uma estrutura predefinida que mostra como você conclui uma regra de análise de lista.

No exemplo a seguir, *`MyTable`* refere-se à sua tabela de dados. Você pode substituir cada *`espaço reservado de entrada do usuário`* por suas próprias informações.

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

```
}
```

Regra de análise de listas - exemplo

O exemplo a seguir demonstra como duas empresas podem colaborar em AWS Clean Rooms usando a análise de listas.

A empresa A tem dados de gerenciamento de relacionamento com o cliente (CRM). A empresa A deseja obter dados adicionais de segmentos sobre seus clientes para saber mais sobre seus clientes e, potencialmente, usar atributos como entrada em outras análises. A empresa B tem dados de segmento compostos por atributos de segmento exclusivos que eles criaram com base em seus dados primários. A empresa B deseja fornecer os atributos exclusivos do segmento para a empresa A somente em clientes que estejam sobrepostos entre seus dados e os dados da empresa A.

As empresas decidem colaborar para que a Empresa A possa enriquecer os dados sobrepostos. A empresa A é o membro que pode consultar e a empresa B é a colaboradora.

Para criar uma colaboração e executar a análise de listas em colaboração, as empresas fazem o seguinte:

1. A empresa A cria uma colaboração e cria uma associação. A colaboração tem a Empresa B como outro membro da colaboração. A empresa A permite o log de consultas na colaboração e permite o log de consultas em sua conta.
2. A empresa B cria uma associação na colaboração. Ele permite o log de consultas em sua conta.
3. A empresa A cria uma tabela configurada de CRM
4. A empresa A adiciona a regra de análise à tabela configurada do cliente, como mostrado no exemplo a seguir.

```
{
  "joinColumns": [
    "identifier1",
    "identifier2"
  ],
  "listColumns": [
    "internalid",
    "segment1",
    "segment2",
    "customercategory"
  ]
```

```
}
```

`joinColumns` – A empresa A deseja usar `hashedemail` e/ou `thirdpartyid` (obtida de um fornecedor de identidade) combinar clientes a partir de dados de CRM com clientes de dados de segmentos. Isso ajudará a garantir que a Empresa A combine dados enriquecidos para os clientes certos. Eles têm duas JoinColumns para melhorar potencialmente a taxa de correspondência da análise.

`listColumns` – A empresa A costuma `listColumns` obter colunas enriquecidas ao lado e `internalid` usá-las em seus próprios sistemas. Eles adicionam `segment1`, `segment2` e `customercategory` para potencialmente limitar o enriquecimento a segmentos específicos, usando-os em filtros.

5. A empresa B cria uma tabela configurada por segmentos.
6. A empresa B adiciona a regra de análise à tabela configurada do segmento.

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

`joinColumns` – A empresa B permite que a empresa A se junte em `identifier2` para combinar clientes, desde dados de segmentos até dados de CRM. A empresa A e a empresa B trabalharam com o fornecedor de identidade para obter `identifier2` o que corresponderia a essa colaboração. Eles não adicionaram outros `joinColumns` porque acreditavam que `identifier2` fornecem a taxa de correspondência mais alta e precisa e que outros identificadores não são necessários para as consultas.

`listColumns` – A empresa B permite que a empresa A enriqueça seus dados com ps atributos `segment3` e `segment4` exclusivos que ela criou, coletou e alinhou (com o cliente A) para fazer parte do enriquecimento de dados. Eles querem que a Empresa A obtenha esses segmentos para a sobreposição em nível de linha, porque essa é uma colaboração de enriquecimento de dados.

7. A empresa A cria uma associação de tabela de CRM à colaboração.
8. A empresa B cria uma associação de tabela de segmentos à colaboração.

9. A empresa A executa consultas, como a seguinte, para enriquecer os dados sobrepostos do cliente.

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

10. A empresa A e a empresa B revisam os logs de consulta. A empresa B verifica se a consulta está alinhada com o que foi acordado no contrato de colaboração.

Regra de análise personalizada em AWS Clean Rooms

Em AWS Clean Rooms, uma regra de análise personalizada é um novo tipo de regra de análise que permite que consultas personalizadas sejam executadas na tabela configurada. As consultas SQL personalizadas ainda estão restritas a ter apenas o comando SELECT, mas podem usar mais construções SQL do que consultas de agregação e lista (por exemplo, funções de janela, OUTER JOIN, CTEs ou subconsultas; consulte a Referência SQL do AWS Clean Rooms para obter uma lista completa). As consultas SQL personalizadas não precisam seguir uma estrutura de consulta, como consultas de agregação e lista.

A regra de análise personalizada é compatível com casos de uso mais avançados do que os permitidos pela regra de agregação e análise de listas, como análise de atribuição personalizada, avaliação comparativa, análise de incrementalidade e descoberta de público. Isso é um acréscimo a um superconjunto dos casos de uso suportados pela regra de agregação e análise de listas.

A regra de análise personalizada também é compatível com a privacidade diferencial. A privacidade diferencial é uma estrutura matematicamente rigorosa para proteção da privacidade de dados. Para ter mais informações, consulte AWS Clean Rooms Privacidade diferencial. Quando você cria um modelo de análise, a Privacidade AWS Clean Rooms Diferencial verifica o modelo para determinar se ele é compatível com a estrutura de consulta de uso geral da Privacidade Diferencial AWS Clean Rooms . Essa validação garante que você não crie um modelo de análise que não seja permitido com uma tabela diferencial protegida por privacidade.

Para configurar a regra de análise personalizada, os proprietários dos dados podem optar por permitir que consultas personalizadas específicas, armazenadas em modelos de análise, sejam executadas em suas tabelas configuradas. Os proprietários dos dados revisam os modelos de análise antes de adicioná-los ao controle de análise permitido na regra de análise personalizada. Os

modelos de análise estão disponíveis e são visíveis somente na colaboração em que foram criados (mesmo que a tabela esteja associada a outras colaborações) e só podem ser executados pelo membro que pode consultar essa colaboração.

Como alternativa, os membros podem optar por permitir que outros membros (provedores de consultas) criem consultas sem revisão. Os membros adicionam as contas dos provedores de consulta que os provedores de consulta permitidos controlam na regra de análise personalizada. Se o provedor de consulta for o membro que pode consultar, ele poderá executar qualquer consulta diretamente na tabela configurada. Os provedores de consultas também podem criar consultas criando modelos de análise. Todas as consultas criadas pelos provedores de consultas podem ser executadas automaticamente na tabela em todas as colaborações nas quais a Conta da AWS está presente e a tabela está associada.

Os proprietários de dados só podem permitir que modelos de análise ou contas criem consultas, não ambos. Se o proprietário dos dados os deixar em branco, o membro que pode consultar não poderá executar consultas na tabela configurada.

Tópicos

Estrutura predefinida da regra de análise personalizada

O exemplo a seguir inclui uma estrutura predefinida que mostra como concluir uma regra de análise personalizada com a privacidade diferencial ativada. O valor de `userIdentifier` é a coluna que identifica exclusivamente seus usuários, como user_id. Quando você tem duas ou mais tabelas com privacidade diferencial ativada em uma colaboração, é AWS Clean Rooms necessário configurar a mesma coluna que a coluna do identificador do usuário em ambas as regras de análise para manter uma definição consistente dos usuários nas tabelas.

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

```
      }
    ]
  }
}
```

Você também pode:

- Adicione ARNs do modelo de análise ao controle de análises permitido. Nesse caso, o controle `allowedAnalysisProviders` não está incluído.

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

- Adicione Conta da AWS IDs de membros ao `allowedAnalysisProviders` controle. Nesse caso, você adiciona `ANY_QUERY` ao controle `allowedAnalyses`.

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

Exemplo de regra de análise personalizada

O exemplo a seguir demonstra como duas empresas podem colaborar no AWS Clean Rooms uso da regra de análise personalizada.

A empresa A tem dados de clientes e vendas. A empresa A está interessada em entender a incrementalidade de vendas de uma campanha publicitária no site da empresa B. A empresa B tem dados de visualização e atributos de segmento que são úteis para a empresa (por exemplo, o dispositivo usado ao visualizar a publicidade).

A empresa A tem uma consulta de incrementalidade específica que deseja executar na colaboração.

Para criar uma colaboração e executar uma análise personalizada em colaboração, as empresas fazem o seguinte:

1. A empresa A cria uma colaboração e cria uma associação. A colaboração tem a Empresa B como outro membro da colaboração. A empresa A permite o registro de consultas na colaboração e permite o registro de consultas em sua conta.

2. A empresa B cria uma associação na colaboração. Ele permite o registro de consultas em sua conta.
3. A empresa A cria uma tabela configurada de CRM
4. A empresa A adiciona uma regra de análise personalizada vazia à tabela configurada de vendas.
5. A empresa A associa a tabela configurada de vendas à colaboração.
6. A empresa B cria uma tabela configurada de visualização.
7. A empresa B adiciona uma regra de análise personalizada vazia à tabela configurada de visualização.
8. A empresa B associa a tabela configurada de visualização à colaboração.
9. A empresa A visualiza a tabela de vendas e a tabela de visualizações associadas à colaboração e cria um modelo de análise, adicionando a consulta de incrementalidade e o parâmetro para o mês da campanha.

```
{
    "analysisParameters": [
    {
        "defaultValue": ""
        "type": "DATE"
        "name": "campaign_month"
    }
    ],
    "description": "Monthly incrementality query using sales and viewership data"
    "format": "SQL"
    "name": "Incrementality analysis"
    "source":
        "WITH labeleddata AS
        (
        SELECT hashedemail, deviceid, purchases, unitprice, purchasedate,
        CASE
            WHEN testvalue IN ('value1', 'value2', 'value3') THEN 0
            ELSE 1
        END AS testgroup
        FROM viewershipdata
        )
        SELECT labeleddata.purchases, provider.impressions
        FROM labeleddata
        INNER JOIN salesdata
          ON labeleddata.hashedemail = provider.hashedemail
        WHERE MONTH(labeleddata.purchasedate) > :campaignmonth
        AND testgroup = :group
```

```
        "
}
```

10 A empresa A adiciona sua conta (por exemplo, 444455556666) ao controle permitido do provedor de análise na regra de análise personalizada. Eles usam o controle permitido do provedor de análise porque desejam permitir que todas as consultas criadas sejam executadas na tabela configurada de vendas.

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

11 A empresa B vê o modelo de análise criado na colaboração e revisa seu conteúdo, incluindo a string de consulta e o parâmetro.

12 A empresa B determina que o modelo de análise atinge o caso de uso de incrementalidade e atende aos requisitos de privacidade de como sua tabela configurada de audiência pode ser consultada.

13 A empresa B adiciona o ARN do modelo de análise ao controle de análise permitido na regra de análise personalizada da tabela de visualizações. Eles usam o controle de análise permitido porque só querem permitir que a consulta de incrementalidade seja executada em sua tabela configurada de visualização.

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

14 A empresa A executa o modelo de análise e usa o valor do parâmetro `05-01-2023`.

Regra de análise personalizada com privacidade diferencial

Em AWS Clean Rooms, a regra de análise personalizada oferece suporte à privacidade diferencial. A privacidade diferencial é uma estrutura matematicamente rigorosa para proteção da privacidade de dados que ajuda você a proteger seus dados contra tentativas de reidentificação.

A privacidade diferencial suporta análises agregadas, como planejamento de campanhas publicitárias, post-ad-campaign mensuração, benchmarking em um consórcio de instituições financeiras e testes A/B para pesquisas em saúde.

A estrutura e a sintaxe de consulta suportadas são definidas em Estrutura e sintaxe da consulta.

Exemplo de regra de análise personalizada com privacidade diferencial

Considere o exemplo de regra de análise personalizada apresentado na seção anterior. Esse exemplo demonstra como você pode usar a privacidade diferencial para proteger seus dados contra tentativas de reidentificação e, ao mesmo tempo, permitir que seu parceiro aprenda informações essenciais para os negócios com base nos seus dados. Suponha que a Empresa B, que tem os dados de audiência, queira proteger seus dados usando a privacidade diferencial. Para concluir a configuração de privacidade diferencial, a Empresa B conclui as seguintes etapas:

1. A empresa B ativa a privacidade diferencial ao adicionar uma regra de análise personalizada à tabela configurada de audiência. A empresa B seleciona `viewershipdata.hashedemail` como coluna de identificação do usuário.
2. A empresa B adiciona uma política de privacidade diferencial à colaboração para disponibilizar sua tabela de dados de audiência para consulta. A empresa B seleciona a política padrão para concluir rapidamente a configuração.

A empresa A, que deseja entender a incrementalidade de vendas de uma campanha publicitária no site da empresa B, executa o modelo de análise. Como a consulta é compatível com a estrutura de consulta de uso geral da privacidade diferencial do AWS Clean Rooms , a consulta é executada com êxito.

Estrutura e sintaxe da consulta

As consultas que contêm pelo menos uma tabela com a privacidade diferencial ativada devem seguir a sintaxe a seguir.

```
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**
>
> Para a estrutura e a sintaxe de consulta de privacidade diferencial, lembre-se de que:
>
> - Subconsultas não são compatíveis.

- Expressões de tabela comuns (CTEs) deverão emitir a coluna de identificador do usuário se uma tabela ou CTE envolver dados protegidos por privacidade diferencial. Filtros, agrupamentos e agregações devem ser feitos no nível do usuário.
- Final_select permite as funções agregadas COUNT DISTINCT, COUNT, SUM, AVG e STDDEV.

Consulte mais detalhes sobre quais palavras-chave de SQL são compatíveis com a privacidade diferencial em Capacidades SQL da AWS Clean Rooms Privacidade Diferencial.

AWS Clean Rooms Privacidade diferencial

AWS Clean Rooms A Privacidade Diferencial ajuda você a proteger a privacidade de seus usuários com uma técnica baseada em matemática que é implementada com controles intuitivos em alguns cliques. Como um recurso totalmente gerenciado, nenhuma experiência prévia de privacidade diferencial é necessária para ajudar você a evitar a reidentificação de seus usuários. AWS Clean Rooms adiciona automaticamente uma quantidade de ruído cuidadosamente calibrada aos resultados da consulta em tempo de execução para ajudar a proteger seus dados em nível individual.

AWS Clean Rooms A Privacidade Diferencial suporta uma ampla variedade de consultas analíticas e é uma boa opção para uma ampla variedade de casos de uso, nos quais uma pequena quantidade de erro nos resultados da consulta não comprometerá a utilidade de sua análise. Com ela, seus parceiros podem gerar insights essenciais para os negócios sobre campanhas publicitárias, decisões de investimento, pesquisas clínicas e muito mais, sem exigir configurações adicionais de seus parceiros.

AWS Clean Rooms A Privacidade Diferencial protege contra transbordamento ou erros de conversão inválidos que fazem uso de funções escalares ou símbolos de operadores matemáticos de forma maliciosa.

Para obter mais informações sobre privacidade AWS Clean Rooms diferencial, consulte os tópicos a seguir.

Tópicos

Privacidade diferencial

A privacidade diferencial permite apenas insights agregados e ofusca a contribuição dos dados de qualquer indivíduo nesses insights. A privacidade diferencial protege os dados de colaboração do

membro, que pode receber resultados aprendendo sobre um indivíduo específico. Sem a privacidade diferencial, o membro que pode receber os resultados pode tentar inferir dados individuais do usuário adicionando ou removendo registros sobre um indivíduo e observando a diferença nos resultados da consulta.

Quando a privacidade diferencial é ativada, uma quantidade específica de ruído é adicionada aos resultados da consulta para ofuscar a contribuição de usuários individuais. Se o membro que pode receber os resultados tentar observar a diferença nos resultados da consulta depois de remover registros sobre um indivíduo do conjunto de dados, a variabilidade no resultado da consulta ajuda a impedir a identificação dos dados do indivíduo. AWS Clean Rooms A Privacidade Diferencial usa o SampCertamostrador, uma implementação comprovadamente correta de amostrador desenvolvida pela. AWS

Como funciona a privacidade diferencial AWS Clean Rooms

O fluxo de trabalho para ativar a privacidade diferencial AWS Clean Rooms requer as seguintes etapas adicionais ao concluir o fluxo de trabalho para AWS Clean Rooms:

1. Você ativa a privacidade diferencial ao adicionar uma regra de análise personalizada.
2. Você configura a política de privacidade diferencial da colaboração para proteger suas tabelas de dados com a privacidade diferencial disponível para consulta.

Depois de concluir essas etapas, o membro que pode consultar pode começar a executar consultas sobre dados protegidos por privacidade diferencial. AWS Clean Rooms retorna resultados que estão em conformidade com a política de privacidade diferencial. AWS Clean Rooms A Privacidade Diferencial rastreia o número estimado de consultas restantes que você pode executar, semelhante ao indicador de gasolina de um carro que mostra o nível atual de combustível do carro. O número de consultas que o membro que pode consultar é capaz de executar é limitado pelos parâmetros orçamento de privacidade e ruído adicionado por consulta definidos no Política de privacidade diferencial.

Considerações

Ao usar a privacidade diferencial em AWS Clean Rooms, considere o seguinte:

- O membro que pode receber os resultados não pode usar a privacidade diferencial. Ele configura uma regra de análise personalizada com a privacidade diferencial desativada para as tabelas configuradas.

- O membro que pode consultar não pode unir tabelas de dois ou mais provedores de dados quando ambos têm a privacidade diferencial ativada.

Política de privacidade diferencial

A política de privacidade diferencial controla quantas funções de agregação o membro que pode consultar é capaz de executar em uma colaboração. O orçamento de privacidade define um recurso comum e finito que é aplicado a todas as tabelas em uma colaboração. O ruído adicionado por consulta rege a taxa na qual o orçamento de privacidade é esgotado.

É necessária uma política de privacidade diferencial para disponibilizar suas tabelas protegidas por privacidade diferencial para consulta. Essa é uma etapa única em uma colaboração e inclui duas entradas:

- Orçamento de privacidade: quantificado em termos de épsilon, o orçamento de privacidade controla o nível de proteção da privacidade. É um recurso comum e finito que é aplicado a todas as tabelas protegidas com a privacidade diferencial na colaboração, porque o objetivo é preservar a privacidade dos usuários cujas informações podem estar presentes em várias tabelas.

  O orçamento de privacidade é consumido toda vez que uma consulta é executada nas tabelas. Quando o orçamento de privacidade é totalmente esgotado, o membro da colaboração que pode consultar não é capaz de executar consultas adicionais até que ele seja aumentado ou atualizado. Ao definir um orçamento de privacidade maior, o membro que pode receber os resultados pode reduzir sua incerteza sobre os indivíduos nos dados. Escolha um orçamento de privacidade que equilibre seus requisitos de colaboração com suas necessidades de privacidade e depois de consultar os tomadores de decisões empresariais.

  É possível selecionar Atualizar o orçamento de privacidade mensalmente para criar automaticamente um orçamento de privacidade a cada mês civil, se você planeja trazer regularmente novos dados para a colaboração. A escolha dessa opção permite que quantidades arbitrárias de informações sejam reveladas sobre as linhas dos dados quando consultadas repetidamente nas atualizações. Evite escolher essa opção se as mesmas linhas forem consultadas repetidamente entre as atualizações do orçamento de privacidade.
- Ruído adicionado por consulta é medido em termos do número de usuários cujas contribuições você deseja ocultar. Esse valor rege a taxa na qual o orçamento de privacidade é esgotado. Um valor de ruído maior reduz a taxa de esgotamento do orçamento de privacidade e, portanto, permite que mais consultas sejam executadas em seus dados. No entanto, isso deve ser

equilibrado com a liberação de informações de dados menos precisas. Considere a precisão desejada para insights de colaboração ao definir esse valor.

Você pode usar a política de privacidade diferencial padrão para concluir rapidamente a configuração ou personalizar sua política de privacidade diferencial de acordo com seu caso de uso. AWS Clean Rooms A Privacidade Diferencial fornece controles intuitivos para configurar a política. AWS Clean Rooms A Privacidade Diferencial permite que você visualize o utilitário em termos do número de agregações possíveis em todas as consultas em seus dados e estime quantas consultas podem ser executadas em uma colaboração de dados.

É possível usar os exemplos interativos para entender como diferentes valores de orçamento de privacidade e ruído adicionado por consulta afetariam os resultados de diferentes tipos de consultas SQL. Em geral, você precisa equilibrar suas necessidades de privacidade com o número de consultas que deseja permitir e a precisão dessas consultas. Um orçamento de privacidade menor ou um ruído adicionado por consulta maior podem proteger melhor a privacidade do usuário, mas fornecem informações menos significativas para seus parceiros de colaboração.

Se você aumentar o orçamento de privacidade e, ao mesmo tempo, mantiver o mesmo parâmetro de ruído adicionado por consulta, o membro que pode consultar poderá executar mais agregações em suas tabelas na colaboração. É possível aumentar o orçamento de privacidade a qualquer momento durante a colaboração. Se você diminuir o orçamento de privacidade e, ao mesmo tempo, mantiver o mesmo parâmetro de ruído adicionado por consulta, o membro que pode consultar poderá executar menos agregações. Não é possível diminuir o orçamento de privacidade depois que o membro que pode consultar começar a analisar seus dados.

Se você aumentar o ruído adicionado por consulta e, ao mesmo tempo, mantiver a mesma entrada de orçamento de privacidade, o membro que pode consultar poderá executar mais agregações em suas tabelas na colaboração. Se você diminuir o ruído adicionado por consulta e, ao mesmo tempo, mantiver a mesma entrada de orçamento de privacidade, o membro que pode consultar poderá executar menos agregações. É possível aumentar ou diminuir o ruído adicionado por consulta a qualquer momento durante a colaboração.

A política de privacidade diferencial é gerenciada pelas ações de API do modelo de orçamento de privacidade.

Capacidades SQL da AWS Clean Rooms Privacidade Diferencial

AWS Clean Rooms A Privacidade Diferencial usa uma estrutura de consulta de uso geral para oferecer suporte a consultas SQL complexas. Os modelos de análise personalizados são validados em relação a essa estrutura para garantir que possam ser executados em tabelas protegidas por privacidade diferencial. A tabela a seguir indica quais funções são compatíveis. Consulte Estrutura e sintaxe da consulta Para mais informações.

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Funções agregadas	• Função ANY_VALUE • Função APPROXIMATE PERCENTILE_DISC • Função AVG • Funções COUNT e COUNT DISTINCT • Função LISTAGG • Função MAX • Função MEDIAN • Função MIN • Função PERCENTILE_CONT • Funções STDDEV_SAMP e STDDEV_POP • Funções SUM e SUM DISTINCT	Suportado com a condição de que os CTEs que usam tabelas protegidas por privacidade diferencial devem resultar em dados com registros em nível de usuário. Você deve escrever a expressão SELECT nesses CTEs usando o `SELECT userIdentifierColumn...' formato.	Agregações suportadas: AVG, COUNT, COUNT DISTINCT, STDDEV e SUM.

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
	• Funções VAR_SAMP e VAR_POP		
CTEs	Cláusula WITH, subconsulta da cláusula WITH	Suportado com a condição de que os CTEs que usam tabelas protegidas por privacidade diferencial devem resultar em dados com registros em nível de usuário. Você deve escrever a expressão SELECT nesses CTEs usando o `SELECT userIdentifierColumn...' formato.	N/D
Subconsultas	Subconsulta da lista SELECT, subconsulta da cláusula FROM, subconsulta da cláusula WHERE	Sem suporte. Não há suporte para subconsultas na consulta que faz referência a uma tabela com a privacidade diferencial ativada. Reescreva suas subconsultas como Expressões de Tabela Comuns (CTEs).	

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Cláusulas de união	• INNER JOIN • LEFT JOIN • RIGHT JOIN • FULL JOIN • Operador [JOIN] OR • CROSS JOIN	Compatível com a condição de que somente as funções JOIN que são junções equivalentes nas colunas de identificador de usuário sejam permitidas e obrigatórias ao consultar duas ou mais tabelas com a privacidade diferencial ativada. As condições obrigatórias de junção equivalente devem estar corretas. Confirme se o proprietário da tabela configurou a mesma coluna de identificador de usuário em todas as tabelas para que a definição de um usuário permaneça consistente em todas elas. As funções CROSS JOIN não são compatíveis ao combinar duas ou mais relações com a privacidade diferencial ativada.	
Configurar operadores	UNION, UNION ALL, INTERSECT, EXCETO | MINUS (esses são sinônimos)	Todos são suportados	Sem compatibilidade

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Funções de janela	Funções agregadas • Função de janela AVG • Função de janela COUNT • Função de janela CUME_DIST • Função de janela DENSE_RANK • Função de janela FIRST_VALUE • Função de janela LAG • Função de janela LAST_VALUE • Função de janela LEAD • Funções de janela MAX • Funções de janela MEDIAN • Funções de janela MIN • Função de janela NTH_VALUE • Função de janela RATIO_TO_REPORT • Funções de janela STDDEV_SAMP	Todos são suportados com a condição de que a coluna de identificador de usuário na cláusula de partição da função de janela seja necessária quando você consulta uma relação com a privacidade diferencial ativada.	Sem compatibilidade

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
	e STDDEV_POP (STDDEV_SAMP e STDDEV são sinônimos) • Funções de janela SUM • Funções de janela VAR_SAMP e VAR_POP (VAR_SAMP e VARIANCE são sinônimos) Funções de classificação • Função de janela DENSE_RANK • Função de janela NTILE • Função de janela PERCENT_RANK • Função de janela RANK • Função de janela ROW_NUMBER		

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Expressões condicionais	• Expressão de condição CASE • Expressão COALESCE • Funções GREATEST e LEAST • Funções NVL e COALESCE • Função NVL2 • Função NULLIF	Todos são suportados	Todos são suportados
Condições	• Condição de comparação • Condições lógicas • Condições de correspondência de padrões • Condições de intervalo BETWEEN • Condição null	`EXISTS`e `IN` não podem ser usados porque exigem subconsultas. Todos os outros são suportados.	Todos são suportados

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Funções de data e hora	• Funções de data e hora em transações • Operador de concatenação • Funções ADD_MONTHS • Função CONVERT_TIMEZONE • Função CURRENT_DATE • Função DATEADD • Função DATEDIFF • Funções DATE_PART • Função DATE_TRUNC • Função EXTRACT • Função GETDATE • Funções TIMEOFDAY • Função TO_TIMESTAMP • Partes da data para funções de data ou de timestamp	Todos são suportados	Todos são suportados

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Funções de string	• Operador || (concatenação) • Função BTRIM • Função CHAR_LENGTH • Função CHARACTER _LENGTH • Função CHARINDEX • Função CONCAT • Funções LEFT e RIGHT • Função LEN • Função LENGTH • Função LOWER • Funções LPAD e RPAD • Função LTRIM • Funções POSITION • Função REGEXP_COUNT • Função REGEXP_INSTR • Função REGEXP_RE PLACE • Função REGEXP_SUBSTR • Função REPEAT	Todos são suportados	Todos são suportados

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
	• Função REPLACE • Função REPLICATE • Função REVERSE • Função RTRIM • Função SOUNDEX • Função SPLIT_PART • Função STRPOS • Função SUBSTRING • Função TEXTLEN • Função TRANSLATE • Funções TRIM • Função UPPER		
Funções de formatação de tipo de dados	• Função CAST • TO_CHAR • Função TO_DATE • TO_NUMBER • Strings de formato datetime • Strings de formato numérico	Todos são suportados	Todos são suportados

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Funções de hash	• Função MD5 • Função SHA • Função SHA1 • Função SHA2 • MURMUR3_32_HASH	Todos são suportados	Todos são suportados
Símbolos de operadores matemáticos	+, -, *,/,% e @	Todos são suportados	Todos são suportados

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Funções matemáticas	• Função ABS • Função ACOS • Função ASIN • Função ATAN • Função ATAN2 • Função CBRT • Função CEILING (ou CEIL) • Função COS • Função COT • Função DEGREES • Função DEXP • Função LTRIM • Função DLOG1 • Função DLOG10 • Função EXP • Função FLOOR • Função LN • Função LOG • Função MOD • Função PI • Função POWER • Função RADIANS • Função RANDOM • Função ROUND • Função SIGN • Função SIN • Funções SQRT	Todos são suportados	Todos são suportados

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
	• Função TRUNC		
Funções de informação de tipo SUPER	• Função DECIMAL_PRECISION • Função DECIMAL_SCALE • Função IS_ARRAY • Função IS_BIGINT • Função IS_CHAR • Função IS_DECIMAL • Função IS_FLOAT • Função IS_INTEGER • Função IS_OBJECT • Função IS_SCALAR • Função IS_SMALLINT • Função IS_VARCHAR • Função JSON_TYPEOF	Todos são suportados	Todos são suportados

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Funções VARBYTE	• Função FROM_HEX • Função FROM_VARBYTE • Função TO_HEX • Função TO_VARBYTE	Todos são suportados	Todos são suportados
JSON	• Função CAN_JSON_PARSE • Função JSON_EXTRACT_ARRAY_ELEMENT_TEXT • Função JSON_EXTRACT_PATH_TEXT • Função JSON_PARSE • Função JSON_SERIALIZE • Função JSON_SERALIZE_TO_VARBYTE	Todos são suportados	Todos são suportados

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Funções de array	• função de array • função array_concat • função array_flatten • função get_array_length • função split_to_array • função de subarray	Sem compatibilidade	Sem compatibilidade
GRUPO ESTENDIDO POR	CONJUNTOS DE AGRUPAMENTO, ROLLUP, CUBO	Sem compatibilidade	Sem compatibilidade
Operação de classificação	ORDER BY	Compatível com a condição de que uma cláusula ORDER BY só seja suportada na cláusula de partição de uma função de janela ao consultar tabelas com a privacidade diferencial ativada.	Compatível
Limites de linha	LIMIT, OFFSET	Não suportado em CTEs usando tabelas protegidas por privacidade diferencial	Todos são suportados
Aliasing de tabelas e colunas		Compatível	Compatível

Nome curto	Estruturas de SQL	Expressões de tabela comuns (CTEs)	Cláusula SELECT final
Funções matemáticas em funções agregadas		Compatível	Compatível
Funções escalares dentro de funções agregadas		Compatível	Compatível

Alternativas comuns para estruturas de SQL incompatíveis

Categoria	Estrutura de SQL	Alternativa
Funções de janela	• LISTAGG • PERCENTILE_CONT • PERCENTILE_DISC	Você pode usar a função agregada equivalente com GROUP BY.
Símbolos de operadores matemáticos	• $column ||/ 2 • $column |/ 2 • $column ^ 2	• CBRT • SQRT • POWER($column, 2)
Funções escalares	• SYSDATE • $column::integer • convert(type, $column)	• CURRENT_DATE • CAST $column AS integer • CAST $column AS type
Literais	INTERVALO DE '1 SEGUNDO'	INTERVALO '1' SEGUNDO
Limitação de linhas	TOP n	LIMITE n
Ingressar	• USING • NATURAL	A cláusula ON deve conter explicitamente um critério de junção.

Dicas e exemplos de consultas de privacidade diferencial

AWS Clean Rooms A Privacidade Diferencial usa uma estrutura de consulta de uso geral para oferecer suporte a uma ampla variedade de construções SQL, como Expressões de Tabela Comuns (CTEs) para preparação de dados e funções agregadas comumente usadas, como ou. `COUNT` `SUM` Para ofuscar a contribuição de qualquer possível usuário em seus dados adicionando ruído aos resultados agregados da consulta em tempo de execução, a Privacidade AWS Clean Rooms Diferencial exige que as funções agregadas no final sejam executadas em dados no nível do usuário. `SELECT statement`

O exemplo a seguir usa duas tabelas chamadas `socialco_impressions` e `socialco_users` de um publicador de mídia que deseja proteger os dados usando a privacidade diferencial enquanto colabora com uma marca esportiva com dados `athletic_brand_sales`. O publicador de mídia configurou a coluna `user_id` como a coluna do identificador do usuário, ao mesmo tempo em que habilitou a privacidade diferencial no AWS Clean Rooms. O anunciante não precisa da proteção de privacidade diferencial e deseja executar uma consulta usando CTEs em dados combinados. Como a CTE usa tabelas protegidas de privacidade diferencial, o anunciante inclui a coluna de identificador de usuário dessas tabelas protegidas na lista de colunas de CTE e une as tabelas protegidas na coluna de identificador de usuário.

```
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
```

Da mesma forma, se você quiser executar funções de janela em tabelas de dados protegidas por privacidade diferencial, deverá incluir a coluna do identificador do usuário na cláusula `PARTITION BY`.

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

Limitações da AWS Clean Rooms privacidade diferencial

AWS Clean Rooms A Privacidade Diferencial não aborda as seguintes situações:

1. AWS Clean Rooms A Privacidade Diferencial não aborda ataques temporizados. Por exemplo, esses ataques são possíveis em cenários em que um usuário individual contribui com um grande número de linhas e adicionar ou remover esse usuário altera significativamente o tempo de computação da consulta.
2. A privacidade diferencial do AWS Clean Rooms não garante privacidade diferencial quando uma consulta SQL pode resultar em estouro ou erros de conversão inválidos em tempo de execução devido ao uso de determinadas construções SQL. A tabela a seguir é uma lista de algumas construções SQL, mas não de todas, que podem produzir erros de tempo de execução e devem ser verificadas em modelos de análise. Recomendamos que você aprove modelos de análise que minimizem as chances de tais erros em tempo de execução e revise periodicamente os registros de consulta para determinar se as consultas estão alinhadas com o contrato de colaboração.

   As seguintes construções SQL são vulneráveis a erros de estouro:

   - Funções agregadas - AVG, LISTAVG, PERCENTILE_COUNT, PERCENTILE_DISC, SUM/ SUM_DISTINCT
   - Funções de formatação de tipo de dados - TO_TIMESTAMP, TO_DATE
   - Funções de data e hora - ADD_MONTHS, DATEADD, DATEDIFF
   - Funções matemáticas - +, -, *,/, POWER
   - Funções de string - ||, CONCAT, REPEAT, REPLICATE

- Funções de janela - AVG, LISTAGG, PERCENTILE_COUNT, PERCENTILE_DISC, RATIO_TO_REPORT, SUM

A função de formatação do tipo de dados CAST é vulnerável a erros de conversão inválidos.

AWS Clean Rooms ML

AWS Clean Rooms ML

AWS Clean Rooms O ML fornece um método de preservação da privacidade para duas partes identificarem usuários semelhantes em seus dados sem a necessidade de compartilhar seus dados entre si. A primeira parte traz os dados de treinamento para que AWS Clean Rooms possam criar e configurar um modelo semelhante e associá-lo a uma colaboração. A segunda parte então traz seus dados iniciais AWS Clean Rooms e gera um segmento semelhante que se assemelha aos dados de treinamento.

Consulte uma explicação mais detalhada de como isso funciona em Trabalhos entre contas.

- Provedor de dados de treinamento: a parte que contribui com os dados de treinamento, cria e configura um modelo de semelhanças e o associa a uma colaboração.
- Provedor de dados de seed: a parte que contribui com os dados de seed, gera um segmento de semelhanças e o exporta.
- Dados de treinamento: os dados do provedor de dados de treinamento, que são usados para gerar um modelo de semelhanças. Os dados de treinamento são usados para medir a semelhança nos comportamentos do usuário.

  Os dados de treinamento devem conter uma coluna de ID de usuário, ID do item e carimbo de data/hora. Opcionalmente, os dados de treinamento podem conter outras interações como atributos numéricos ou categóricos. Exemplos de interações são uma lista de vídeos assistidos, itens comprados ou artigos lidos.
- Dados de seed: os dados do provedor de dados de seed, que são usados para criar um segmento de semelhanças. A saída do segmento de semelhanças é um conjunto de usuários dos dados de treinamento que mais se assemelha aos usuários de seed.
- Modelo de semelhanças: um modelo de machine learning dos dados de treinamento usado para encontrar usuários semelhantes em outros conjuntos de dados.

  Ao usar a API, o termo modelo de público é usado de forma equivalente ao modelo de semelhanças. Por exemplo, você usa a CreateAudienceModel API para criar um modelo parecido.
- Segmento semelhante — Um subconjunto dos dados de treinamento que mais se assemelha aos dados iniciais.

Ao usar a API, você cria um segmento semelhante com a StartAudienceGenerationJobAPI.

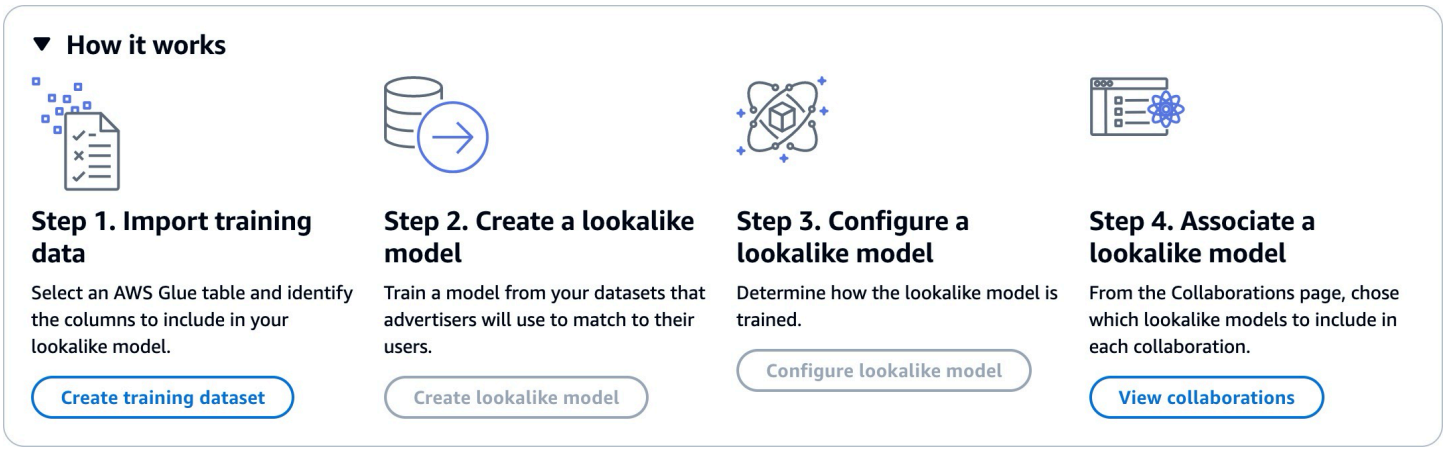
Os dados do provedor de dados de treinamento nunca são compartilhados com o provedor de dados de seed e os dados do provedor de dados de seed nunca são compartilhados com o provedor de dados de treinamento. A saída do segmento de semelhanças é compartilhada com o provedor de dados de treinamento, mas nunca com o provedor de dados de seed.

Para ter mais informações sobre modelos de semelhanças, consulte os tópicos a seguir.

Tópicos

- Como funciona o AWS Clean Rooms ML

Como funciona o AWS Clean Rooms ML



O Clean Rooms ML exige que duas partes, um provedor de dados de treinamento e um provedor de dados iniciais, trabalhem sequencialmente AWS Clean Rooms para reunir seus dados em uma colaboração. Esse é o fluxo de trabalho que o provedor de dados de treinamento deve concluir primeiro:

1. Os dados do provedor de dados de treinamento devem ser armazenados em uma tabela de catálogo de AWS Glue dados de interações com itens do usuário. No mínimo, os dados de treinamento devem conter uma coluna de ID de usuário, uma coluna de ID de interação e uma coluna de carimbo de data/hora.
2. O provedor de dados de treinamento registra os dados de treinamento com AWS Clean Rooms.
3. O provedor de dados de treinamento cria um modelo de semelhanças que pode ser compartilhado com vários provedores de dados de seed. O modelo de semelhanças é uma rede neural

profunda que pode levar até 24 horas para ser treinado. Ele não é retreinado automaticamente e recomendamos que você retreine o modelo semanalmente.

4. O provedor de dados de treinamento configura o modelo de semelhanças, incluindo se deseja compartilhar métricas de relevância e a localização dos segmentos de saída do Amazon S3. O provedor de dados de treinamento pode criar vários modelos de semelhanças configurados com base em um único modelo de semelhanças.
5. O provedor de dados de treinamento associa o modelo de público configurado a uma colaboração que é compartilhada com um provedor de dados de seed.

Esse é o fluxo de trabalho que o provedor de dados de seed deve concluir a seguir:

1. Os dados do provedor de dados de seed devem ser armazenados em um bucket do Amazon S3.
2. O provedor de dados de seed abre a colaboração que compartilha com o provedor de dados de treinamento.
3. O provedor de dados iniciais cria um segmento semelhante na guia Clean Rooms ML da página de colaboração.
4. O provedor de dados de seed poderá avaliar as métricas de relevância, se elas foram compartilhadas, e exportar o segmento de semelhanças para uso fora do AWS Clean Rooms.

Proteções de privacidade do ML AWS Clean Rooms

O Clean Rooms ML foi projetado para reduzir o risco de ataques de inferência de membros, em que o provedor de dados de treinamento pode saber quem está nos dados iniciais e o provedor de dados iniciais pode saber quem está nos dados de treinamento. Várias etapas são seguidas para evitar esse ataque.

Primeiro, os provedores de dados iniciais não observam diretamente a saída de ML do Clean Rooms e os provedores de dados de treinamento nunca podem observar os dados iniciais. Os provedores de dados de seed podem optar por incluir os dados de seed no segmento de saída.

A seguir, o modelo de semelhanças é criado com base em uma amostra aleatória dos dados de treinamento. Essa amostra inclui um número significativo de usuários que não correspondem ao público de seed. Esse processo torna mais difícil determinar se um usuário não estava nos dados, o que é outra forma de inferência de associação.

Além disso, vários clientes de seed podem ser usados para cada parâmetro do treinamento de modelos de semelhanças específicos para seed. Isso limita o quanto o modelo pode ser

sobreajustado e, portanto, o quanto pode ser inferido sobre um usuário. Como resultado, recomendamos que o tamanho mínimo dos dados de seed seja de 500 usuários.

Por fim, as métricas no nível de usuário nunca são fornecidas aos provedores de dados de treinamento, o que elimina outra via para um ataque de inferência de associação.

AWS Clean Rooms Métricas de avaliação do modelo de ML

O Clean Rooms ML calcula a pontuação de recall e relevância para determinar o desempenho do seu modelo. O Recall compara a semelhança entre os dados semelhantes e os dados de treinamento. A pontuação de relevância é usada para decidir o tamanho do público, não se o modelo tem um bom desempenho.

O recall é uma medida imparcial da semelhança do segmento semelhante com os dados de treinamento. O recall é a porcentagem dos usuários mais semelhantes (por padrão, os 20% mais semelhantes) de uma amostra dos dados de treinamento que são incluídos no público-alvo inicial pelo trabalho de geração de público. Os valores variam de 0 a 1, valores maiores indicam um público melhor. Um valor de recall aproximadamente igual à porcentagem máxima do compartimento indica que o modelo de público é equivalente à seleção aleatória.

Consideramos essa uma métrica de avaliação melhor do que exatidão, precisão e pontuações F1 porque o Clean Rooms ML não rotulou com precisão os verdadeiros usuários negativos ao criar seu modelo.

A pontuação de relevância no nível de segmento é uma medida de similaridade com valores que variam de -1 (menos semelhante) a 1 (mais semelhante). O Clean Rooms ML calcula um conjunto de pontuações de relevância para vários tamanhos de segmentos para ajudá-lo a determinar o melhor tamanho de segmento para seus dados. As pontuações de relevância diminuem monotonicamente à medida que o tamanho do segmento aumenta, portanto, à medida que o tamanho do segmento aumenta, ele pode ser menos semelhante aos dados iniciais. Quando a pontuação de relevância no nível do segmento atinge 0, o modelo prevê que todos os usuários no segmento de semelhanças são da mesma distribuição dos dados de seed. É provável que o aumento do tamanho da saída inclua usuários no segmento de semelhanças que não são da mesma distribuição dos dados de seed.

As pontuações de relevância são normalizadas em uma única campanha e não devem ser usadas para comparação entre campanhas. As pontuações de relevância não devem ser usadas como uma evidência de fonte única para qualquer resultado comercial, pois elas são afetadas por vários fatores

complexos, além da relevância, como qualidade do inventário, tipo de inventário, horário do anúncio publicitário e assim por diante.

As pontuações de relevância não devem ser usadas para avaliar a qualidade de seed, mas sim se ela pode ser aumentada ou diminuída. Considere os seguintes exemplos:

- Todas as pontuações positivas: isso indica que há mais usuários de saída previstos como semelhantes do que os incluídos no segmento de semelhanças. Isso é comum em dados de seed que fazem parte de um grande mercado, como todos que compraram pasta de dente no mês passado. Recomendamos analisar dados de seed menores, como todos que compraram pasta de dente mais de uma vez no mês passado.
- Todas as pontuações negativas ou negativas para o tamanho de segmento semelhante desejado — Isso indica que o Clean Rooms ML prevê que não há usuários semelhantes suficientes no tamanho de segmento semelhante desejado. Talvez os dados de seed sejam muito específicos ou o mercado seja muito pequeno. Recomendamos aplicar menos filtros aos dados de seed ou ampliar o mercado. Por exemplo, se os dados de seed originais fossem de clientes que compraram um carrinho de bebê e uma cadeirinha para carro, você poderia expandir o mercado para clientes que compraram vários produtos para bebês.

Os provedores de dados de treinamento determinam se as pontuações de relevância estão expostas e os compartimentos de bucket onde as pontuações de relevância são calculadas.

Trabalhando com AWS Clean Rooms ML

Um modelo de semelhanças é um modelo dos dados de um provedor de dados de treinamento que permite que um provedor de dados de seed crie um segmento de semelhanças dos dados do provedor de dados de treinamento que mais se assemelhe aos dados de seed. Para criar um modelo de semelhanças que possa ser usado em uma colaboração, você deve importar seus dados de treinamento, criar um modelo de semelhanças, configurar esse modelo de semelhanças e, depois, associá-lo a uma colaboração.

Depois que o provedor de dados de treinamento terminar de criar o modelo de ML, o provedor de dados de seed poderá criar e exportar o segmento de seed.

Tópicos

- Próximas etapas

Trabalhando com modelos semelhantes (provedor de dados de treinamento)

Importar dados de treinamento

Antes de criar um modelo semelhante, você deve especificar a AWS Glue tabela que contém os dados de treinamento. O Clean Rooms ML não armazena uma cópia desses dados, apenas metadados que permitem que ele acesse os dados.

Para importar dados de treinamento em AWS Clean Rooms

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, selecione Modelagem de ML.
3. Na guia Conjuntos de dados de treinamento, escolha Criar conjunto de dados de treinamento.
4. Insira um Nome e uma Descrição opcional.
5. Em Fonte de dados, escolha sua AWS Glue tabela:
   a. Escolha o Banco de dados que você deseja configurar na lista suspensa.
   b. Escolha a fonte de dados de treinamento selecionando o banco de dados e a tabela que você deseja configurar nas listas suspensas.

> **Note**
>
> Para verificar se essa é a tabela correta, faça um dos seguintes:
>
> - Escolha Exibir em AWS Glue.
> - Ative Exibir esquema para ver o esquema.

6. Para obter detalhes do treinamento, escolha a coluna Identificador do usuário, a coluna Identificador do item e a coluna Timestamp nos seus dados. Os dados de treinamento devem conter essas três colunas. Você também pode selecionar qualquer outra coluna que queira incluir nos dados de treinamento.

Os dados na coluna Timestamp devem estar no formato de tempo de época do Unix em segundos.

7. No Acesso ao serviço, você deve especificar uma função de serviço que possa acessar seus dados e fornecer uma chave KMS se seus dados estiverem criptografados. Escolha Criar e usar uma nova função de serviço e o Clean Rooms ML criará automaticamente uma função de serviço e adicionará a política de permissões necessária. Escolha Usar uma função de serviço existente e insira-a no campo Nome da função de serviço se você tiver uma função de serviço específica que deseja usar.

   Se seus dados estiverem criptografados, insira sua chave KMS no AWS KMS keycampo ou clique em Criar uma AWS KMS key para gerar uma nova chave KMS.
8. Se você quiser habilitar Tags para o conjunto de dados de treinamento, escolha Adicionar nova tag e insira o par de Chave e Valor.
9. Escolha Criar conjunto de dados de treinamento.

Para ver a ação de API correspondente, consulte CreateTrainingConjunto de dados.

Criar um modelo de semelhanças

Depois de criar um conjunto de dados de treinamento, estará tudo pronto para criar um modelo de semelhanças. É possível criar vários modelos de semelhanças com base em um único conjunto de dados de treinamento.

Você deve criar um banco de dados padrão em sua função AWS Glue Data Catalog ou incluir a `glue:createDatabase` permissão na função fornecida.

Para criar um modelo semelhante em AWS Clean Rooms

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, selecione Modelagem de ML.
3. Na guia Modelos de semelhanças, escolha Criar modelo de semelhanças.
4. Para Criar modelo de semelhanças, em Detalhes do modelo de semelhanças:
   a. Insira um Nome e uma Descrição opcional.
   b. Escolha o Conjunto de dados de treinamento que você deseja modelar na lista suspensa.

c. Insira uma Janela de treinamento opcional.

5. Se você quiser habilitar as configurações de criptografia personalizadas para o modelo de semelhanças, escolha Personalizar configurações de criptografia e insira a chave do KMS.
6. Se você quiser habilitar Tags para o modelo de semelhanças, escolha Adicionar nova tag e insira o par de Chave e Valor.
7. Escolha Criar modelo de semelhanças.

Para a ação de API correspondente, consulte CreateAudienceModelo.

Configurar um modelo de semelhanças

Depois de criar um modelo de semelhanças, estará tudo pronto para configurá-lo para uso em uma colaboração. É possível criar vários modelos de semelhanças configurados com base em um único modelo de semelhanças.

Para configurar um modelo semelhante no AWS Clean Rooms

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, selecione Modelagem de ML.
3. Na guia Modelos de semelhanças configurados, escolha Configurar modelo de semelhanças.
4. Para Configurar modelo de semelhanças, em Configurar detalhes do modelo de semelhanças:

   a. Insira um Nome e uma Descrição opcional.

   b. Escolha o Modelo de semelhanças que você deseja configurar na lista suspensa.

   c. Escolha o Tamanho mínimo de propagação correspondente que você deseja. Esse é o número mínimo de usuários nos dados do provedor de dados de seed que se sobrepõem aos usuários nos dados de treinamento. Esse valor deve ser maior que 0.
5. Em Métricas para compartilhar com outros membros, escolha se você deseja que o provedor de dados de seed em sua colaboração receba métricas do modelo, incluindo pontuações de relevância.
6. Em Localização do destino do segmento de semelhanças, insira o bucket do Amazon S3 para o qual o segmento de semelhanças é exportado. Esse bucket deve estar localizado na mesma região que seus outros recursos.
7. Em Acesso ao serviço, escolha o Nome do perfil de serviço existente que será usado para acessar essa tabela.

8. Escolha Configurar modelo semelhante.
9. Se quiser habilitar Tags para o recurso de tabela configurado, escolha Adicionar nova tag e, em seguida, insira o par Chave e Valor.

Para ver a ação de API correspondente, consulte CreateConfiguredAudienceModel.

Associar um modelo de semelhanças configurado

Depois de configurar um modelo de semelhanças, você pode associá-lo a uma colaboração.

Para associar um modelo semelhante configurado em AWS Clean Rooms

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Na guia Com associação ativa, escolha uma colaboração.
4. Na guia Modelagem de ML, escolha Associar modelo de semelhanças.
5. Para Associar modelo de semelhanças configurado, em Associar detalhes do modelo de semelhanças:
    a. Insira um Nome para o modelo de público configurado associado.
    b. Insira uma Descrição da tabela.

        A descrição ajuda a diferenciar entre outros modelos de público configurados associados com nomes semelhantes.
6. Para Modelo de semelhanças configurado, escolha um modelo de semelhanças configurado na lista suspensa.
7. Selecione Associar.

Para a ação de API correspondente, consulte CreateConfiguredAudienceModelAssociação.

Atualizar um modelo semelhante configurado

Depois de associar um modelo semelhante configurado, você pode atualizá-lo para alterar informações como nome, métricas a serem compartilhadas ou a localização de saída do Amazon S3.

Para atualizar um modelo semelhante configurado associado no AWS Clean Rooms

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Modelagem de ML.
3. Na guia Modelos semelhantes configurados, escolha um modelo semelhante configurado e selecione Editar.
4. Para Configurar modelo de semelhanças, em Configurar detalhes do modelo de semelhanças:
    a. Escolha o modelo Lookalike que você deseja configurar na lista suspensa.
    b. Escolha o Tamanho mínimo de propagação correspondente que você deseja. Esse é o número mínimo de usuários nos dados do provedor de dados de seed que se sobrepõem aos usuários nos dados de treinamento. Esse valor deve ser maior que 0.
5. Em Métricas para compartilhar com outros membros, escolha se você deseja que o provedor de dados de seed em sua colaboração receba métricas do modelo, incluindo pontuações de relevância.
6. Em Localização do destino do segmento de semelhanças, insira o bucket do Amazon S3 para o qual o segmento de semelhanças é exportado. Esse bucket deve estar localizado na mesma região que seus outros recursos.
7. Em Acesso ao serviço, escolha o Nome do perfil de serviço existente que será usado para acessar essa tabela.
8. Para Configuração avançada do tamanho do compartimento, escolha como você deseja configurar os tamanhos do compartimento de público.
9. Escolha Salvar alterações.

Para ver a ação de API correspondente, consulte UpdateConfiguredAudienceModel.

Trabalhando com segmentos semelhantes (provedor de dados iniciais)

Criar um segmento de semelhanças

Um segmento de semelhanças é um subconjunto dos dados de treinamento que mais se assemelha aos dados de seed.

Para criar um segmento semelhante no AWS Clean Rooms

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Na guia Com associação ativa, escolha uma colaboração.
4. Na guia Modelagem de ML, escolha Criar segmento de semelhanças.
5. Em Criar segmento de semelhanças, para Detalhes do segmento de semelhanças, insira um Nome e uma Descrição opcional.
6. Para Perfis de propagação, escolha a Fonte de entrada do Amazon S3 em que seus dados de propagação são armazenados.
7. Em Acesso ao serviço, escolha o Nome do perfil de serviço existente que será usado para acessar essa tabela.
8. Se você quiser habilitar Tags para o conjunto de dados de treinamento, escolha Adicionar nova tag e insira o par de Chave e Valor.
9. Escolha Criar segmento de semelhanças.

Para ver a ação de API correspondente, consulte StartAudienceGenerationJob.

Exportar um segmento de semelhanças

Depois de criar um segmento de semelhanças, é possível exportar os dados para um bucket do Amazon S3.

Para exportar um segmento semelhante em AWS Clean Rooms

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Na guia Com associação ativa, escolha uma colaboração.
4. Na guia Modelagem de ML, selecione um segmento de semelhanças e escolha Exportar.
5. Para Exportar modelo de semelhanças, em Exportar detalhes do modelo de semelhanças, insira um Nome e uma Descrição opcional.
6. Em Tamanho do segmento, escolha o tamanho desejado para o segmento exportado.
7. Escolha Exportar.

Para ver a ação de API correspondente, consulte StartAudienceExportJob.

Próximas etapas

Agora que você criou um modelo de semelhanças e exportou um segmento de seed, está tudo pronto para:

- Gerencie AWS Clean Rooms

Computação criptográfica para o Clean Rooms

A Computação Criptográfica para Clean Rooms (C3R) é um recurso AWS Clean Rooms que pode ser usado além das regras de análise. Com o C3R, as organizações podem reunir dados confidenciais para obter novos insights da análise de dados e, ao mesmo tempo, limitar criptograficamente o que pode ser aprendido por qualquer parte do processo. O C3R pode ser usado por duas ou mais partes que desejam colaborar com seus dados confidenciais, mas precisam usar apenas dados criptografados na nuvem.

O cliente de criptografia C3R é uma ferramenta de criptografia do lado do cliente que você pode usar para criptografar seus dados para uso. AWS Clean Rooms Quando você usa o cliente de criptografia C3R, os dados permanecem protegidos criptograficamente enquanto são usados em uma colaboração do AWS Clean Rooms . Como em uma AWS Clean Rooms colaboração regular, os dados de entrada são tabelas de banco de dados relacionais e o cálculo é expresso como uma consulta SQL. No entanto, o C3R suporta apenas um subconjunto limitado de consultas SQL em dados criptografados.

Especificamente, o C3R suporta SQL instruções JOIN e SELECT em dados protegidos criptograficamente. Cada coluna na tabela de entrada pode ser usada em exatamente um dos seguintes tipos de instrução SQL:

- As colunas protegidas criptograficamente para uso em JOIN declarações são chamadas de colunas fingerprint.
- As colunas protegidas criptograficamente para uso em SELECT declarações são chamadas de colunas sealed.
- As colunas que não são protegidas criptograficamente para uso em instruções JOIN ou SELECT são chamadas de colunas cleartext.

Em alguns casos, as instruções GROUP BY são apoiadas em colunas fingerprint. Para ter mais informações, consulte colunas Fingerprint. Atualmente, o C3R não suporta o uso de outras estruturas SQL em dados criptografados, como cláusulas WHERE ou funções agregadas como SUM e AVERAGE, mesmo que, de outra forma, fossem permitidas pelas regras de análise relevantes.

O C3R foi projetado para proteger dados em células individuais de uma tabela. Usando a configuração padrão do C3R, os dados subjacentes que um cliente disponibiliza para terceiros por meio de uma colaboração permanecem criptografados enquanto o conteúdo está em uso no AWS Clean Rooms. O C3R usa criptografia AES-GCM padrão do setor para todas as sealed

colunas e uma função pseudoaleatória padrão do setor, conhecida como Código de Autenticação de Mensagens Por Hash (HMAC), para proteger as colunas fingerprint.

Embora o C3R criptografe os dados em suas tabelas, as seguintes informações ainda podem ser inferidas:

- Informações sobre as tabelas em si, incluindo o número de colunas, os nomes das colunas e o número de linhas na tabela.
- Como acontece com a maioria das formas padrão de criptografia, o C3R não tenta ocultar o tamanho dos valores criptografados. O C3R oferece a capacidade de preencher valores criptografados para ocultar o tamanho exato dos textos transparentes. No entanto, um limite superior no comprimento dos textos não criptografados em cada coluna ainda pode ser revelado para outra pessoa.
- Informações em nível de log, como quando uma linha específica foi adicionada a uma tabela C3R criptografada.

Para obter mais informações sobre o C3R, consulte os tópicos a seguir.

Tópicos

Considerações ao usar a computação criptográfica para o Clean Rooms

A computação criptográfica para o Clean Rooms (C3R) busca maximizar a proteção de dados. No entanto, alguns casos de uso podem se beneficiar de níveis mais baixos de proteção de dados em troca de funcionalidades adicionais. Você pode fazer essas compensações específicas modificando

o C3R a partir de sua configuração mais segura. Como cliente, você deve estar ciente dessas desvantagens e determinar se elas são apropriadas para seu caso de uso. Compensações a serem consideradas incluem o seguinte:

Tópicos

- Permitir dados mistos cleartext e criptografados em suas tabelas
- Permitir valores repetidos em colunas fingerprint
- Afrouxar as restrições sobre como as colunas fingerprint são nomeadas
- Determinar como os valores NULL são representados

Para obter mais informações sobre como definir parâmetros para esses cenários, consulte Parâmetros de computação criptográfica.

Permitir dados mistos cleartext e criptografados em suas tabelas

Ter todos os dados criptografados do lado do cliente fornece a máxima proteção de dados. No entanto, isso limita certos tipos de consultas (por exemplo, a função agregada SUM). O risco de permitir dados cleartext é que é possível que qualquer pessoa com acesso às tabelas criptografadas possa inferir algumas informações sobre valores criptografados. Isso pode ser feito realizando uma análise estatística dos dados associados cleartext.

Por exemplo, imagine que você tivesse as colunas de `City` e `State`. A coluna `City` está cleartext e a coluna `State` está criptografada. Quando você vê o valor `Chicago` na coluna `City`, isso ajuda a determinar com alta probabilidade que `State` é `Illinois`. Por outro lado, se uma coluna é `City` e a outra coluna é `EmailAddress`, é improvável que um cleartext `City` revele algo sobre uma criptografia `EmailAddress`.

Para obter mais informações sobre o parâmetro para este cenário, consulte Parâmetro Permitir colunas cleartext.

Permitir valores repetidos em colunas fingerprint

Para uma abordagem mais segura, presumimos que qualquer coluna fingerprint contenha exatamente uma instância de uma variável. Nenhum item pode ser repetido em uma coluna fingerprint. O cliente de criptografia C3R mapeia esses valores cleartext em valores exclusivos que são indistinguíveis de valores aleatórios. Portanto, é impossível inferir informações sobre cleartext partir desses valores aleatórios.

O risco de valores repetidos em uma coluna fingerprint é que valores repetidos resultarão em valores repetidos de aparência aleatória. Assim, qualquer pessoa que tenha acesso às tabelas criptografadas poderia, em teoria, realizar uma análise estatística das colunas fingerprint que poderiam revelar informações sobre valores cleartext.

Novamente, suponha que a fingerprint coluna seja `State`, e que cada linha da tabela corresponda a uma família dos EUA. Ao fazer uma análise de frequência, pode-se inferir qual estado é `California` e qual é `Wyoming` com alta probabilidade. Essa inferência é possível porque `California` tem muito mais residentes do que `Wyoming`. Em contraste, digamos que a coluna fingerprint esteja em um identificador familiar e cada família apareça no banco de dados entre 1 e 4 vezes em um banco de dados de milhões de entradas. É improvável que uma análise de frequência revele alguma informação útil.

Para obter mais informações sobre o parâmetro para este cenário, consulte Parâmetro Permitir duplicatas.

Afrouxar as restrições sobre como as colunas fingerprint são nomeadas

Por padrão, presumimos que, quando duas tabelas são unidas usando colunas fingerprint criptografadas, essas colunas têm o mesmo nome em cada tabela. A razão técnica para esse resultado é que, por padrão, derivamos uma chave criptográfica diferente para criptografar cada coluna fingerprint. Essa chave é derivada de uma combinação da chave secreta compartilhada para a colaboração e do nome da coluna. Se tentarmos unir duas colunas com nomes de colunas diferentes, derivaremos chaves diferentes e não conseguiremos calcular uma junção válida.

Para resolver esse problema, você pode desativar o atributo que deriva as chaves do nome de cada coluna. Em seguida, o cliente de criptografia C3R usa uma única chave derivada para todas as colunas fingerprint. O risco é que outro tipo de análise de frequência possa ser feito para revelar informações.

Vamos usar o exemplo `City` e `State` novamente. Se obtivermos os mesmos valores aleatórios para cada coluna fingerprint (não incorporando o nome da coluna), `New York` tem o mesmo valor aleatório nas colunas `City` e `State`. Nova York é uma das poucas cidades dos EUA em que o `City` nome é igual ao nome `State`. Por outro lado, se seu conjunto de dados tiver valores completamente diferentes em cada coluna, nenhuma informação será vazada.

Para obter mais informações sobre o parâmetro para este cenário, consulte Parâmetro de permissão JOIN de colunas com nomes diferentes.

Determinar como os valores NULL são representados

A opção disponível para você é processar valores criptograficamente (criptografar e HMAC) como qualquer outro valor NULL. Se você não processar valores NULL como qualquer outro valor, as informações poderão ser reveladas.

Por exemplo, suponha que NULL na coluna `Middle Name` em cleartext indique pessoas sem nome do meio. Se você não criptografar esses valores, divulgará quais linhas na tabela criptografada são usadas por pessoas sem segundo nome. Essa informação pode ser um sinal de identificação para algumas pessoas em algumas populações. Mas se você processa valores NULL criptograficamente, certas consultas SQL agem de forma diferente. Por exemplo, as cláusulas GROUP BY não agrupam valores fingerprint NULL em colunas fingerprint.

Para obter mais informações sobre o parâmetro para este cenário, consulte Parâmetro de preservação de valores NULL.

Tipos de arquivos e dados suportados na computação criptográfica para o Clean Rooms

O cliente de criptografia C3R reconhece os seguintes tipos de arquivo:

- Arquivos CSV
- arquivos Parquet

Você pode usar o sinalizador `--fileFormat` no cliente de criptografia C3R para especificar explicitamente um formato de arquivo. Quando especificado explicitamente, o formato do arquivo não é determinado pela extensão do arquivo.

Tópicos

- Arquivos CSV
- arquivos Parquet
- Criptografar valores que não sejam de string

Arquivos CSV

Presume-se que um arquivo com extensão.csv esteja no formato CSV e contenha texto codificado em UTF-8. O cliente de criptografia C3R trata todos os valores como cadeias de caracteres.

Propriedades compatíveis em arquivos.csv

O cliente de criptografia C3R exige que os arquivos.csv tenham as seguintes propriedades:

- Pode ou não conter uma linha de cabeçalho inicial que nomeie cada coluna de forma exclusiva.
- Delimitado por vírgula. (Atualmente, não há suporte para delimitadores personalizados.)
- Texto codificado em UTF-8.

Corte de espaço em branco a partir de entradas.csv

Os espaços em branco à esquerda e à direita são cortados das entradas.csv.

Codificação personalizada NULL para um arquivo.csv

Um arquivo.csv pode usar codificação personalizada NULL.

Com o cliente de criptografia C3R, você pode especificar codificações personalizadas para entradas NULL nos dados de entrada usando o sinalizador `--csvInputNULLValue=<csv-input-null>`. O cliente de criptografia C3R pode usar codificações personalizadas no arquivo de saída gerado para entradas NULL usando o sinalizador `--csvOutputNULLValue=<csv-output-null>`.

> **Note**
>
> Uma entrada NULL é considerada sem conteúdo, especificamente no contexto de um formato tabular mais rico, como uma tabela SQL. Embora o domínio.csv não suporte explicitamente essa caracterização por motivos históricos, é uma convenção comum considerar uma entrada vazia que contém apenas espaço em branco NULL. Portanto, esse é o comportamento padrão do cliente de criptografia C3R e pode ser personalizado conforme necessário.

Como as entradas.csv são interpretadas pelo C3R

A tabela a seguir fornece exemplos de como as entradas.csv são organizadas (cleartext a cleartext para maior clareza) com base nos valores (se houver) fornecidos para os sinalizadores `--csvInputNULLValue=<csv-input-null>` e `--csvOutputNULLValue=<csv-output-null>`. Os espaços em branco à esquerda e à direita fora das aspas são cortados antes que o C3R interprete o significado de qualquer valor.

<csv-input-null>	**<csv-output-null>**	Entrada	Saída
Nenhum	Nenhum	,AnyProduct,	,AnyProduct,
Nenhum	Nenhum	, AnyProduct ,	,AnyProduct,
Nenhum	Nenhum	,"AnyProduct",	,AnyProduct,
Nenhum	Nenhum	, "AnyProduct" ,	,AnyProduct,
Nenhum	Nenhum	,,	,,
Nenhum	Nenhum	, ,	,,
Nenhum	Nenhum	,"",	,,
Nenhum	Nenhum	," ",	," ",
Nenhum	Nenhum	, " " ,	," ",
"AnyProduct"	"NULL"	,AnyProduct,	,NULL,
"AnyProduct"	"NULL"	, AnyProduct ,	,NULL,
"AnyProduct"	"NULL"	,"AnyProduct",	,NULL,
"AnyProduct"	"NULL"	, "AnyProduct" ,	,NULL,
Nenhum	"NULL"	,,	,NULL,
Nenhum	"NULL"	, ,	,NULL,
Nenhum	"NULL"	,"",	,NULL,
Nenhum	"NULL"	," ",	," ",
Nenhum	"NULL"	, " " ,	," ",
""	"NULL"	,,	,NULL,

<csv-input-null>	**<csv-output-null>**	Entrada	Saída
""	"NULL"	, ,	,NULL,
""	"NULL"	,"",	,"",
""	"NULL"	," ",	," ",
""	"NULL"	, " " ,	," ",
"\"\""	"NULL"	,,	,,
"\"\""	"NULL"	, ,	,,
"\"\""	"NULL"	,"",	,NULL,
"\"\""	"NULL"	," ",	," ",
"\"\""	"NULL"	, " " ,	," ",

Arquivo CSV sem cabeçalhos

O arquivo.csv de origem não precisa ter cabeçalhos na primeira linha que nomeiem cada coluna de forma exclusiva. No entanto, um arquivo.csv sem uma linha de cabeçalho requer um esquema de criptografia posicional. O esquema de criptografia posicional é necessário em vez do esquema mapeado típico usado para arquivos.csv com uma linha de cabeçalho e arquivos Parquet.

Um esquema de criptografia posicional especifica as colunas de saída por posição em vez de por nome. Um esquema de criptografia mapeado mapeia os nomes das colunas de origem para os nomes das colunas de destino. Para obter mais informações, incluindo uma discussão detalhada e exemplos dos dois formatos de esquema, consulte Esquemas de tabelas mapeadas e posicionais.

arquivos Parquet

Presume-se que um arquivo com uma extensão .parquet esteja no formato Apache Parquet.

Tipos de dados compatíveis Parquet

O cliente de criptografia C3R pode processar qualquer dado não complexo (ou seja, tipo primitivo) em um arquivo Parquet que represente um tipo de dados suportado pelo AWS Clean Rooms.

No entanto, somente colunas de string podem ser usadas para colunas sealed.

Os seguintes tipos de dados Parquet são compatíveis:

- Tipo primitivo `Binary` com as seguintes anotações lógicas:
  - Nenhum se `--parquetBinaryAsString` estiver definido (tipo de dados `STRING`)
  - `Decimal(scale, precision)` (tipo de dados`DECIMAL`)
  - `String` (tipo de dados `STRING`)
- Tipo de dados primitivo `Boolean` sem anotação lógica (tipo de dados `BOOLEAN`)
- Tipo de dados primitivo `Double` sem anotação lógica (tipo de dados `DOUBLE`)
- Tipo de dados primitivo `Fixed_Len_Binary_Array` com anotação lógica `Decimal(scale, precision)` (tipo de dados `DECIMAL`)
- Tipo de dados primitivo `Float` sem anotação lógica (tipo de dados `FLOAT`)
- Tipo de dados primitivo `Int32` com as seguintes anotações lógicas:
  - Nenhum (tipo de dados `INT`)
  - `Date` (tipo de dados `DATE`)
  - `Decimal(scale, precision)` (tipo de dados `DECIMAL`)
  - `Int(16, true)` (tipo de dados `SMALLINT`)
  - `Int(32, true)` (tipo de dados `INT`)
- Tipo de dados primitivo `Int64` com as seguintes anotações lógicas:
  - Nenhum (tipo de dados `BIGINT`)
  - `Decimal(scale, precision)` (tipo de dados `DECIMAL`)
  - `Int(64, true)` (tipo de dados `BIGINT`)
  - `Timestamp(isUTCAdjusted, TimeUnit.MILLIS)` (tipo de dados `TIMESTAMP`)
  - `Timestamp(isUTCAdjusted, TimeUnit.MICROS)` (tipo de dados `TIMESTAMP`)
  - `Timestamp(isUTCAdjusted, TimeUnit.NANOS)` (tipo de dados `TIMESTAMP`)

Criptografar valores que não sejam de string

Atualmente, somente valores de string são compatíveis com as colunas sealed.

Para arquivos.csv, o cliente de criptografia C3R trata todos os valores como texto codificado em UTF-8 e não faz nenhuma tentativa de interpretá-los de forma diferente antes da criptografia.

Para colunas de impressão digital, os tipos são agrupados em classes de equivalência. Uma classe de equivalência é um conjunto de tipos de dados que podem ser comparados de forma inequívoca em termos de igualdade por meio de um tipo de dados representativo.

As classes de equivalência permitem que impressões digitais idênticas sejam atribuídas ao mesmo valor semântico, independentemente da representação original. No entanto, o mesmo valor em duas classes de equivalência não resultará na mesma coluna de impressão digital.

Por exemplo, o valor `INTEGRAL 42` receberá a mesma impressão digital, independentemente de ser originalmente um `SMALLINT`, `INT` ou `BIGINT`. Além disso, o valor `INTEGRAL 0` nunca corresponderá ao valor `BOOLEAN FALSE` (que é representado pelo valor `0`).

As seguintes classes de equivalência e AWS Clean Rooms os tipos de dados correspondentes são suportados por colunas de impressão digital:

Classe de equivalência	Tipos de dados AWS Clean Rooms compatíveis
`BOOLEAN`	`BOOLEAN`
`DATE`	`DATE`
`INTEGRAL`	`BIGINT`, `INT`, `SMALLINT`
`STRING`	`CHAR`, `STRING`, `VARCHAR`

Nomes de colunas em computação criptográfica para o Clean Rooms

Por padrão, os nomes das colunas são importantes na Computação Criptográfica para o Clean Rooms.

Se o valor do parâmetro Permitir JOIN de colunas com nomes diferentes for falso, os nomes das colunas serão usados durante a criptografia das colunas fingerprint. Por esse motivo, por padrão, os colaboradores devem se coordenar com antecedência e usar os mesmos nomes de colunas de destino para dados que usarão instruções JOIN em consultas. Por padrão, colunas criptografadas para JOIN com nomes diferentes não são bem-sucedidas JOIN em nenhum valor.

Se o valor do parâmetro Permitir JOIN de colunas com nomes diferentes for verdadeiro, as instruções JOIN em colunas criptografadas como colunas fingerprint serão bem-sucedidas. Criptografar dados com esse parâmetro pode permitir alguma inferência dos valores cleartext. Por exemplo, se uma linha tiver o mesmo valor de Código de Autenticação de Mensagens por Hash (HMAC) na coluna `City` e na coluna `State`, o valor poderá ser `New York`.

Normalização dos nomes dos cabeçalhos das colunas

Os nomes dos cabeçalhos das colunas são normalizados pelo cliente de criptografia C3R. Qualquer espaço em branco à esquerda e à direita é removido e o nome da coluna é colocado em minúsculas para a saída transformada.

A normalização é aplicada antes de todos os outros cálculos, cálculos ou outras operações que possam ser afetadas pelos nomes das colunas. O arquivo de saída emitido contém apenas os nomes normalizados.

Tipos de colunas em computação criptográfica para o Clean Rooms

Este tópico fornece informações sobre os tipos de coluna na Computação Criptográfica para o Clean Rooms.

Tópicos

- colunas Fingerprint
- Colunas seladas
- colunas Cleartext

colunas Fingerprint

Colunas Fingerprint são colunas protegidas criptograficamente para uso em instruções de JOIN.

Os dados das colunas fingerprint não podem ser descriptografados. Somente dados de colunas seladas podem ser descriptografados.

As colunas Fingerprint só devem ser usadas nas seguintes cláusulas e funções SQL:

- JOIN (INNER, OUTER, LEFT, RIGHT, or FULL) em relação a outras colunas fingerprint:
  - Se o valor do parâmetro `allowJoinsOnColumnsWithDifferentNames` for definido como `false`, as duas colunas fingerprint do JOIN também deverão ter o mesmo nome.
- `SELECT COUNT()`
- `SELECT COUNT(DISTINCT )`
- `GROUP BY` (Use somente se a colaboração tiver definido o valor do parâmetro `preserveNulls` como `true`.)

As consultas que violam essas restrições podem gerar resultados incorretos.

Colunas seladas

Colunas seladas são colunas protegidas criptograficamente para uso em instruções de SELECT.

As colunas seladas devem ser usadas somente nas seguintes cláusulas e funções SQL:

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

> **Note**
>
> Não há suporte ao `SELECT COUNT(DISTINCT )`.

As consultas que violam essas restrições podem gerar resultados incorretos.

Preenchimento de dados para uma coluna sealed antes da criptografia

Quando você especifica que uma coluna deve ser uma coluna sealed, o C3R pergunta que tipo de preenchimento escolher. Preencher os dados antes da criptografia é opcional. Sem preenchimento (um tipo de bloco de `none`), o comprimento dos dados criptografados indica o tamanho do cleartext. Em algumas circunstâncias, o tamanho do cleartext pode expor o texto sem formatação. Com o

preenchimento (um tipo de teclado de `fixed` ou `max`), todos os valores são primeiro preenchidos em um tamanho comum e depois criptografados. Com o preenchimento, o tamanho dos dados criptografados não fornece informações sobre o tamanho original de cleartext, além de fornecer um limite superior para seu tamanho.

Se quiser preenchimento para uma coluna e o comprimento máximo em bytes dos dados nessa coluna for conhecido, use o preenchimento de `fixed`. Use um valor `length` que seja pelo menos tão grande quanto o comprimento em bytes do valor mais longo nessa coluna.

> **Note**
>
> Ocorre um erro e a criptografia falha se um valor for maior que o fornecido `length`.

Se você quiser preenchimento para uma coluna e o comprimento máximo em bytes dos dados nessa coluna não for conhecido, use o preenchimento. `max` Esse modo de preenchimento preenche todos os dados até o tamanho do valor mais longo, mais bytes adicionais `length`.

> **Note**
>
> Talvez você queira criptografar dados em lotes ou atualizar suas tabelas com novos dados periodicamente. Lembre-se de que o preenchimento de `max` preencherá as entradas até o comprimento (mais de `length` bytes) da entrada de texto simples mais longa em um determinado lote. Isso significa que o tamanho do texto cifrado pode variar de lote para lote. Portanto, se você souber o comprimento máximo de bytes de uma coluna, deverá usar `fixed` em vez de `max`.

colunas Cleartext

Cleartextcolunas são colunas que não são protegidas criptograficamente para uso em instruções JOIN ouSELECT.

As colunas Cleartext podem ser usadas em qualquer parte da consulta SQL.

Parâmetros de computação criptográfica

Os parâmetros de computação criptográfica estão disponíveis para colaborações usando a Computação Criptográfica para o Clean Rooms (C3R) ao criar uma colaboração. Você pode criar

uma colaboração usando o AWS Clean Rooms console ou a operação `CreateCollaboration` da API. No console, você pode definir valores para os parâmetros em Parâmetros de computação criptográfica depois de ativar a opção Suporte à computação criptográfica. Para obter mais informações, consulte os tópicos a seguir.

Tópicos

Parâmetro Permitir colunas cleartext

No console, você pode definir o parâmetro Permitir colunas cleartext ao criar uma colaboração para especificar se os dados cleartext são permitidos em uma tabela com dados criptografados.

A tabela a seguir descreve os valores do parâmetro Permitir colunas cleartext.

Valor do parâmetro	Descrição
Não	As colunas Cleartext não são permitidas na tabela criptogra fada. Todos os dados são protegidos criptograficamente.
Sim	As colunas Cleartext são permitidas na tabela criptografada. As colunas Cleartext não são protegidas criptograficamente e são incluídas como cleartext. Você deve observar o que os dados cleartext de suas linhas podem revelar sobre os outros dados na tabela. Para executar SUM ou AVG em colunas específicas, as colunas devem estar dentro de cleartext.

Usando a operação da API `CreateCollaboration`, para o parâmetro `dataEncryptionMetadata`, você pode definir o valor `allowCleartext` como `true` ou `false`. Para obter mais informações sobre operações de API, consulte a Referência de API do AWS Clean Rooms.

As colunas Cleartext correspondem às colunas que são classificadas como cleartext no esquema específico da tabela. Os dados nessas colunas não são criptografados e podem ser usados de qualquer forma. As colunas Cleartext podem ser úteis se os dados não forem confidenciais e/ou se for necessária mais flexibilidade do que uma coluna criptografada sealed ou fingerprint permite.

Parâmetro Permitir duplicatas

No console, você pode definir o parâmetro Permitir duplicatas ao criar uma colaboração para especificar se as colunas criptografadas para consultas JOIN podem conter valores não duplicados NULL.

> **Important**
>
> Os parâmetros Permitir duplicatas, Permitir JOIN de colunas com nomes diferentes e Preservar valores NULL têm efeitos separados, mas relacionados.

A tabela a seguir descreve os valores do parâmetro Permitir duplicatas.

Valor do parâmetro	Descrição
Não	Valores repetidos não são permitidos em uma coluna fingerpri nt. Todos os valores em uma única coluna fingerprint devem ser exclusivos.
Sim	Valores repetidos são permitidos em uma coluna fingerprint. Se você precisar unir colunas com valores repetidos, defina esse valor como Sim. Quando definido como Sim, os padrões de frequência que aparecem nas colunas fingerprint da tabela C3R ou nos resultados podem implicar em algumas informaçõ es adicionais sobre a estrutura dos dados cleartext.

Usando a operação da API `CreateCollaboration`, para o parâmetro `dataEncryptionMetadata`, você pode definir o valor `allowDuplicates` como `true` ou `false`. Para obter mais informações sobre operações de API, consulte a Referência de API do AWS Clean Rooms.

Por padrão, se dados criptografados precisarem ser usados em consultas JOIN, o cliente de criptografia C3R exigirá que essas colunas não tenham valores duplicados. Esse requisito é um esforço para aumentar a proteção de dados. Esse comportamento pode ajudar a garantir que padrões repetidos nos dados não sejam observáveis. No entanto, se quiser trabalhar com dados criptografados em consultas JOIN e não estiver preocupado com valores duplicados, o parâmetro Permitir duplicatas pode desativar essa verificação conservadora.

Parâmetro de permissão JOIN de colunas com nomes diferentes

No console, você pode definir o parâmetro Permitir JOIN de colunas com nomes diferentes ao criar uma colaboração para especificar se as instruções JOIN entre colunas com nomes diferentes são suportadas.

Para mais informações, consulte Normalização dos nomes dos cabeçalhos das colunas .

A tabela a seguir descreve os valores do parâmetro Permitir JOIN de colunas com nomes diferentes.

Valor do parâmetro	Descrição
Não	Não há suporte para junções de colunas fingerprint com nomes diferentes. Declarações JOINsó fornecem resultados precisos em colunas que têm o mesmo nome. **Important** O valor Não fornece maior segurança das informaçõ es, mas exige que os participantes da colaboração concordem previamente com os nomes das colunas. Se duas colunas tiverem nomes diferentes quando criptografadas como colunas fingerprint e a opção Permitir JOIN de colunas com nomes diferentes estiver definida como Não, as instruções JOIN nessas colunas não produzirão resultados. Isso ocorre porque nenhum valor pós-criptografia é compartilhado entre eles.
Sim	Há suporte para junções de colunas com nomes diferente s fingerprint. Para maior flexibilidade, os usuários podem

Valor do parâmetro	Descrição
	definir esse valor como Sim, o que permite instruções JOIN em colunas, independentemente do nome da coluna. Se definido como Sim, o cliente de criptografia C3R não considera o nome da coluna ao proteger as colunas fingerpri nt. Como resultado, valores comuns em diferentes colunas fingerprint são observáveis na tabela C3R. Por exemplo, se uma linha tiver o mesmo valor JOIN criptogra fado em uma coluna `City` e em uma coluna `State`, pode ser razoável inferir que esse valor é `New York`.

Usando a operação da API `CreateCollaboration`, para o parâmetro `dataEncryptionMetadata`, você pode definir o valor `allowJoinsOnColumnsWithDifferentNames` como `true` ou `false`. Para obter mais informações sobre operações de API, consulte a Referência de API do AWS Clean Rooms.

Por padrão, a criptografia da coluna fingerprint `targetHeader` é afetada pela configuração dessa coluna Etapa 4: gerar um esquema de criptografia para um arquivo tabular . Portanto, o mesmo valor cleartext tem representações criptografadas diferentes em cada coluna fingerprint diferente para a qual é criptografado.

Esse parâmetro pode ser útil para impedir a inferência de valores cleartext em alguns casos. Por exemplo, ver o mesmo valor criptografado em colunas fingerprint `City` e `State` pode ser usado para inferir razoavelmente que o valor é `New York`. No entanto, o uso desse parâmetro requer coordenação adicional com antecedência, para que todas as colunas a serem unidas nas consultas tenham nomes compartilhados.

Você pode usar o parâmetro Permitir JOIN de colunas com nomes diferentes para afrouxar essa restrição. Quando o valor do parâmetro é definido como `Yes`, ele permite que qualquer coluna criptografada JOIN seja usada em conjunto, independentemente do nome.

Parâmetro de preservação de valores NULL

No console, você pode definir o parâmetro Preservar valores NULL ao criar uma colaboração para indicar que não há nenhum valor presente para essa coluna.

A tabela a seguir descreve os valores do parâmetro Preservar valores NULL.

Valor do parâmetro	Descrição
Não	Os valores NULL não são preservados. Os valores NULL não aparecem como NULL em uma tabela criptografada. Os valores NULL aparecem como valores aleatórios exclusivos em uma tabela C3R.
Sim	Os valores NULL são preservados. Os valores NULL aparecem como NULL em uma tabela criptografada. Se você precisar de semântica de valores NULL SQL, você pode definir esse valor como Sim. Como resultado, as entradas NULL aparecem como NULL na tabela C3R, independentemente de a coluna estar criptografada e independentemente da configuração do parâmetro para Permitir duplicatas.

Usando a operação da API `CreateCollaboration`, para o parâmetro `dataEncryptionMetadata`, você pode definir o valor `preserveNulls` como `true` ou `false`. Para obter mais informações sobre operações de API, consulte a Referência de API do AWS Clean Rooms.

Quando o parâmetro Preservar valores NULL estiver definido como Não para a colaboração:

1. As entradas NULL nas colunas `cleartext` permanecem inalteradas.
2. As entradas NULL em colunas `fingerprint` criptografadas são criptografadas como valores aleatórios para ocultar seu conteúdo. A união em uma coluna criptografada com entradas NULL na coluna cleartext não produz nenhuma correspondência para nenhuma das entradas NULL. Nenhuma combinação é feita porque cada uma recebe seu próprio conteúdo aleatório exclusivo.
3. As entradas NULL em colunas `sealed` criptografadas são criptografadas.

Quando o valor do parâmetro Preservar valores NULL é definido como Sim para a colaboração, as entradas NULL de todas as colunas permanecem inalteradas, independentemente de a coluna NULL estar criptografada.

O parâmetro Preservar valores NULL é útil em cenários como enriquecimento de dados, nos quais você deseja compartilhar a falta de informações expressas como NULL. O parâmetro Preservar

valores NULL também é útil no formato fingerprint HMAC se você tiver valores NULL na coluna que deseja JOIN ou GROUP BY.

Se o valor dos parâmetros Permitir duplicatas e Preservar valores NULL estiver definido como Não, ter mais de uma entrada NULL em uma coluna fingerprint produzirá um erro e interromperá a criptografia. Se o valor de um dos parâmetros for definido como Sim, esse erro não ocorrerá.

Sinalizadores opcionais em computação criptográfica para o Clean Rooms

As seções a seguir descrevem os sinalizadores opcionais que você pode definir ao criptografar dados usando o cliente de criptografia C3R para personalização e teste de arquivos tabulares.

Tópicos

sinalizador `--csvInputNULLValue`

Você pode usar o sinalizador `--csvInputNULLValue` para especificar codificações personalizadas para entradas NULL nos dados de entrada ao criptografar dados usando o cliente de criptografia C3R.

A tabela a seguir resume o uso e os parâmetros desse sinalizador.

Uso	Parâmetros
Opcional. Os usuários podem especificar codificações personalizadas para entradas NULL nos dados de entrada.	Codificação de valores NULL especificada pelo usuário no arquivo CSV de entrada

Uma entrada NULL é uma entrada considerada sem conteúdo, especificamente no contexto de um formato tabular mais rico, como uma tabela SQL. Embora o domínio.csv não suporte explicitamente

essa caracterização por motivos históricos, é uma convenção comum considerar uma entrada vazia contendo apenas espaço em branco NULL. Portanto, esse é o comportamento padrão do cliente de criptografia C3R e pode ser personalizado conforme necessário.

sinalizador `--csvOutputNULLValue`

Você pode usar o sinalizador `--csvOutputNULLValue` para especificar codificações personalizadas para entradas NULL nos dados de saída ao criptografar dados usando o cliente de criptografia C3R.

A tabela a seguir resume o uso e os parâmetros desse sinalizador.

Uso	Parâmetros
Opcional. Os usuários podem especificar codificações personalizadas no arquivo de saída gerado para as entradas NULL.	Codificação de valores NULL especificada pelo usuário no arquivo CSV de saída

Uma entrada NULL é uma entrada considerada sem conteúdo, especificamente no contexto de um formato tabular mais rico, como uma tabela SQL. Embora o domínio.csv não suporte explicitamente essa caracterização por motivos históricos, é uma convenção comum considerar uma entrada vazia contendo apenas espaço em branco NULL. Portanto, esse é o comportamento padrão do cliente de criptografia C3R e pode ser personalizado conforme necessário.

sinalizador `--enableStackTraces`

Ao criptografar dados usando o cliente de criptografia C3R, use o sinalizador `--enableStackTraces` para fornecer informações contextuais adicionais para relatórios de erros quando o C3R encontrar um erro.

AWS não coleta erros. Se você encontrar um erro, use o rastreamento de pilha para solucionar o erro sozinho ou envie o rastreamento de pilha para AWS Support obter ajuda.

A tabela a seguir resume o uso e os parâmetros desse sinalizador.

Uso	Parâmetros
Opcional. Usado para fornecer informações contextuais adicionais para relatórios de erros	Nenhum

Uso	Parâmetros
quando o cliente de criptografia C3R encontra um erro.	

sinalizador `--dryRun`

Os comandos criptografar e descriptografar o cliente de criptografia C3R incluem um sinalizador opcional `--dryRun`. O sinalizador pega todos os argumentos fornecidos pelo usuário e verifica sua validade e consistência.

Você pode usar o sinalizador `--dryRun` para verificar se o arquivo do esquema é válido e consistente com o arquivo de entrada correspondente.

A tabela a seguir resume o uso e os parâmetros desse sinalizador.

Uso	Parâmetros
Opcional. Faz com que o cliente de criptografia C3R analise os parâmetros e verifique os arquivos, mas não realiza criptografia nem descriptografia.	Nenhum

sinalizador `--tempDir`

Talvez você queira usar um diretório temporário porque, às vezes, arquivos criptografados podem ser maiores do que arquivos não criptografados, dependendo de suas configurações. Os conjuntos de dados também devem ser criptografados por colaboração para funcionarem corretamente.

Ao criptografar dados usando o C3R, use o sinalizador `--tempDir` para especificar o local em que os arquivos temporários podem ser criados durante o processamento da entrada.

A tabela a seguir resume o uso e os parâmetros desse sinalizador.

Uso	Parâmetros
Os usuários podem especificar o local onde os arquivos temporários podem ser criados durante o processamento da entrada.	O padrão é o diretório temporário do sistema.

Consultas com computação criptográfica para o Clean Rooms

Este tópico fornece informações sobre como escrever consultas que usam tabelas de dados que foram criptografadas usando Computação Criptográfica para o Clean Rooms.

Tópicos

Consultas que se ramificam em NULL

Ter uma ramificação de consulta em uma instrução NULL significa usar uma sintaxe como `IF x IS NULL THEN 0 ELSE 1`.

As consultas sempre podem se ramificar nas instruções NULL em colunas cleartext.

As consultas podem se ramificar em nas instruções NULL em colunas sealed e colunas fingerprint somente quando o valor do parâmetro Preservar valores NULL (`preserveNulls`) estiver definido como `true`.

As consultas que violam essas restrições podem gerar resultados incorretos.

Mapeamento de uma coluna de origem para várias colunas de destino

Uma coluna de origem pode ser mapeada para várias colunas de destino. Por exemplo, talvez você queira usar JOIN e SELECT em uma coluna.

Para ter mais informações, consulte Usar os mesmos dados para ambas as consultas JOIN e SELECT.

Usar os mesmos dados para ambas as consultas JOIN e SELECT

Se os dados em uma coluna não forem confidenciais, eles poderão aparecer em uma coluna de destino cleartext, o que permite que sejam usados para qualquer finalidade.

Se os dados em uma coluna forem confidenciais e precisarem ser usados para consultas SELECT, mapeie essa coluna de origem para duas colunas de destino no arquivo de saída JOIN. Uma coluna é criptografada com `type` como coluna fingerprint e uma coluna é criptografada com `type` como coluna selada. A geração do esquema interativo do cliente de criptografia C3R sugere sufixos de cabeçalho de `_fingerprint` e `_sealed`. Esses sufixos de cabeçalho podem ser uma convenção útil para diferenciar essas colunas rapidamente.

Diretrizes para o cliente de criptografia C3R

O cliente de criptografia C3R é uma ferramenta que permite às organizações reunir dados confidenciais para obter novos insights da análise de dados. A ferramenta limita criptograficamente o que pode ser aprendido por qualquer parte e AWS no processo. Embora isso seja de vital importância, o processo de proteger dados criptograficamente pode adicionar uma sobrecarga significativa em termos de recursos de computação e armazenamento. Portanto, é importante entender as vantagens e desvantagens de usar cada configuração e como otimizá-las e, ao mesmo tempo, manter as garantias criptográficas desejadas. Este tópico se concentra nas implicações de desempenho de diferentes configurações no cliente e nos esquemas de criptografia C3R.

Todas as configurações de criptografia do cliente de criptografia C3R oferecem diferentes garantias criptográficas. As configurações em nível de colaboração são mais seguras por padrão. Ativar funcionalidades adicionais ao criar uma colaboração enfraquece as garantias de privacidade, permitindo que atividades como análise de frequência sejam conduzidas no texto cifrado. Para obter mais informações sobre como essas configurações são usadas e quais são suas implicações, consulte Computação criptográfica.

Tópicos

- Implicações de desempenho para tipos de coluna
- Solução de problemas de aumentos imprevistos no tamanho do texto cifrado

Implicações de desempenho para tipos de coluna

O C3R usa três tipos de coluna: cleartext, fingerprint e sealed. Cada um desses tipos de coluna fornece garantias criptográficas diferentes e tem diferentes usos pretendidos. Nas seções a seguir, são discutidas as implicações de desempenho do tipo de coluna e o impacto no desempenho de cada configuração.

Tópicos

colunas Cleartext

As colunas Cleartext não são alteradas de seu formato original e não são processadas criptograficamente de forma alguma. Esse tipo de coluna não pode ser configurado e não afeta o desempenho do armazenamento ou da computação.

colunas Fingerprint

As colunas Fingerprint devem ser usadas para unir dados em várias tabelas. Para esse fim, o tamanho do texto cifrado resultante deve ser sempre o mesmo. No entanto, essas colunas são afetadas pelas configurações de nível de colaboração. As colunas Fingerprint podem ter vários graus de impacto no tamanho do arquivo de saída, dependendo do conteúdo cleartext contido na entrada.

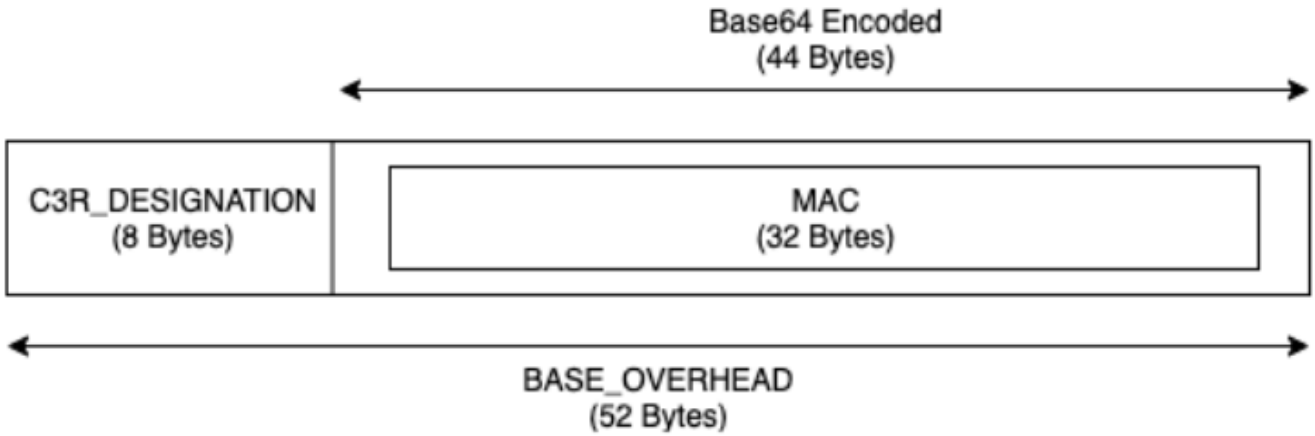
Tópicos

Sobrecarga básica para colunas fingerprint

Há uma sobrecarga básica para colunas fingerprint. Essa sobrecarga é constante e substitui o tamanho dos cleartext bytes.

Os dados nas colunas fingerprint são processados criptograficamente por meio de uma função de Código de Autenticação de Mensagens por Hash (HMAC), que transforma os dados em um código de autenticação de mensagem (MAC) de 32 bytes. Esses dados são então processados por meio de um codificador base64, adicionando aproximadamente 33% ao tamanho do byte. Ele é pré-fixado com uma designação C3R de 8 bytes para designar o tipo de coluna à qual os dados pertencem e a versão do cliente que os produziu. O resultado final é 52 bytes. Esse resultado é então multiplicado pela contagem de linhas para obter a sobrecarga base total (use o número total de valores não `null` se `preserveNulls` estiver definido como verdadeiro).

A imagem a seguir mostra como *`BASE_OVERHEAD = C3R_DESIGNATION + (MAC * 1.33)`*



O texto cifrado de saída nas colunas fingerprint sempre será de 52 bytes. Isso pode ser uma diminuição significativa no armazenamento se a média cleartext dos dados de entrada for superior a 52 bytes (por exemplo, endereços completos). Isso pode ser um aumento significativo no armazenamento se a média cleartext dos dados de entrada for inferior a 52 bytes (por exemplo, idade do cliente).

Configurações de colaboração para colunas fingerprint

Configuração da **`preserveNulls`**

Quando a configuração do nível de colaboração `preserveNulls` é `false` (padrão), cada valor `null` é substituído por 32 bytes exclusivos e aleatórios e processado como se não fosse `null`. O resultado é que cada valor `null` agora tem 52 bytes. Isso pode adicionar requisitos de armazenamento significativos para tabelas que contêm dados muito esparsos em comparação com quando essa configuração é `true` e `null` os valores são passados como `null`.

Se você não precisar das garantias de privacidade dessa configuração e preferir reter valores `null` em seus conjuntos de dados, habilite a configuração `preserveNulls` no momento em que a

colaboração for criada. A configuração `preserveNulls` não pode ser alterada após a criação da colaboração.

Dados de exemplo para uma coluna fingerprint

Veja a seguir um exemplo de conjunto de dados de entrada e saída para uma coluna fingerprint com configurações a serem reproduzidas. Outras configurações em nível de colaboração, como `allowCleartext` e `allowDuplicates` não afetam os resultados, e podem ser definidas como `true` ou `false` se você estiver tentando se reproduzir localmente.

Exemplo de segredo compartilhado: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Exemplo de ID de colaboração: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

allowJoinsOnColumnsWithDifferentNames: essa configuração `True` não afeta os requisitos de desempenho ou armazenamento. No entanto, essa configuração torna a escolha do nome da coluna irrelevante ao reproduzir os valores mostrados nas tabelas a seguir.

Exemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Saída	`null`
Deterministic	`Yes`
Bytes de entrada	0
Bytes de saída	0

Exemplo 2

Entrada	`null`
`preserveNulls`	`FALSE`
Saída	`01:hmac:3lkFjthvV3IUu6mMvFc1a+XAHwgw/ElmOq4p3Yg25kk=`

Deterministic	No
Bytes de entrada	0
Bytes de saída	52

Exemplo 3

Entrada	`empty string`
`preserveNulls`	-
Saída	`01:hmac:oKTgi3Gba+eUb3JteSz 2EMgXUkF1WgM77UP0Ydw5kPQ=`
Deterministic	`Yes`
Bytes de entrada	0
Bytes de saída	52

Exemplo 4

Entrada	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Saída	`01:hmac:kU/IqwG7FMmzzshr0B9 scomE0UJUEE7j9keTctplGww=`
Deterministic	`Yes`
Bytes de entrada	26
Bytes de saída	52

Exemplo 5

Entrada	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Saída	`01:hmac:ks3htnQbw2vdhCRFF6J NzW5LMndJaHG57uvE26mBtSs=`
Deterministic	`Yes`
Bytes de entrada	62
Bytes de saída	52

Colunas fingerprint de solução de problemas

Por que o texto cifrado em minhas colunas fingerprint é várias vezes maior do que o tamanho do cleartext que estava nele?

O texto cifrado em uma coluna fingerprint tem sempre 52 bytes de comprimento. Se seus dados de entrada forem pequenos (por exemplo, a idade dos clientes), eles mostrarão um aumento significativo no tamanho. Isso também pode acontecer se a configuração `preserveNulls` estiver definida como `false`.

Por que o texto cifrado em minhas colunas fingerprint é várias vezes menor do que o tamanho do cleartext que estava nele?

O texto cifrado em uma coluna fingerprint tem sempre 52 bytes de comprimento. Se seus dados de entrada forem grandes (por exemplo, os endereços completos dos clientes), eles mostrarão uma diminuição significativa no tamanho.

Como posso saber se preciso das garantias criptográficas fornecidas por **`preserveNulls`**?

Infelizmente, a resposta é que depende. No mínimo, the section called “Parâmetros” deve ser revisado como a configuração `preserveNulls` está protegendo seus dados. No entanto, recomendamos que você consulte os requisitos de tratamento de dados da sua organização e quaisquer contratos aplicáveis à respectiva colaboração.

Por que eu tenho que incorrer na sobrecarga de base64?

Para permitir a compatibilidade com formatos de arquivo tabulares, como CSV, a codificação base64 é necessária. Embora alguns formatos de arquivo Parquet possam suportar representações binárias de dados, é importante que todos os participantes de uma colaboração representem os dados da mesma forma para garantir resultados de consulta adequados.

colunas Sealed

As colunas Sealed devem ser usadas para transferir dados entre membros de uma colaboração. O texto cifrado nessas colunas não é determinístico e tem um impacto significativo no desempenho e no armazenamento com base na configuração das colunas. Essas colunas podem ser configuradas individualmente e geralmente têm o maior impacto no desempenho do cliente de criptografia C3R e no tamanho do arquivo de saída resultante.

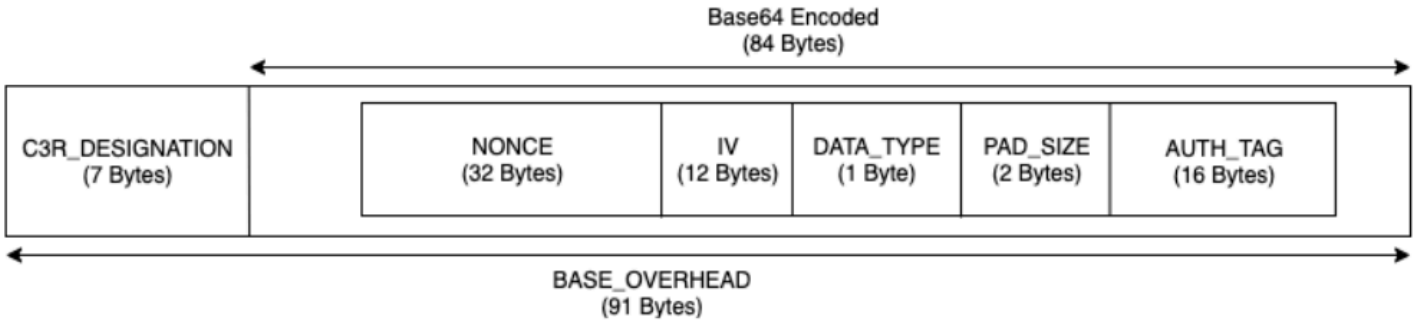
Tópicos

Sobrecarga básica para colunas sealed

Há uma sobrecarga básica para colunas sealed. Essa sobrecarga é constante e é adicionada ao tamanho dos bytes de preenchimento cleartext e (se houver).

Antes de qualquer criptografia, os dados nas colunas sealed são prefixados com um caractere de 1 byte que designa o tipo de dado contido. Se o preenchimento for selecionado, os dados serão então preenchidos e anexados com 2 bytes indicando o tamanho do bloco. Depois que esses bytes são adicionados, os dados são processados criptograficamente usando o AES-GCM e armazenados com IV (12 bytes), nonce (32 bytes) e Auth Tag (16 bytes). Esses dados são então processados por meio de um codificador base64, adicionando aproximadamente 33% ao tamanho do byte. Os dados são prefixados com uma designação C3R de 7 bytes para designar a que tipo de coluna os dados pertencem e a versão do cliente usada para produzi-los. O resultado é uma sobrecarga básica final de 91 bytes. Esse resultado pode então ser multiplicado pela contagem de linhas para obter a sobrecarga base total (use o número total de valores não nulos se `preserveNulls` estiver definido como verdadeiro).

A imagem a seguir mostra como *BASE_OVERHEAD = C3R_DESIGNATION + ((NONCE + IV + DATA_TYPE + PAD_SIZE + AUTH_TAG) * 1.33)*



Configurações de colaboração para colunas sealed

Configuração da **`preserveNulls`**

Quando a configuração do nível de colaboração `preserveNulls` é `false` (padrão), cada valor `null` é exclusivo, aleatório de 32 bytes e processado como se não fosse `null`. O resultado é que cada valor `null` agora tem 91 bytes (mais se for preenchido). Isso pode adicionar requisitos de armazenamento significativos para tabelas que contêm dados muito esparsos em comparação com quando essa configuração é `true` e `null` os valores são passados como`null`.

Se você não precisar das garantias de privacidade dessa configuração e preferir reter valores `null` em seus conjuntos de dados, habilite a configuração `preserveNulls` no momento em que a colaboração for criada. A configuração `preserveNulls` não pode ser alterada após a criação da colaboração.

Colunas sealed de configurações do esquema: tipos de preenchimento

Tópicos

- Tipo de almofada de none
- Tipo de almofada de fixed
- Tipo de almofada de max

Tipo de almofada de **none**

Selecionar um tipo de bloco de `none` não adiciona nenhum preenchimento ao cleartext e não adiciona nenhuma sobrecarga adicional à sobrecarga básica descrita anteriormente. Nenhum preenchimento resulta no tamanho de saída mais eficiente em termos de espaço. No entanto, ele

não oferece as mesmas garantias de privacidade que os tipos de preenchimento `fixed` e `max`. Isso ocorre porque o tamanho do subjacente cleartext é discernível do tamanho do texto cifrado.

Tipo de almofada de **`fixed`**

Selecionar um tipo de bloco de `fixed` é uma medida de preservação da privacidade para ocultar os tamanhos dos dados contidos em uma coluna. Isso é feito preenchendo tudo o que é cleartext fornecido `pad_length` antes de ser criptografado. Qualquer dado que exceda esse tamanho faz com que o cliente de criptografia C3R falhe.

Como o preenchimento é adicionado ao cleartext antes de ser criptografado, o AES-GCM tem um mapeamento de 1 para 1 de dois bytes de texto cifrado cleartext. A codificação base64 adicionará 33 por cento. A sobrecarga adicional de armazenamento do preenchimento pode ser calculada subtraindo o comprimento médio do valor cleartext do `pad_length` e multiplicando-o por 1,33. O resultado é a sobrecarga média de preenchimento por registro. Esse resultado pode então ser multiplicado pelo número de linhas para obter a sobrecarga total de preenchimento (use o número total de valores não `null` se `preserveNulls` estiver definido como `true`).

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

Recomendamos que você selecione o mínimo `pad_length` que engloba o maior valor em uma coluna. Por exemplo, se o maior valor for 50 bytes, um `pad_length` de 50 é suficiente. Um valor maior do que isso só aumentará a sobrecarga de armazenamento.

O preenchimento fixo não adiciona nenhuma sobrecarga computacional significativa.

Tipo de almofada de **`max`**

Selecionar um tipo de bloco de `max` é uma medida de preservação da privacidade para ocultar os tamanhos dos dados contidos em uma coluna. Isso é feito preenchendo todo o valor cleartext até o maior valor na coluna, mais o adicional, `pad_length` antes de ser criptografado. Geralmente, o preenchimento `max` fornece as mesmas garantias que o preenchimento `fixed` para um único conjunto de dados, ao mesmo tempo em que permite não saber o maior valor cleartext na coluna. No entanto, o preenchimento `max` pode não fornecer as mesmas garantias de privacidade que o preenchimento `fixed` entre atualizações, pois o maior valor nos conjuntos de dados individuais pode ser diferente.

Recomendamos que você selecione um adicional `pad_length` de 0 ao usar o preenchimento `max`. Esse comprimento preenche todos os valores para que tenham o mesmo tamanho do maior valor na coluna. Um valor maior do que isso só aumentará a sobrecarga de armazenamento.

Se o maior valor cleartext for conhecido para uma determinada coluna, recomendamos que você use o tipo `fixed` pad em vez disso. O uso do preenchimento `fixed` cria consistência nos conjuntos de dados atualizados. O uso do preenchimento `max` resulta em cada subconjunto de dados sendo preenchido até o maior valor que estava no subconjunto.

Dados de exemplo para uma coluna sealed

Veja a seguir um exemplo de conjunto de dados de entrada e saída para uma coluna sealed com configurações a serem reproduzidas. Outras configurações em nível de colaboração, como `allowCleartext`, `allowJoinsOnColumnsWithDifferentNames` e `allowDuplicates` não afetam os resultados e podem ser definidas como `true` ou `false` se você estiver tentando se reproduzir localmente. Embora essas sejam as configurações básicas a serem reproduzidas, a coluna sealed não é determinística e os valores mudarão sempre. O objetivo é mostrar os bytes de entrada em comparação com os bytes de saída. Os valores `pad_length` de exemplo foram escolhidos intencionalmente. Eles mostram que o preenchimento `fixed` resulta nos mesmos valores do preenchimento `max` com as configurações `pad_length` mínimas recomendadas ou quando um preenchimento adicional é desejado.

Exemplo de segredo compartilhado: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Exemplo de ID de colaboração: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

Tópicos

Tipo de preenchimento de **none**

Exemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Saída	`null`

Deterministic	Yes
Bytes de entrada	0
Bytes de saída	0

Exemplo 2

Entrada	null
preserveNulls	FALSE
Saída	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSPbNIJfG3iXmu6cbCUrizuV
Deterministic	No
Bytes de entrada	0
Bytes de saída	91

Exemplo 3

Entrada	empty string
preserveNulls	-
Saída	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSPEM6qR8DWC2PB2GMlX41YK
Deterministic	No
Bytes de entrada	0
Bytes de saída	91

Exemplo 4

Entrada	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9sGL5VLDQeHzh6DmPpyWNuI=`
Deterministic	No
Bytes de entrada	26
Bytes de saída	127

Exemplo 5

Entrada	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Deterministic	No
Bytes de entrada	62
Bytes de saída	175

Tipo de almofada de **`fixed`** (Exemplo 1)

Neste exemplo, `pad_length` é 62 e a maior entrada é 62 bytes.

Exemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Saída	`null`
Deterministic	`Yes`
Bytes de entrada	0
Bytes de saída	0

Exemplo 2

Entrada	`null`
`preserveNulls`	`FALSE`
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=`
Deterministic	`No`
Bytes de entrada	0
Bytes de saída	175

Exemplo 3

Entrada	`empty string`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=`
Deterministic	No
Bytes de entrada	0
Bytes de saída	175

Exemplo 4

Entrada	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`
Deterministic	No
Bytes de entrada	26
Bytes de saída	175

Exemplo 5

Entrada	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqdP4/ QOQ3cXb/pbvPcnnohrHIGSX54ua+1/ JfcVjc=`
Deterministic	No
Bytes de entrada	62
Bytes de saída	175

Tipo de almofada de **`fixed`** (Exemplo 2)

Neste exemplo, `pad_length` é 162 e a maior entrada é 62 bytes.

Exemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Saída	`null`
Deterministic	`Yes`
Bytes de entrada	0
Bytes de saída	0

Exemplo 2

Entrada	`null`
`preserveNulls`	`FALSE`
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb`
Deterministic	No
Bytes de entrada	0
Bytes de saída	307

Exemplo 3

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

	pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT
Deterministic	No
Bytes de entrada	0
Bytes de saída	307

Exemplo 4

Entrada	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
Saída	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf
Deterministic	No
Bytes de entrada	26
Bytes de saída	307

Exemplo 5

Entrada	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/QOQ3cXb/pbvPcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i``
Deterministic	No
Bytes de entrada	62
Bytes de saída	307

Tipo de almofada de **`max`** (Exemplo 1)

Neste exemplo, `pad_length` é 0 e a maior entrada é 62 bytes.

Exemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Saída	`null`
Deterministic	`Yes`

Bytes de entrada	0
Bytes de saída	0

Exemplo 2

Entrada	`null`
`preserveNulls`	`FALSE`
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=`
Deterministic	No
Bytes de entrada	0
Bytes de saída	175

Exemplo 3

Entrada	`empty string`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=`

Deterministic	No
Bytes de entrada	0
Bytes de saída	175

Exemplo 4

Entrada	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`
Deterministic	No
Bytes de entrada	26
Bytes de saída	175

Exemplo 5

Entrada	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8t`

	`RFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Deterministic	`No`
Bytes de entrada	62
Bytes de saída	175

Tipo de almofada de **`max`** (Exemplo 2)

Neste exemplo, `pad_length` é 100 e a maior entrada é 62 bytes.

Exemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Saída	`null`
Deterministic	`Yes`
Bytes de entrada	0
Bytes de saída	0

Exemplo 2

Entrada	`null`
`preserveNulls`	`FALSE`
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcnkB0xbLWD7z`

	`NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb`
Deterministic	No
Bytes de entrada	0
Bytes de saída	307

Exemplo 3

Entrada	`empty string`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT`
Deterministic	No
Bytes de entrada	0
Bytes de saída	307

Exemplo 4

Entrada	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Saída	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf`
Deterministic	No
Bytes de entrada	26
Bytes de saída	307

Exemplo 5

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

	`NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i`
Deterministic	No
Bytes de entrada	62
Bytes de saída	307

Colunas sealed de solução de problemas

Por que o texto cifrado em minhas colunas sealed é várias vezes maior do que o tamanho do cleartext que estava nele?

Isso depende de diversos fatores. Por um lado, o texto cifrado em uma coluna Cleartext tem sempre pelo menos 91 bytes de comprimento. Se seus dados de entrada forem pequenos (por exemplo, a idade dos clientes), eles mostrarão um aumento significativo no tamanho. Segundo, se `preserveNulls` fossem definidos como `false` e seus dados de entrada contivessem muitos valores `null`, cada um desses valores `null` teria sido transformado em 91 bytes de texto cifrado. Por fim, se você usa preenchimento, por definição, bytes são adicionados aos dados cleartext antes de serem criptografados.

A maioria dos meus dados em uma coluna sealed é muito pequena e preciso usar preenchimento. Posso simplesmente remover os valores grandes e processá-los separadamente para economizar espaço?

Não recomendamos remover valores grandes e processá-los separadamente. Isso altera as garantias de privacidade que o cliente de criptografia C3R está fornecendo. Como modelo de ameaça, suponha que um observador possa ver os dois conjuntos de dados criptografados. Se o observador perceber que um subconjunto de dados tem uma coluna preenchida significativamente mais ou menos do que outro subconjunto, ele poderá fazer inferências sobre o tamanho dos dados em cada subconjunto. Por exemplo, suponha que uma coluna `fullName` seja preenchida com um total de 40 bytes em um arquivo e seja preenchida com 800 bytes em outro arquivo. Um observador pode presumir que um conjunto de dados contém o nome mais longo do mundo (747 bytes).

Preciso fornecer preenchimento extra ao usar o tipo de preenchimento**`max`**?

Não. Ao usar o preenchimento `max`, recomendamos que o `pad_length`, também conhecido como preenchimento adicional além do maior valor na coluna, seja definido como 0.

Posso simplesmente escolher um grande **`pad_length`** ao usar o preenchimento **`fixed`** para evitar me preocupar se o maior valor caberá?

Sim, mas o tamanho grande da almofada é ineficiente e usa mais espaço de armazenamento do que o necessário. Recomendamos que você verifique o tamanho do maior valor e defina `pad_length` com esse valor.

Como posso saber se preciso das garantias criptográficas fornecidas por **`preserveNulls`**?

Infelizmente, a resposta é que depende. No mínimo, Computação criptográfica para o Clean Rooms deve ser revisado como a configuração `preserveNulls` está protegendo seus dados. No entanto, recomendamos que você consulte os requisitos de tratamento de dados da sua organização e quaisquer contratos aplicáveis à respectiva colaboração.

Por que eu tenho que incorrer na sobrecarga de base64?

Para permitir a compatibilidade com formatos de arquivo tabulares, como CSV, a codificação base64 é necessária. Embora alguns formatos de arquivo Parquet possam suportar representações binárias de dados, é importante que todos os participantes de uma colaboração representem os dados da mesma forma para garantir resultados de consulta adequados.

Solução de problemas de aumentos imprevistos no tamanho do texto cifrado

Digamos que você criptografou seus dados e o tamanho dos dados resultantes seja surpreendentemente grande. As etapas a seguir podem ajudá-lo a identificar onde ocorreu o aumento de tamanho e quais ações, se houver, você pode tomar.

Identificar onde ocorreu o aumento de tamanho

Antes de solucionar o motivo pelo qual seus dados criptografados são significativamente maiores do que seus dados cleartext, você deve primeiro identificar onde está o aumento no tamanho. As colunas Cleartext podem ser ignoradas com segurança porque não foram alteradas. Examine as colunas fingerprint e sealed restantes e escolha uma que pareça significativa.

Identificar o motivo pelo qual o aumento de tamanho ocorreu

Uma coluna fingerprint ou sealed pode contribuir para o aumento do tamanho.

Tópicos

O aumento de tamanho vem de uma coluna fingerprint?

Se a coluna que mais contribui para o aumento no armazenamento for uma coluna fingerprint, provavelmente é porque os dados cleartext são pequenos (por exemplo, idade do cliente). Cada texto cifrado fingerprint resultante tem 52 bytes de comprimento. Infelizmente, nada pode ser feito sobre esse problema em uma column-by-column base. Para obter mais informações, consulte Sobrecarga básica para colunas fingerprint para obter detalhes sobre essa coluna, inclusive como ela afeta os requisitos de armazenamento.

A outra causa possível do aumento de tamanho em uma coluna fingerprint é a configuração de colaboração, `preserveNulls`. Se a configuração de colaboração para `preserveNulls` estiver desativada (a configuração padrão), todos os valores `null` nas colunas fingerprint se tornarão 52 bytes de texto cifrado. Não há nada que possa ser feito para isso na colaboração atual. A configuração `preserveNulls` é definida no momento em que uma colaboração é criada e todos os colaboradores devem usar a mesma configuração para garantir os resultados corretos da consulta. Para obter mais informações sobre a configuração `preserveNulls` e como ativá-la afeta as garantias de privacidade de seus dados, consulte Computação criptográfica.

O aumento de tamanho vem de uma coluna sealed?

Se a coluna que mais contribui para o aumento no armazenamento for uma coluna sealed, há alguns detalhes que podem contribuir para o aumento do tamanho.

Se os dados cleartext forem pequenos (por exemplo, idade do cliente), cada texto cifrado sealed resultante terá pelo menos 91 bytes de comprimento. Infelizmente, nada pode ser feito sobre esse problema. Para obter mais informações, consulte Sobrecarga básica para colunas sealed para obter detalhes sobre essa coluna, inclusive como ela afeta os requisitos de armazenamento.

A segunda principal causa do aumento do armazenamento nas colunas sealed é o preenchimento. O preenchimento adiciona bytes extras ao cleartext antes de ser criptografado para ocultar o tamanho dos valores individuais em um conjunto de dados. Recomendamos que você defina o preenchimento com o valor mínimo possível para seu conjunto de dados. No mínimo, `pad_length` para o preenchimento `fixed` deve ser definido para abranger o maior valor possível na coluna. Qualquer configuração maior do que essa não adiciona garantias adicionais de privacidade. Por exemplo, se

você sabe que o maior valor possível em uma coluna pode ser de 50 bytes, recomendamos que você defina o valor `pad_length` para 50 bytes. No entanto, se a coluna sealed estiver usando preenchimento `max`, recomendamos que você defina `pad_length` como 0 bytes. Isso ocorre porque o preenchimento `max` se refere ao preenchimento adicional além do maior valor na coluna.

A causa final possível do aumento de tamanho em uma coluna sealed é a configuração de colaboração, `preserveNulls`. Se a configuração de colaboração para `preserveNulls` estiver desativada (a configuração padrão), todos os valores `null` nas colunas sealed se tornarão 91 bytes de texto cifrado. Não há nada que possa ser feito para isso na colaboração atual. A configuração `preserveNulls` é definida no momento em que uma colaboração é criada, e todos os colaboradores devem usar a mesma configuração para garantir os resultados corretos da consulta. Para obter mais informações sobre essa configuração e como ativá-la afeta as garantias de privacidade de seus dados, consulte Computação criptográfica.

Login de consulta AWS Clean Rooms

O registro de consultas é um recurso do AWS Clean Rooms. Quando você cria uma colaboração e ativa o registro de consultas, os membros podem armazenar registros de consultas relevantes para eles no Amazon CloudWatch Logs.

Com os logs de consultas, os membros podem determinar se as consultas estão em conformidade com as regras de análise e se alinham ao contrato de colaboração. Além disso, os logs de consulta ajudam a apoiar as auditorias.

Quando a opção Registro de consultas está ativada no AWS Clean Rooms console, os registros de consulta incluem o seguinte:

- `analysisRule` – A regra de análise para a tabela configurada.
- `analysisTemplateArn` – O modelo de análise que foi executado (aparece dependendo da regra de análise).
- `collaborationId` – O identificador exclusivo para colaboração na qual a consulta foi executada.
- `configuredTableID` – O identificador exclusivo da tabela configurada referenciada na consulta.
- `directQueryAnalysisRulePolicy.custom.allowedAnalysis` – O modelo de análise pode ser executado na tabela configurada (aparece dependendo da regra de análise).
- `directQueryAnalysisRulePolicy.v1.custom.allowedAnalysisProviders` – Os provedores de consulta autorizados a criar uma consulta (aparece dependendo da regra de análise).
- `eventID` – O identificador exclusivo da consulta executada. Depois de 31 de agosto de 2023, o identificador exclusivo é o mesmo que o `protectedQueryID`.
- `eventTimestamp` – O tempo de execução da consulta.
- `parameters.parametervalue` – Os valores dos parâmetros (aparecem dependendo do texto da consulta).
- `queryText` – A definição SQL da execução da consulta. Se houver parâmetros, eles serão rotulados como `:parametervalue`.
- `queryValidationErrors` – Os erros de consulta na validação da consulta.
- `schemaName` – O nome da associação de tabela configurada referenciada na consulta.

Recebimento de logs de consultas

Você não precisa realizar nenhuma ação fora do AWS Clean Rooms para configurar os registros de consulta. AWS Clean Rooms cria grupos de registros para colaborações depois que cada membro da colaboração cria uma associação.

Membros que podem consultar, membros que podem receber resultados e membros cujas tabelas de configuração são referenciadas na consulta receberão um registro de consultas.

O membro que pode consultar e o membro que pode receber os resultados receberão registros de consulta para cada tabela configurada referenciada na consulta. Se eles não forem proprietários da tabela configurada, não poderão visualizar o ID da tabela configurada (`configuredTableID`).

Se um membro tiver várias associações de tabela configuradas referenciadas na consulta, ele receberá um log de consulta para cada tabela configurada.

Os registros são criados para consultas que contêm SQL incompatível e compatível no AWS Clean Rooms. Para obter mais detalhes, consulte a Referência SQL do AWS Clean Rooms.

Os logs também são criados quando as consultas fazem referência a tabelas configuradas que não estão associadas à colaboração.

Os registros não são criados para SQL incorreto em AWS Clean Rooms.

Os logs de consulta não indicam que uma consulta foi bem-sucedida e que a saída da consulta foi entregue. Eles confirmam que uma consulta foi enviada pelo membro que pode consultar. Os registros de consulta também confirmam que a consulta contém SQL compatível AWS Clean Rooms e faz referência às tabelas configuradas associadas à colaboração.

Example

Por exemplo, um registro não será produzido se a consulta for cancelada após a AWS Clean Rooms validação de sua conformidade com as regras de análise e durante o processamento da consulta.

Se você excluir o grupo de logs, deverá recriar o grupo de logs manualmente com o mesmo nome do grupo de logs (ID de colaboração da colaboração). Ou você pode desativar e ativar o log em sua assinatura.

Para obter mais informações sobre como ativar consultas em log, consulte Criando uma colaboração em AWS Clean Rooms.

Para obter mais informações sobre o Amazon CloudWatch Logs, consulte o Guia do usuário do Amazon CloudWatch Logs.

Usar o registro de consultas

Recomendamos que os membros tomem as seguintes precauções periodicamente:

- Para verificar se as consultas correspondem aos casos de uso ou às consultas que foram acordadas para a colaboração, revise as consultas que são executadas na colaboração.

  Para obter mais informações sobre como visualizar consultas recentes, consulte Visualização de consultas recentes.
- Para verificar se as colunas da tabela configurada correspondem ao que foi acordado para a colaboração, revise as colunas da tabela configurada que são usadas nas regras de análise dos membros da colaboração e nas consultas.

  Para obter mais informações sobre como visualizar as colunas configuradas, consulte Visualização de tabelas e regras de análise.

Conf AWS Clean Rooms iguração

Os tópicos a seguir explicam como configurar AWS Clean Rooms.

Tópicos

Inscreva-se para AWS

Antes de usar qualquer um AWS service (Serviço da AWS), inclusive AWS Clean Rooms, você deve se inscrever no AWS.

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.
3. Quando você se inscreve em um Conta da AWS, um usuário Conta da AWS root é criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário raiz para realizar as tarefas que exigem acesso do usuário raiz.

Configurar funções de serviço para AWS Clean Rooms

Tópicos

Criação de um usuário administrador

Para usar AWS Clean Rooms, você precisa criar um usuário administrador para si mesmo e adicionar o usuário administrador a um grupo de administradores.

Para criar um usuário administrador, selecione uma das opções a seguir.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
Centro de Identidade do IAM (Recomendado)	Use credenciais de curto prazo para acessar a AWS. Isso está de acordo com as práticas recomendadas de segurança. Para obter informações sobre as práticas recomendadas, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.	Seguindo as instruções em Conceitos básicos no Guia do usuário do AWS IAM Identity Center .	Configure o acesso programático configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário.
No IAM (Não recomendado)	Use credenciais de curto prazo para acessar a AWS.	Seguindo as instruções em Criar o seu primeiro usuário administrador e um grupo de usuários do IAM no Guia do usuário do IAM.	Para configurar o acesso programático, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM.

Criar um perfil do IAM para um membro da colaboração

Um membro é um AWS cliente que participa de uma colaboração.

Para criar um perfil do IAM para um membro da colaboração

1. Siga o procedimento Criação de uma função para delegar permissões a um usuário do IAM no Guia do AWS Identity and Access Management usuário.
2. Para a etapa Criar política, selecione a guia JSON no editor de políticas e adicione políticas de acordo com as habilidades concedidas ao membro da colaboração.

   AWS Clean Rooms oferece as seguintes políticas gerenciadas com base em casos de uso comuns:

Se você deseja ...	Em seguida, use ...
Veja os recursos e os meta-dados	AWS política gerenciada: `AWSCleanRoomsReadOnlyAccess`
Consulta	AWS política gerenciada: `AWSCleanRoomsFullAccess`
Consulte e receba resultados	AWS política gerenciada: `AWSCleanRoomsFullAccess`
Gerencie recursos de colaboração, mas não faça consultas	AWS política gerenciada: `AWSCleanRoomsFullAccessNoQuerying`

   Para obter informações sobre as diferentes políticas gerenciadas oferecidas pela AWS Clean Rooms, consulte AWS políticas gerenciadas para AWS Clean Rooms

Criar um perfil de serviço para ler dados

AWS Clean Rooms usa uma função de serviço para ler os dados.

Há duas maneiras de criar essa função de serviço:

Se...	Então
Você tem as permissões do IAM necessárias para criar uma função de serviço	Use o AWS Clean Rooms console para criar uma função de serviço.
Você não tem `iam:CreateRole` , `iam:CreatePolicy` nem `iam:AttachRolePolicy` permissões ou Você quer criar as funções do IAM manualmente	Execute um destes procedimentos: • Use o procedimento a seguir para criar uma função de serviço. • Peça ao administrador que crie a função de serviço usando o procedimento a seguir.

Para criar um perfil de serviço para ler dados

> **Note**
>
> Você ou seu administrador do IAM só devem seguir esse procedimento se não tiverem as permissões necessárias para criar uma função de serviço usando o AWS Clean Rooms console.

1. Siga o procedimento Criar uma função usando políticas de confiança personalizadas (console) no Guia do AWS Identity and Access Management usuário.
2. Use a seguinte política de confiança personalizada de acordo com o procedimento Criar uma função usando políticas de confiança personalizadas (console).

   > **Note**
   >
   > Se quiser garantir que o perfil só possa ser usado no contexto de uma determinada associação de colaboração, você pode detalhar ainda mais a política de confiança. Para ter mais informações, consulte Prevenção do problema do substituto confuso entre serviços.

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

3. Use a política de permissões a seguir de acordo com o procedimento Criar uma função usando políticas de confiança personalizadas (console).

> **Note**
>
> O exemplo de política a seguir suporta as permissões necessárias para ler AWS Glue meta-dados e seus dados correspondentes do Amazon S3. No entanto, talvez seja necessário modificar essa política dependendo de como você configurou seus dados do S3. Por exemplo, se você configurou uma chave KMS personalizada para seus dados do S3, talvez seja necessário alterar essa política com permissões adicionais. AWS KMS Seus AWS Glue recursos e os recursos subjacentes do Amazon S3 devem estar no mesmo nível da Região da AWS colaboração. AWS Clean Rooms

```
{
    "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. Substitua cada *espaço reservado* por suas próprias informações.
5. Continue seguindo o procedimento Criando uma função usando políticas de confiança personalizadas (console) para criar a função.

Crie uma função de serviço para receber resultados

> **Note**
>
> Se você for o membro que só pode receber resultados (no console, Suas habilidades de membro são Somente Receber resultados), siga este procedimento.
> Se você for um membro que pode consultar e receber resultados (no console, suas habilidades de membro são Consultar e Receber resultados), você pode pular esse procedimento.

Para membros da colaboração que só podem receber resultados, AWS Clean Rooms usa uma função de serviço para gravar os resultados dos dados consultados na colaboração no bucket do Amazon S3 especificado.

Há duas maneiras de criar essa função de serviço:

Se...	Então
Você tem as permissões do IAM necessárias para criar uma função de serviço	Use o AWS Clean Rooms console para criar uma função de serviço.
Você não tem `iam:CreateRole` , `iam:CreatePolicy` nem `iam:AttachRolePolicy` permissões ou Você quer criar as funções do IAM manualmente	Execute um destes procedimentos: • Use o procedimento a seguir para criar uma função de serviço. • Peça ao administrador que crie a função de serviço usando o procedimento a seguir.

Para criar uma função de serviço para receber resultados

> **Note**
>
> Você ou seu administrador do IAM só devem seguir esse procedimento se não tiverem as permissões necessárias para criar uma função de serviço usando o AWS Clean Rooms console.

1. Siga o procedimento Criar uma função usando políticas de confiança personalizadas (console) no Guia do AWS Identity and Access Management usuário.
2. Use a seguinte política de confiança personalizada de acordo com o procedimento Criar uma função usando políticas de confiança personalizadas (console).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowIfExternalIdMatches",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "sts:ExternalId":
 "arn:aws:*:region:*:dbuser:*/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa*"
                }
            }
        },
        {
            "Sid": "AllowIfSourceArnMatches",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ForAnyValue:ArnEquals": {
                    "aws:SourceArn": [
                        "arn:aws:cleanrooms:us-east-1:555555555555:membership/
a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
                    ]

                }
            }
        }
    ]
}
```

3. Use a política de permissões a seguir de acordo com o procedimento Criar uma função usando políticas de confiança personalizadas (console).

> **Note**
>
> O exemplo de política a seguir suporta as permissões necessárias para ler AWS Glue meta-dados e seus dados correspondentes do Amazon S3. No entanto, talvez seja necessário modificar essa política dependendo de como você configurou seus dados do S3.
>
> Seus AWS Glue recursos e os recursos subjacentes do Amazon S3 devem estar no mesmo nível da Região da AWS colaboração. AWS Clean Rooms

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

4. Substitua cada *espaço reservado* por suas próprias informações:

   - *região* – O nome da Região da AWS. Por exemplo, **us-east-1**.
   - *a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa* – A ID de associação do membro que pode consultar. A ID de membro pode ser encontrada na guia Detalhes da colaboração. Isso

garante que AWS Clean Rooms esteja assumindo a função somente quando esse membro executa a análise nessa colaboração.

- *arn:aws:cleanrooms:us-east- 1:555555555555:membership/a1b2c3d4-5678-90ab-cdef-exampleAAAAA* – O único ARN de associação do membro que pode consultar. O ARN da associação pode ser encontrado na guia Detalhes da colaboração. Isso garante AWS Clean Rooms que ele assuma a função somente quando esse membro executa a análise nessa colaboração.
- *bucket_name* – O nome do recurso da Amazon (ARN) do bucket S3. O nome do recurso da Amazon (ARN) pode ser encontrado na guia Propriedades do bucket no Amazon S3.
- *accountId* — Conta da AWS O ID no qual o bucket do S3 está localizado.

  bucket_name/optional_key_prefix — O nome do recurso da Amazon (ARN) do destino dos resultados no S3. O nome do recurso da Amazon (ARN) pode ser encontrado na guia Propriedades do bucket no Amazon S3.

5. Continue seguindo o procedimento Criando uma função usando políticas de confiança personalizadas (console) para criar a função.

Configurar funções de serviço para AWS Clean Rooms ML

Tópicos

- Criar um perfil de serviço para ler dados de treinamento
- Criar um perfil de serviço para escrever um segmento de semelhanças
- Criar um perfil de serviço para ler dados de seed

Criar um perfil de serviço para ler dados de treinamento

AWS Clean Rooms usa uma função de serviço para ler dados de treinamento. Você pode criar esse perfil usando o console se você tiver as permissões necessárias do IAM. Se você não tiver `CreateRole` permissões, peça ao administrador que crie a função de serviço.

Para criar um perfil de serviço para treinar um conjunto de dados

1. Faça login no console do IAM em (https://console.aws.amazon.com/iam/) com sua conta de administrador.
2. Em Access management (Gerenciamento de acesso), escolha Policies (Políticas).

3. Escolha Create policy (Criar política).
4. No Editor de políticas, selecione a guia JSON e copie e cole a política a seguir.

> **Note**
>
> O exemplo de política a seguir suporta as permissões necessárias para ler AWS Glue meta-dados e seus dados correspondentes do Amazon S3. No entanto, talvez seja necessário modificar essa política dependendo de como você configurou seus dados do S3. Essa política não inclui uma chave KMS para descriptografar dados.
> Seus AWS Glue recursos e os recursos subjacentes do Amazon S3 devem estar no mesmo nível da Região da AWS colaboração. AWS Clean Rooms

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

```
                "arn:aws:glue:region:accountId:database/default"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::bucket"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "accountId"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucketFolders/*"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "accountId"
                    ]
                }
            }
        }
    ]
}
```

Se você precisar usar uma chave KMS para descriptografar dados, adicione esta AWS KMS instrução ao modelo anterior:

```
{
```

```
            "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. Escolha Próximo.
6. Em Analisar e criar, insira um Nome da política e uma Descrição e analise o Resumo.
7. Escolha Criar política.

   Você criou uma política para AWS Clean Rooms.
8. Em Gerenciamento de acesso, escolha Perfis.

   Com Perfis, é possível criar credenciais de curto prazo, o que é recomendado para aumentar a segurança. Você também pode escolher Usuários para criar credenciais de longo prazo.
9. Selecione Criar perfil.
10. No assistente Criar perfil, para Tipo de entidade confiável, escolha Política de confiança personalizada.
11. Copie e cole a seguinte política de confiança personalizada no editor 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/*"
                }
            }
        }
    ]
}
```

A AWS conta `SourceAccount` é sempre sua. O `SourceArn` pode ser limitado a um conjunto de dados de treinamento específico, mas somente após a criação desse conjunto de dados. Como você não pode conhecer com antecedência o ARN do conjunto de dados de treinamento, o caractere curinga é especificado aqui.

12. Escolha Próximo e, em Adicionar permissões, insira o nome da política que você acabou de criar. (Você pode precisar recarregar a página.)
13. Marque a caixa de seleção ao lado do nome da política que você criou e escolha Próximo.
14. Para Nome, revisar e criar, insira um nome de perfil e uma descrição.

> **Note**
>
> O nome do perfil deve corresponder ao padrão nas `passRole` permissões concedidas ao membro que pode consultar e receber resultados e funções do membro.

    a. Revise Selecionar entidades confiáveis e edite, se necessário.
    b. Revise as permissões em Adicionar permissões e edite, se necessário.
    c. Revise as tags e adicione tags, se necessário.
    d. Selecione Criar perfil.
15. A função de serviço para AWS Clean Rooms foi criada.

Criar um perfil de serviço para escrever um segmento de semelhanças

AWS Clean Rooms usa uma função de serviço para gravar segmentos semelhantes em um bucket. Você pode criar esse perfil usando o console se você tiver as permissões necessárias do IAM. Se você não tiver `CreateRole` permissões, peça ao administrador que crie a função de serviço.

Para criar um perfil de serviço para escrever um segmento de semelhanças

1. Faça login no console do IAM em (https://console.aws.amazon.com/iam/) com sua conta de administrador.
2. Em Access management (Gerenciamento de acesso), escolha Policies (Políticas).
3. Escolha Create policy (Criar política).
4. No Editor de políticas, selecione a guia JSON e copie e cole a política a seguir.

> **Note**
>
> O exemplo de política a seguir suporta as permissões necessárias para ler AWS Glue meta-dados e seus dados correspondentes do Amazon S3. No entanto, talvez seja necessário modificar essa política dependendo de como você configurou seus dados do S3. Essa política não inclui uma chave KMS para descriptografar dados.
> Seus AWS Glue recursos e os recursos subjacentes do Amazon S3 devem estar no mesmo nível da Região da AWS colaboração. AWS Clean Rooms

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

Se você precisar usar uma chave KMS para criptografar dados, adicione esta AWS KMS declaração ao modelo:

```
{
            "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*"
                }
            }
```

```
        }
  ]
}
```

Se você precisar usar uma chave KMS para descriptografar dados, adicione esta AWS KMS instrução ao modelo:

```
{
            "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. Escolha Próximo.
6. Em Analisar e criar, insira um Nome da política e uma Descrição e analise o Resumo.
7. Escolha Criar política.

   Você criou uma política para AWS Clean Rooms.
8. Em Gerenciamento de acesso, escolha Perfis.

   Com Perfis, é possível criar credenciais de curto prazo, o que é recomendado para aumentar a segurança. Você também pode escolher Usuários para criar credenciais de longo prazo.
9. Selecione Criar perfil.
10. No assistente Criar perfil, para Tipo de entidade confiável, escolha Política de confiança personalizada.
11. Copie e cole a seguinte política de confiança personalizada no editor 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/*"
                }
            }
        }
    ]
}
```

A AWS conta `SourceAccount` é sempre sua. O `SourceArn` pode ser limitado a um conjunto de dados de treinamento específico, mas somente após a criação desse conjunto de dados. Como você não pode conhecer com antecedência o ARN do conjunto de dados de treinamento, o caractere curinga é especificado aqui.

12. Escolha Próximo.
13. Marque a caixa de seleção ao lado do nome da política que você criou e escolha Próximo.
14. Para Nome, revisar e criar, insira um nome de perfil e uma descrição.

> **Note**
>
> O nome do perfil deve corresponder ao padrão nas `passRole` permissões concedidas ao membro que pode consultar e receber resultados e funções do membro.

a. Revise Selecionar entidades confiáveis e edite, se necessário.

b. Revise as permissões em Adicionar permissões e edite, se necessário.

c. Revise as tags e adicione tags, se necessário.

d. Selecione Criar perfil.

15. A função de serviço para AWS Clean Rooms foi criada.

Criar um perfil de serviço para ler dados de seed

AWS Clean Rooms usa uma função de serviço para ler dados iniciais. Você pode criar esse perfil usando o console se você tiver as permissões necessárias do IAM. Se você não tiver `CreateRole` permissões, peça ao administrador que crie a função de serviço.

Para criar um perfil de serviço para ler dados de seed

1. Faça login no console do IAM em (https://console.aws.amazon.com/iam/) com sua conta de administrador.
2. Em Access management (Gerenciamento de acesso), escolha Policies (Políticas).
3. Escolha Create policy (Criar política).
4. No Editor de políticas, selecione a guia JSON e copie e cole a política a seguir.

> **Note**
>
> O exemplo de política a seguir suporta as permissões necessárias para ler AWS Glue meta-dados e seus dados correspondentes do Amazon S3. No entanto, talvez seja necessário modificar essa política dependendo de como você configurou seus dados do S3. Essa política não inclui uma chave KMS para descriptografar dados.
> Seus AWS Glue recursos e os recursos subjacentes do Amazon S3 devem estar no mesmo nível da Região da AWS colaboração. AWS Clean Rooms

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

Se você precisar usar uma chave KMS para descriptografar dados, adicione esta AWS KMS instrução ao modelo:

```
{
            "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. Escolha Próximo.
6. Em Analisar e criar, insira um Nome da política e uma Descrição e analise o Resumo.
7. Escolha Criar política.

   Você criou uma política para AWS Clean Rooms.
8. Em Gerenciamento de acesso, escolha Perfis.

   Com Perfis, é possível criar credenciais de curto prazo, o que é recomendado para aumentar a segurança. Você também pode escolher Usuários para criar credenciais de longo prazo.
9. Selecione Criar perfil.
10. No assistente Criar perfil, para Tipo de entidade confiável, escolha Política de confiança personalizada.
11. Copie e cole a seguinte política de confiança personalizada no editor 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/*"
```

```
                }
            }
        }
    ]
}
```

A AWS conta `SourceAccount` é sempre sua. O `SourceArn` pode ser limitado a um conjunto de dados de treinamento específico, mas somente após a criação desse conjunto de dados. Como você não pode conhecer com antecedência o ARN do conjunto de dados de treinamento, o caractere curinga é especificado aqui.

12. Escolha Próximo.
13. Marque a caixa de seleção ao lado do nome da política que você criou e escolha Próximo.
14. Para Nome, revisar e criar, insira um nome de perfil e uma descrição.

> **Note**
>
> O nome do perfil deve corresponder ao padrão nas `passRole` permissões concedidas ao membro que pode consultar e receber resultados e funções do membro.

    a. Revise Selecionar entidades confiáveis e edite, se necessário.
    b. Revise as permissões em Adicionar permissões e edite, se necessário.
    c. Revise as tags e adicione tags, se necessário.
    d. Selecione Criar perfil.
15. A função de serviço para AWS Clean Rooms foi criada.

Criando uma colaboração em AWS Clean Rooms

Uma colaboração é um limite lógico seguro AWS Clean Rooms no qual os membros podem realizar consultas SQL em tabelas configuradas.

Qualquer membro AWS Clean Rooms pode criar uma colaboração.

O criador da colaboração pode designar um único membro para consultar e receber resultados. No entanto, o criador da colaboração pode querer impedir que o membro que pode consultar tenha acesso aos resultados da consulta. Nesse caso, o criador da colaboração pode designar um membro para quem pode consultar e outro membro que pode receber os resultados.

Na maioria dos casos, o membro que pode consultar também é o membro que paga pelos custos de computação da consulta. No entanto, o criador da colaboração pode configurar um membro diferente para ser responsável pelo pagamento dos custos de computação da consulta.

Para obter informações sobre como criar uma colaboração usando os SDKs AWS, consulte a Referência da API AWS Clean Rooms.

Tópicos

Crie uma colaboração

Antes de começar, certifique-se de ter cumprido os seguintes pré-requisitos:

- Você tem o nome e o ID Conta da AWS de cada membro que deseja convidar para a colaboração.
- Você tem permissão para compartilhar o nome e o ID Conta da AWS de cada membro com todos os membros da colaboração.

> **Note**
>
> Você não pode adicionar mais membros após a criação da colaboração.

Para criar uma colaboração usando o console AWS Clean Rooms

1. Faça login no AWS Management Console e abra o console AWS Clean Rooms com o Conta da AWS que funcionará como criador da colaboração.
2. No painel de navegação à esquerda, selecione Colaborações.
3. No canto superior direito, selecione Criar colaboração.
4. Em Etapa 1: definir a colaboração, faça o seguinte:

    a. Em Detalhes, insira o Nome e a Descrição da colaboração.

    Essas informações ficarão visíveis para os membros da colaboração que forem convidados a participar da colaboração. O Nome e a Descrição os ajudam a entender a que se refere a colaboração.

    b. Para Membros:

        i. Para Membro 1: Você, insira o Nome de exibição do Membro conforme você deseja que ele apareça para a colaboração.

        > **Note**
        >
        > Seu ID Conta da AWS é incluído automaticamente como ID de membro Conta da AWS.

        ii. Para Membro 2, insira o Nome de exibição do membro e o ID do membro Conta da AWS que você deseja convidar para a colaboração.

        O Nome de exibição do membro e o ID do membro Conta da AWS estarão visíveis para todos os convidados para a colaboração. Depois de inserir e salvar os valores desses campos, eles não são editáveis.

        > **Note**
        >
        > Você deve informar ao membro da colaboração que seu ID de membro Conta da AWS e Nome de exibição do membro estarão visíveis para todos os colaboradores convidados e ativos na colaboração.

iii. Se você quiser adicionar outro membro, escolha Adicionar outro membro. Em seguida, insira o nome de exibição do membro e o ID do membro Conta da AWS para cada membro que pode contribuir com dados que você deseja convidar para a colaboração.

c. Para Habilidades de membro, escolha uma das seguintes opções,

Se você deseja...	Então…
Consulte os dados na colaboração e receba os resultados	1. Escolha você mesmo como o membro que pode Executar consultas. 2. Deixe que a configuração padrão do membro que pode Receber resultados seja a Mesma de quem executa consultas.
Consulte os dados na colaboração e designe um membro diferente para receber os resultados	1. Escolha você mesmo como o membro que pode Executar consultas. 2. Selecione o membro que pode Receber resultados na lista suspensa.
Receba os resultados da consulta na colaboração e designe um membro diferente para consultar os dados	1. Selecione o membro que pode Executar consultas na lista suspensa. 2. Escolha você mesmo como membro que pode Receber resultados da lista suspensa.
Crie e gerencie a colaboração, designe um membro diferente para consultar os dados e atribua um membro diferente para receber os resultados	1. Selecione o membro que pode Executar consultas na lista suspensa. 2. Selecione o membro que pode Receber resultados na lista suspensa.

d. Para Configuração de pagamento, escolha uma das seguintes opções:

Se você deseja...	Então…
Designe o membro que pode Executar consultas para ser o membro que paga pelos custos de computação da consulta	Deixe que a configuração padrão do membro que Pagará pelas consultas seja a Mesma de quem executa as consultas.
Atribua um membro diferente para pagar pelos custos de computação da consulta	Selecione o membro que Pagará pelas consultas na lista suspensa.

e. Se você quiser habilitar o Log de consultas, marque a caixa de seleção Suporte ao log de consultas para esta colaboração.

f. Se você quiser habilitar o recurso de Computação criptográfica, marque a caixa de seleção Suporte à computação criptográfica nesta colaboração e escolha os seguintes parâmetros de computação criptográfica:

- Permitir colunas cleartext

  Escolha Não se você não quiser que as colunas cleartext sejam permitidas na tabela criptografada.

  Escolha Sim se quiser que as colunas cleartext sejam permitidas na tabela criptografada.

  Para executar SUM ou AVG em determinadas colunas, as colunas devem estar dentro de cleartext.

- Permitir duplicatas

  Escolha Não se você não quiser que entradas duplicadas sejam permitidas em uma coluna fingerprint.

  Escolha Sim se quiser que entradas duplicadas sejam permitidas em uma coluna fingerprint.

- Permitir colunas JOIN com nomes diferentes

  Escolha Não se você não quiser unir colunas fingerprint com nomes diferentes.

  Escolha Sim se quiser unir colunas fingerprint com nomes diferentes.

- Preserve valores NULL

  Escolha Não se você não quiser preservar os valores NULL. Os valores NULL não aparecerão como NULL em uma tabela criptografada.

  Escolha Sim se quiser preservar os valores NULL. Os valores NULL aparecerão como NULL em uma tabela criptografada.

Para obter mais informações sobre Parâmetros de computação criptográfica, consulte Parâmetros de computação criptográfica.

Para obter mais informações sobre como criptografar seus dados para uso em AWS Clean Rooms, consulte Preparando tabelas de dados criptografadas com computação criptográfica para Clean Rooms.

> **Note**
>
> Verifique essas configurações cuidadosamente antes de concluir a próxima etapa. Depois de criar a colaboração, você só pode editar o nome da colaboração, a descrição e se os logs de consulta estão armazenados no Amazon CloudWatch Logs.

g. Se você quiser habilitar Tags para o recurso de colaboração, escolha Adicionar nova tag e, em seguida, insira o par Chave e Valor.

h. Escolha Next (Próximo).

5. Para a Etapa 2: Configurar associação, faça o seguinte:

   a. Selecione uma opção:

Se você escolher...	Então…
Sim, cadastrar-se criando uma associação agora	Tanto a colaboração quanto sua associação são criadas. Seu status na colaboração está ativo.
Não, vou criar uma associação mais tarde	Somente a colaboração é criada.

Se você escolher...	Então…
	Seu status na colaboração é inativo.

b. Se você for o membro que pode Receber resultados, em Padrões de configurações de resultados da consulta, escolha uma opção:

Se você…	Então…
Mantenha a caixa de seleção Definir configurações padrão agora marcada. (Isso é selecionado por padrão.)	1. Para o Destino dos resultados no Amazon S3, insira o destino do Amazon S3. 2. Para o Formato do resultado da consulta, escolha CSV ou PARQUET.
Desmarque a caixa de seleção Definir configurações padrão agora	Somente a colaboração é criada. Seu status na colaboração é inativo.

c. Se você optar por habilitar o Log de consultas na etapa 4.e, escolha uma das seguintes opções para armazenamento de logs no Amazon CloudWatch Logs:

Se você escolher...	Então…
Ativar	Os registros de consulta relevantes para você são armazenados no Amazon CloudWatch Logs. Cada membro pode receber somente logs de consultas iniciadas por ele ou que contenham seus dados. O membro que pode receber os resultados também recebe logs de todas as consultas executadas em uma colaboração, mesmo que seus dados não sejam acessados em uma consulta.

Se você escolher...	Então…
Desativar	Os logs de consulta relevantes para você não são armazenados na sua conta do Amazon CloudWatch Logs.

> **Note**
>
> Depois de ativar o logs de consultas, pode levar alguns minutos para que o armazenamento de registros seja configurado e comece a receber logs no Amazon CloudWatch Logs. Durante esse breve período, o membro que pode consultar pode executar consultas que, na verdade, não enviam logs.

d. Se você quiser habilitar Tags para o recurso de associação, escolha Adicionar nova tag e insira o par Chave e Valor.

e. Se você for o membro que está Pagando pelas consultas, indique sua aceitação marcando a caixa de seleção Eu concordo em pagar pelos custos de computação da consulta nesta colaboração.

> **Note**
>
> Você deve marcar essa caixa de seleção para continuar.
> Para obter mais informações sobre como o preço é calculado, consulte Preços para AWS Clean Rooms.

Se você for o Membro que paga pelos custos de computação da consulta, mas não o Membro que pode consultar, é recomendável usar AWS Budgets para configurar um orçamento para AWS Clean Rooms e receber notificações quando o orçamento máximo for atingido. Para obter mais informações sobre como configurar um orçamento, consulte Gerenciando seus custos comAWS Budgets no Guia do Usuário AWS Cost Management. Para obter mais informações sobre a configuração de notificações, consulte o tópico Criação de um Amazon SNS para notificações de orçamento no Guia do usuário AWS Cost Management. Se o orçamento máximo tiver sido atingido, você pode entrar em contato com o membro que pode fazer consultas ou sair da colaboração. Se você deixar a colaboração,

não será mais permitida a execução de consultas e, portanto, você não será mais cobrado pelos custos de computação da consulta.

f. Escolha Next (Próximo).

6. Para a Etapa 3: revisar e criar, faça o seguinte:

a. Revise as seleções feitas nas etapas anteriores e edite, se necessário.

b. Escolha uma das seguintes opções:

Se você escolheu...	A seguir, escolha…
Crie uma associação com a colaboração (Sim, cadastrar-se criando uma associaçã o agora)	Criar colaboração e associação
Criar a colaboração e não criar uma associação no momento (Não, criarei uma associação mais tarde)	Criar colaboração

Depois que sua colaboração for criada com sucesso, você poderá ver a página de detalhes da colaboração em Colaborações.

Próximas etapas

Agora está tudo pronto para:

- Prepare sua tabela de dados para ser consultada AWS Clean Rooms. (Opcional se você quiser consultar seus próprios dados.)
- Associar a tabela configurada à sua colaboração. (Opcional se você quiser consultar seus próprios dados.)
- Configurar uma regra de análise para a tabela configurada. (Opcional se você quiser consultar seus próprios dados.)
- Crie uma associação e participe de uma colaboração.
- Gerenciar sua colaboração.

Criar uma associação e participando de uma colaboração

Uma associação é um recurso criado quando um membro se junta a uma colaboração no AWS Clean Rooms.

Você pode participar de uma colaboração como membro que pode consultar dados, membro que pode receber resultados de uma consulta ou ambos. Você também pode participar de uma colaboração como membro pagando pelos custos de computação da consulta. Todos os membros podem contribuir com dados.

Para obter informações sobre como criar uma associação e participar de uma colaboração usando os SDKs da AWS , consulte a Referência da API do AWS Clean Rooms.

Tópicos

Crie uma associação e participe de uma colaboração

Para criar uma associação e participar de uma colaboração

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu membro Conta da AWS.
2. No painel de navegação à esquerda, selecione Colaborações.
3. Na guia Disponível para participar, em Colaborações disponíveis para participar, escolha o Nome da colaboração.
4. Na página de detalhes da colaboração, visualize os detalhes da colaboração, incluindo os detalhes do seu membro e uma lista dos outros membros.

   Verifique se os Conta da AWS IDs de cada membro da colaboração são aqueles com os quais você pretende entrar na colaboração.
5. Escolha Criar associação.
6. Na página Criar associação, na Visão geral, visualize o nome da colaboração, a descrição da colaboração, o Conta da AWS ID do criador da colaboração, suas habilidades de membro e o Conta da AWS ID do membro que pagará pelas consultas.

7. Se o criador da colaboração tiver optado por ativar o registro de consultas, escolha uma das seguintes opções para armazenamento de registros no Amazon CloudWatch Logs:

Se você escolher...	Então…
Ativar	Os registros de consulta relevantes para você são armazenados no Amazon CloudWatch Logs. Cada membro pode receber somente logs de consultas iniciadas por ele ou que contenham seus dados. O membro que pode receber os resultados também recebe registros de todas as consultas executadas em uma colaboração, mesmo que seus dados não sejam acessados em uma consulta.
Desativar	Os registros de consulta relevantes para você não são armazenados na sua conta Amazon CloudWatch Logs.

> **Note**
>
> Depois de ativar o registro de consultas, pode levar alguns minutos para que o armazenamento de registros seja configurado e comece a receber registros no Amazon CloudWatch Logs. Durante esse breve período, o membro que pode consultar pode executar consultas que, na verdade, não enviam logs.

8. Se Suas habilidades de membro incluírem Receber resultados:

   a. Para Configurações de resultados de consulta,

      i. Especifique o Destino dos resultados no Amazon S3 inserindo o destino do S3 ou escolha Procurar no S3 para selecionar em uma lista de buckets do S3 disponíveis.

Example

Por exemplo: **`s3://bucket/prefix`**

ii. Escolha o Formato do resultado (CSV ou PARQUET).

b. Para Acesso ao serviço, escolha Criar e usar um novo perfil de serviço ou Usar uma função de serviço existente.

> **Note**
>
> Você deve selecionar uma função de serviço existente ou ter permissões para criar uma nova. Para ter mais informações, consulte Crie uma função de serviço para receber resultados.

9. Se quiser habilitar Tags para o recurso de associação, escolha Adicionar nova tag e, em seguida, insira o par Chave e Valor.

10. Se o criador da colaboração designou você como o membro que Pagará pelas consultas, indique sua aceitação marcando a caixa de seleção Eu concordo em pagar pelos custos de computação da consulta nesta colaboração.

> **Note**
>
> Você deve marcar essa caixa de seleção para continuar.
> Para obter mais informações sobre como o preço é calculado, consulte Preços para AWS Clean Rooms.

Se você for o membro que paga pelos custos de computação da consulta, mas não o membro que pode consultar, é recomendável usar AWS Budgets para configurar um orçamento AWS Clean Rooms e receber notificações quando o orçamento máximo for atingido. Para obter mais informações sobre como configurar um orçamento, consulte Gerenciando seus custos com AWS Budgets no Guia do Usuário do AWS Cost Management . Para obter mais informações sobre a configuração de notificações, consulte o tópico Criação de um Amazon SNS para notificações de orçamento no Guia do usuário do AWS Cost Management . Se o orçamento máximo tiver sido atingido, você pode entrar em contato com o membro que pode fazer consultas ou sair da colaboração. Se você deixar a colaboração, não será mais permitida a execução de consultas e, portanto, você não será mais cobrado pelos custos de computação da consulta.

11. Se tiver certeza de que deseja criar uma associação e participar da colaboração, escolha Criar associação.

Você tem acesso de leitura aos metadados da colaboração. Isso inclui informações como o nome de exibição e a descrição da colaboração, além de todos os nomes e IDs Conta da AWS de outros membros.

Para obter informações sobre como sair de uma colaboração, consulte Saindo de uma colaboração.

Próximas etapas

Agora está tudo pronto para:

- Prepare sua tabela de dados para ser consultada AWS Clean Rooms. (Opcional se quiser consultar seus próprios dados.)
- Associe a tabela configurada à sua colaboração.
- Configure uma regra de análise para a tabela configurada.

Preparando tabelas de dados para consultas no AWS Clean Rooms

> **Note**
>
> A preparação de tabelas de dados pode ocorrer antes ou depois de você se juntar a uma colaboração. Depois que uma tabela é preparada, você pode reutilizá-la em várias colaborações, desde que suas necessidades de privacidade para essa tabela sejam as mesmas.

Como membro da colaboração, você deve preparar suas tabelas de dados antes que elas possam ser consultadas AWS Clean Rooms pelo membro da colaboração que pode consultar.

Se seu caso de uso não exigir que você traga seus próprios dados, você pode pular esse procedimento.

Se suas tabelas de dados já estiverem catalogadas AWS Glue, vá para. Criar uma tabela configurada no AWS Clean Rooms

A preparação de suas tabelas de dados envolve as seguintes etapas:

- Etapa 1: Concluir os pré-requisitos
- Etapa 2: (Opcional) Preparar seus dados para computação criptográfica
- Etapa 3: Carregar seu backup no Amazon S3
- Etapa 4: criar uma AWS Glue tabela
- Próximas etapas

Para obter mais informações sobre os formatos de dados que podem ser usados para consultas, consulte Formatos de dados para AWS Clean Rooms.

Etapa 1: Concluir os pré-requisitos

Para preparar suas tabelas de dados para uso com AWS Clean Rooms, você deve preencher os seguintes pré-requisitos:

- Seus conjuntos de dados devem ser salvos como um dos formatos de dados compatíveis com o AWS Clean Rooms.
- Suas tabelas de dados devem ser catalogadas AWS Glue e usar os tipos de dados compatíveis para AWS Clean Rooms.
- Todas as suas tabelas de dados devem ser armazenadas no Amazon Simple Storage Service (Amazon S3) no Região da AWS mesmo local em que a colaboração foi criada.
- Eles AWS Glue Data Catalog devem estar na mesma região em que a colaboração foi criada.
- Eles AWS Glue Data Catalog devem ser iguais Conta da AWS aos membros.
- O bucket do Amazon S3 não pode ser registrado no. AWS Lake Formation
- O criador da colaboração configurou uma colaboração no AWS Clean Rooms. Para ter mais informações, consulte Criando uma colaboração em AWS Clean Rooms.
- O criador da colaboração enviou a ID da colaboração para você como participante da colaboração.

Etapa 2: (Opcional) Preparar seus dados para computação criptográfica

(Opcional) Se você estiver usando computação criptográfica e sua tabela de dados contiver informações confidenciais que você deseja criptografar, você deverá criptografar a tabela de dados usando o cliente de criptografia C3R.

Para preparar seus dados para a computação criptográfica, siga os procedimentos em Preparando tabelas de dados criptografadas com computação criptográfica para Clean Rooms.

Etapa 3: Carregar seu backup no Amazon S3

> **Note**
>
> Se você pretende usar tabelas de dados criptografadas na colaboração, você deve primeiro criptografar os dados para computação criptográfica antes de carregar sua tabela de dados para o Amazon S3. Para ter mais informações, consulte Preparando tabelas de dados criptografadas com computação criptográfica para Clean Rooms.

Para fazer upload de sua tabela de dados no Amazon S3

1. Faça login AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Escolha Buckets e escolha um bucket no qual deseja armazenar sua tabela de dados.
3. Escolha Upload e siga as instruções.
4. Escolha a guia Objetos para visualizar o prefixo do onde seus dados são armazenados. Anote o nome da pasta.

   É possível selecionar a pasta para visualizar os dados.

Etapa 4: criar uma AWS Glue tabela

Se você já tem uma tabela de AWS Glue dados, pode pular essa etapa.

Nesta etapa, você configura um rastreador AWS Glue que rastreia todos os arquivos em seu bucket do S3 e cria uma tabela. AWS Glue Para obter mais informações, consulte Definição de rastreadores AWS Glue no Guia do AWS Glue usuário.

Para obter mais informações sobre AWS Glue Data Catalog os tipos de dados compatíveis, consulteTipos de dados compatíveis.

> **Note**
>
> AWS Clean Rooms atualmente não oferece suporte a buckets S3 registrados com. AWS Lake Formation

O procedimento a seguir descreve como criar uma AWS Glue tabela. Se você quiser usar um AWS Glue Data Catalog objeto criptografado com uma chave AWS Key Management Service (AWS KMS), precisará configurar a política de permissões da chave KMS para permitir o acesso a essa tabela criptografada. Para obter mais informações, consulte Como configurar a criptografia no AWS Glue no Guia do desenvolvedor do AWS Glue .

Para criar uma AWS Glue tabela

1. Siga o procedimento Trabalhando com rastreadores no AWS Glue console no Guia do AWS Glue usuário.

2. Anote o nome do AWS Glue banco de dados e o nome AWS Glue da tabela.

Próximas etapas

Agora que você preparou suas tabelas de dados, você está pronto para:

- Crie uma tabela configurada
- Crie um modelo de ML

Formatos de dados para AWS Clean Rooms

Os conjuntos de dados que você usa para consultas geralmente AWS Clean Rooms são os mesmos tipos de conjuntos de dados que você usa para outros aplicativos. Por exemplo, os mesmos tipos de conjuntos de dados são usados com Amazon Athena, Amazon EMR, Amazon Redshift Spectrum e Amazon. QuickSight Você pode consultar os dados em seu formato original diretamente no Amazon Simple Storage Service (Amazon S3).

Para consultar dados, os conjuntos de dados devem estar em um formato AWS Clean Rooms compatível. O bucket do Amazon S3 com os conjuntos de dados e o AWS Clean Rooms cluster deve estar no mesmo. Região da AWS

Formatos de dados suportados

AWS Clean Rooms suporta os seguintes formatos estruturados:

- Tabelas Apache Iceberg
- Parquet
- RCFile
- TextFile
- SequenceFile
- RegexSerde
- OpenCSV
- AVRO
- JSON

> **Note**
>
> Um `timestamp` valor em um arquivo de texto deve estar no formato `yyyy-MM-dd HH:mm:ss.SSSSSS`. Por exemplo: `2017-05-01 11:30:59.000000`.

Recomendamos usar um formato de arquivo de armazenamento colunar, como Apache Parquet. Com um formato de arquivo colunar para o armazenamento, é possível minimizar a transferência de dados do Amazon S3 selecionando apenas as colunas necessárias. Para um desempenho ideal, objetos grandes devem ser divididos em objetos de 100 MB a 1 GB.

Tipos de dados compatíveis

Para uma experiência ideal com AWS Clean Rooms, todos os seus dados devem ser catalogados em AWS Glue. Para obter mais informações, consulte a seção intitulada Introdução ao AWS Glue Data Catalog no Guia do desenvolvedor do AWS Glue .

AWS Clean Rooms suporta os seguintes tipos de AWS Glue Data Catalog dados:

- bigint
- boolean
- char
- date
- decimal
- double
- float
- int
- Tipos de dados aninhados, como:
  - array
  - map
  - struct
- smallint
- string
- timestamp

- varchar

AWS Clean Rooms não suporta:

- binary
- interval

Tipos de compactação de arquivos para AWS Clean Rooms

Para reduzir o espaço de armazenamento, melhorar o desempenho e minimizar custos, recomendamos fortemente que você compacte seus conjuntos de dados.

AWS Clean Rooms reconhece os tipos de compactação de arquivos com base na extensão do arquivo e oferece suporte aos tipos e extensões de compactação mostrados na tabela a seguir.

Algoritmo de compactação	Extensão de arquivo
GZIP	.gz
Bzip2	.bz2
Snappy	.snappy

Você pode aplicar compactação em diferentes níveis. O mais comum é compactar um arquivo inteiro ou blocos individuais dentro de um arquivo. A compactação de formatos colunares no nível do arquivo não traz benefícios de desempenho.

Criptografia do lado do servidor para AWS Clean Rooms

> **Note**
>
> A criptografia do lado do servidor não substitui a computação criptográfica para os casos de uso que a exigem.

AWS Clean Rooms descriptografa de forma transparente conjuntos de dados que são criptografados usando as seguintes opções de criptografia:

- SSE-S3 – Criptografia do lado do servidor usando uma chave de criptografia AES-256 gerenciada pelo Amazon S3
- SSE-KMS — criptografia do lado do servidor com chaves gerenciadas por AWS Key Management Service

Para usar o SSE-S3, a função de AWS Clean Rooms serviço usada para associar a tabela configurada à colaboração deve ter permissões do KMS-Decrypt. Para usar o SSE-KMS, a política de chaves do KMS também deve permitir que a função de AWS Clean Rooms serviço seja descriptografada.

AWS Clean Rooms não oferece suporte à criptografia do lado do cliente do Amazon S3. Para obter mais informações sobre criptografia no lado do servidor, consulte Proteger dados usando criptografia no lado do servidor no Guia do usuário do Amazon Simple Storage Service.

Usando Apache Iceberg tabelas em AWS Clean Rooms

Apache Icebergé um formato de tabela de código aberto para data lakes. AWS Clean Rooms pode usar as estatísticas armazenadas nos Apache Iceberg metadados para otimizar os planos de consulta e reduzir as varreduras de arquivos durante o processamento de consultas em sala limpa. Para obter mais informações, consulte na documentação do Apache Iceberg.

Considere o seguinte ao usar AWS Clean Rooms com tabelas Iceberg:

- Tabelas dentro do AWS Glue Data Catalog único — Apache Iceberg as tabelas devem ser definidas no AWS Glue Data Catalog com base na implementação do catálogo de cola de código aberto.
- Formato de arquivo Parquet — AWS Clean Rooms só suporta tabelas Iceberg no formato de arquivo de dados Parquet.
- Compressão GZIP e Snappy — AWS Clean Rooms suporta Parquet com GZIP e compressão. Snappy
- Versões do Iceberg — AWS Clean Rooms suporta a execução de consultas nas tabelas Iceberg da versão 1 e da versão 2.
- Partições — Você não precisa adicionar partições manualmente às suas Apache Iceberg tabelas. AWS Glue AWS Clean Rooms detecta novas partições nas Apache Iceberg tabelas automaticamente e nenhuma operação manual é necessária para atualizar as partições na definição da tabela. As partições Iceberg aparecem como colunas regulares no esquema da tabela

AWS Clean Rooms e não separadamente como uma chave de partição no esquema da tabela configurada.

- Limitações
  - Somente novas tabelas Iceberg

    Apache Iceberg tabelas convertidas de tabelas Apache Parquet não são suportadas.
  - Consultas de viagem no tempo

    AWS Clean Rooms não suporta consultas de viagem no tempo com Apache Iceberg tabelas.
  - Mecanismo do Athena versão 2

    Iceberg tabelas criadas com a versão 2 do Athena Engine não são suportadas.
  - Formatos de arquivo

    Avro e os formatos de arquivo Optimized Row Columnar (ORC) não são suportados.
  - Compactação

    Zstandard A compactação (Zstd) para Parquet não é suportada.

Tipos de dados suportados para tabelas Iceberg no Athena

AWS Clean Rooms pode consultar Iceberg tabelas que contêm os seguintes tipos de dados:

- boolean
- date
- decimal
- double
- float
- int
- list
- long
- map
- string
- struct
- timestamp without time zone

Para obter mais informações sobre tipos de dados do Iceberg, consulte Esquemas para o Iceberg na documentação do Apache Iceberg.

Preparando tabelas de dados criptografadas com computação criptográfica para Clean Rooms

Computação criptográfica para Clean Rooms (C3R) é um recurso em. AWS Clean Rooms Você pode usar o C3R para limitar criptograficamente o que pode ser aprendido por qualquer parte e AWS em uma colaboração. AWS Clean Rooms

Você pode criptografar a tabela de dados usando o cliente de criptografia C3R, uma ferramenta de criptografia do lado do cliente, antes de fazer o upload da tabela de dados para o Amazon Simple Storage Service (Amazon S3).

Para ter mais informações, consulte Computação criptográfica para o Clean Rooms.

A preparação de tabelas de dados criptografadas com o C3R envolve as seguintes etapas:

Etapas

- Etapa 1: Concluir os pré-requisitos
- Etapa 2: Baixe o cliente de criptografia C3R
- (Opcional) Etapa 3: Exibir os comandos disponíveis no cliente de criptografia C3R
- Etapa 4: gerar um esquema de criptografia para um arquivo tabular
- Etapa 5: criar uma chave secreta compartilhada
- Etapa 6: armazenar a chave secreta compartilhada em uma variável de ambiente
- Etapa 7: criptografar dados
- Etapa 8: verificar a criptografia de dados
- (Opcional) Crie um esquema (usuários avançados)

Etapa 1: Concluir os pré-requisitos

Para preparar suas tabelas de dados para uso com o C3R, você deve preencher os seguintes pré-requisitos:

- Você pode acessar a Computação Criptográfica para o Clean Rooms repositório em: GitHub

  https://github.com/aws/c3r

- Você configurou AWS as credenciais para usar o cliente de criptografia C3R. Essas credenciais são usadas pelo cliente de criptografia C3R para chamadas de API somente para leitura para recuperar metadados de colaboração. AWS Clean Rooms Para obter mais informações, consulte Configurando o AWS CLI no Guia do AWS Command Line Interface Usuário para a versão 2.
- Você tem Java Runtime Environment (JRE) 11 ou posterior instalado em sua máquina.
  - O recomendadoJava Runtime Environment, Amazon Corretto 11 ou superior, pode ser baixado em https://aws.amazon.com/corretto.
  - O Java Development Kit (JDK) inclui um correspondente JRE da mesma versão. No entanto, os recursos adicionais do não JDK são necessários para executar o cliente de criptografia Cryptographic Computing for Clean Rooms (C3R).
- Seus arquivos de dados tabulares (.csv) ou Parquet arquivos (. parquet) são salvos localmente.
- Você ou outro membro da colaboração tem a capacidade de criar uma chave secreta compartilhada. Para ter mais informações, consulte Etapa 5: criar uma chave secreta compartilhada.
- O criador da colaboração criou uma colaboração AWS Clean Rooms com a computação criptográfica habilitada para a colaboração. Para ter mais informações, consulte Criando uma colaboração em AWS Clean Rooms.
- O criador da colaboração enviou a ID da colaboração para você como participante da colaboração. O Amazon Resource Name (ARN) da colaboração está incluído no convite enviado, que contém o ID da colaboração.

Etapa 2: Baixe o cliente de criptografia C3R

Para baixar o cliente de criptografia C3R de GitHub

1. Acesse o Clean RoomsAWSGitHub repositório de Computação Criptográfica: https://github.com/aws/c3r
2. Selecione e baixe os arquivos.

   O código-fonte, as licenças e o material relacionado podem ser clonados ou baixados como um. ziparquivo da página inicial do GitHub repositório. (Veja o botão Código no canto superior direito da lista de conteúdo do repositório).

   O cliente de criptografia C3R assinado mais recente Java Executable File (ou seja, o aplicativo de interface de linha de comando) está na página Releases do GitHub repositório.

O pacote do cliente de criptografia C3R para Apache Spark (`c3r-cli-spark`) é uma versão do c3r-cli que deve ser enviada como um trabalho para um servidor Apache Spark em execução. Para obter mais informações, consulte Executando o C3R no Apache Spark.

(Opcional) Etapa 3: Exibir os comandos disponíveis no cliente de criptografia C3R

Use esse procedimento para se familiarizar com os comandos disponíveis no cliente de criptografia C3R.

Para ver todos os comandos disponíveis no cliente de criptografia C3R

1. Em uma interface de linha de comando (CLI), navegue até a pasta que contém o arquivo baixadoc3r-cli.jar.
2. Execute o seguinte comando: `java -jar c3r-cli.jar`
3. Veja a lista de comandos e opções disponíveis.

Etapa 4: gerar um esquema de criptografia para um arquivo tabular

Para criptografar dados, é necessário um esquema de criptografia descrevendo como os dados serão usados. Esta seção descreve como o cliente de criptografia C3R ajuda na geração de um esquema de criptografia para um arquivo CSV com uma linha de cabeçalho ou um arquivo. Parquet

Você só precisa fazer isso uma vez por arquivo. Depois que o esquema existir, ele poderá ser reutilizado para criptografar o mesmo arquivo (ou qualquer arquivo com nomes de colunas idênticos). Se os nomes das colunas ou o esquema de criptografia desejado mudarem, você deverá atualizar o arquivo do esquema. Para ter mais informações, consulte (Opcional) Crie um esquema (usuários avançados).

> **Important**
>
> É fundamental que todas as partes colaboradoras usem a mesma chave secreta compartilhada. As partes colaboradoras também devem coordenar os nomes das colunas de acordo com se elas serão JOIN editadas ou comparadas de outra forma para garantir a igualdade nas consultas. Caso contrário, as consultas SQL podem produzir resultados

inesperados ou incorretos. No entanto, isso não é necessário se o criador da colaboração habilitou a configuração de `allowJoinsOnColumnsWithDifferentNames` criptografia durante a criação da colaboração. Para obter mais informações sobre configurações relevantes para criptografia, consulte. Parâmetros de computação criptográfica

Quando executado no modo de esquema, o cliente de criptografia C3R percorre o arquivo de entrada coluna por coluna, perguntando se e como essa coluna deve ser tratada. Se o arquivo contiver muitas colunas que não são desejadas para a saída criptografada, a geração do esquema interativo pode se tornar entediante porque você deve ignorar cada coluna indesejada. Para evitar isso, você pode escrever manualmente um esquema ou criar uma versão simplificada do arquivo de entrada com apenas as colunas desejadas. Em seguida, o gerador de esquema interativo poderia ser executado nesse arquivo reduzido. O cliente de criptografia C3R gera informações sobre o arquivo do esquema e pergunta como as colunas de origem devem ser incluídas ou criptografadas (se houver) na saída de destino.

Para cada coluna de origem no arquivo de entrada, você será solicitado a fornecer:

1. Quantas colunas de destino devem ser geradas
2. Como cada coluna de destino deve ser criptografada (se for o caso)
3. O nome de cada coluna de destino
4. Como os dados devem ser preenchidos antes da criptografia se a coluna estiver sendo criptografada como uma sealed coluna

> **Note**
>
> Ao criptografar dados de uma coluna que foi criptografada como uma sealed coluna, você deve determinar quais dados precisam ser preenchidos. O cliente de criptografia C3R sugere um preenchimento padrão durante a geração do esquema que preenche todas as entradas em uma coluna com o mesmo tamanho.
> Ao determinar o tamanho de`fixed`, observe que o preenchimento está em bytes, não em bits.

A seguir está uma tabela de decisão para criar o esquema.

Tabela de decisão do esquema

Decisão	Número de colunas de destino da coluna de origem <' name-of-column '>?	Tipo de coluna de destino: [c]cleartext, [f] fingerprint ou [s]sealed?	Nome do cabeçalho da coluna de destino <default 'name-of-column'>	Adicione um sufixo <suffix>ao cabeçalho para indicar como ele foi criptografado, [y] sim ou [n] não <default 'yes'>	<' name-of-column _sealed'> tipo de preenchimento: [n] um, [f] fixo ou [m] max <default 'max'>
Deixe a coluna sem criptografia.	1	c	Não aplicável	Não aplicável	Não aplicável
Criptografe a coluna como uma fingerprint coluna.	1	f	Escolha padrão ou insira um novo nome de cabeçalho.	Digite y para escolher o padrão (`_fingerprint`) ou insiran.	Não aplicável
Criptografe a coluna como uma sealed coluna.	1	s	Escolha padrão ou insira um novo nome de cabeçalho.	Digite y para escolher o padrão (`_sealed`) ou insiran.	Escolha o tipo de preenchimento. Para ter mais informações, consulte (Opcional) Crie um esquema (usuários avançados).

Decisão	Número de colunas de destino da coluna de origem <' name-of-column '>?	Tipo de coluna de destino: [c]cleartext, [f] fingerprint ou [s]sealed?	Nome do cabeçalho da coluna de destino <default 'name-of-column'>	Adicione um sufixo <suffix>ao cabeçalho para indicar como ele foi criptografado, [y] sim ou [n] não <default 'yes'>	<' name-of-column _sealed'> tipo de preenchimento: [n] um, [f] fixo ou [m] max <default 'max'>
Criptografe a coluna como fingerprint e. sealed	2	Insira a primeira coluna de destino: f. Insira a segunda coluna de destino: s.	Escolha os cabeçalhos de destino para cada coluna de destino.	Digite y para escolher o padrão ou insira n.	Escolha o tipo de preenchimento (somente para sealed colunas). Para ter mais informações, consulte (Opcional) Crie um esquema (usuários avançados).

A seguir estão dois exemplos de como criar esquemas de criptografia. O conteúdo exato da sua interação depende do arquivo de entrada e das respostas que você fornece.

Exemplos

- Exemplo: gerar um esquema de criptografia para uma fingerprint coluna e uma cleartext coluna
- Exemplo: gerar um esquema de criptografia comsealed,fingerprint, e colunas cleartext

Exemplo: gerar um esquema de criptografia para uma fingerprint coluna e uma cleartext coluna

Neste exemplo, para`ads.csv`, há apenas duas colunas: `username` `ad_variant` e. Para essas colunas, queremos o seguinte:

- Para que a `username` coluna seja criptografada como uma `fingerprint` coluna
- Para que a `ad_variant` coluna seja uma `cleartext` coluna

Para gerar um esquema de criptografia para uma fingerprint coluna e uma cleartext coluna

1. (Opcional) Para garantir que o c3r-cli.jar arquivo e o arquivo a serem criptografados estejam presentes:

   a. Navegue até o diretório desejado e execute `ls` (se estiver usando a Mac ouUnix/Linux) ou `dir` se estiver usandoWindows).

   b. Visualize a lista de arquivos de dados tabulares (por exemplo, .csv) e escolha um arquivo para criptografar.

      Neste exemplo, `ads.csv` é o arquivo que queremos criptografar.

2. Na CLI, execute o comando a seguir para criar um esquema interativamente.

   ```
   java -jar c3r-cli.jar schema ads.csv --interactive --output=ads.json
   ```

   > **Note**
   >
   > - Você pode correr`java --jar PATH/TO/c3r-cli.jar`. Ou, se você adicionou `PATH/TO/c3r-cli.jar` à sua variável de ambiente CLASSPATH, você também pode executar o nome da classe. O cliente de criptografia C3R procurará no CLASSPATH para encontrá-la (por exemplo,). `java com.amazon.psion.cli.Main`
   > - O `--interactive` sinalizador seleciona o modo interativo para desenvolver o esquema. Isso orienta o usuário por um assistente para criar o esquema. Usuários com habilidades avançadas podem criar seu próprio esquema JSON sem usar o assistente. Para ter mais informações, consulte (Opcional) Crie um esquema (usuários avançados).

- O `--output` sinalizador define um nome de saída. Se você não incluir o `--output` sinalizador, o cliente de criptografia C3R tentará escolher um nome de saída padrão (como `<input>.out.csv` ou para o esquema). `<input>.json`

3. Para`Number of target columns from source column ‘username’?`, insira **1** e, em seguida, pressione Enter.
4. Para`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, insira **f** e, em seguida, pressione Enter.
5. Para`Target column headername <default 'username'>`, pressione Enter.

   O nome padrão '`username`' é usado.
6. Para`Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, insira **y** e, em seguida, pressione Enter.

> **Note**
>
> O modo interativo sugere sufixos para adicionar aos cabeçalhos das colunas criptografadas (`_fingerprint`para fingerprint colunas e `_sealed` para sealed colunas). Os sufixos podem ser úteis quando você está executando tarefas como carregar dados Serviços da AWS ou criar AWS Clean Rooms colaborações. Esses sufixos podem ajudar a indicar o que pode ser feito com os dados criptografados em cada coluna. Por exemplo, as coisas não funcionarão se você criptografar uma coluna como uma sealed coluna (`_sealed`) e tentar JOIN digitá-la ou tentar o contrário.

7. Para`Number of target columns from source column ‘ad_variant’?`, insira **1** e, em seguida, pressione Enter.
8. Para`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, insira **c** e, em seguida, pressione Enter.
9. Para`Target column headername <default 'username'>`, pressione Enter.

   O nome padrão '`ad_variant`' é usado.

   O esquema é gravado em um novo arquivo chamado`ads.json`.

> **Note**
>
> Você pode visualizar o esquema abrindo-o em qualquer editor de texto, como ativado Windows ou Notepad TextEdit ativadomacOS.

10. Agora você está pronto para criptografar dados.

Exemplo: gerar um esquema de criptografia comsealed,fingerprint, e colunas cleartext

Neste exemplo, para`sales.csv`, há três colunas: `username``purchased`, `product` e. Para essas colunas, queremos o seguinte:

- Para que a `product` coluna seja uma `sealed` coluna
- Para que a `username` coluna seja criptografada como uma `fingerprint` coluna
- Para que a `purchased` coluna seja uma `cleartext` coluna

Para gerar um esquema de criptografia comsealed,fingerprint, e colunas cleartext

1. (Opcional) Para garantir que o c3r-cli.jar arquivo e o arquivo a serem criptografados estejam presentes:

   a. Navegue até o diretório desejado e execute `ls` (se estiver usando a Mac ouUnix/Linux) ou `dir` se estiver usandoWindows).

   b. Veja a lista de arquivos de dados tabulares (.csv) e escolha um arquivo para criptografar.

      Neste exemplo, `sales.csv` é o arquivo que queremos criptografar.

2. Na CLI, execute o comando a seguir para criar um esquema interativamente.

```
java -jar c3r-cli.jar schema sales.csv --interactive --
output=sales.json
```

> **Note**
>
> - O `--interactive` sinalizador seleciona o modo interativo para desenvolver o esquema. Isso orienta o usuário por um fluxo de trabalho guiado para criar o esquema.
> - Se você for um usuário avançado, poderá criar seu próprio esquema JSON sem usar o fluxo de trabalho guiado. Para ter mais informações, consulte (Opcional) Crie um esquema (usuários avançados).
> - Para arquivos.csv sem cabeçalhos de coluna, consulte a `--noHeaders` sinalização do comando schema disponível na CLI.
> - O `--output` sinalizador define um nome de saída. Se você não incluir o `--output` sinalizador, o cliente de criptografia C3R tentará escolher um nome de saída padrão (como `<input>.out` ou para o esquema). `<input>.json`

3. Para `Number of target columns from source column ‘username’?`, insira **1** e, em seguida, pressione Enter.
4. Para `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, insira **f** e, em seguida, pressione Enter.
5. Para `Target column headername <default 'username'>`, pressione Enter.

   O nome padrão 'username' é usado.
6. Para `Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, insira **y** e, em seguida, pressione Enter.
7. Para `Number of target columns from source column ‘purchased’?`, insira **1** e, em seguida, pressione Enter.
8. Para `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, insira **c** e, em seguida, pressione Enter.
9. Para `Target column headername <default 'purchased'>`, pressione Enter.

   O nome padrão 'purchased' é usado.
10. Para `Number of target columns from source column ‘product’?`, insira **1** e, em seguida, pressione Enter.
11. Para `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, insira **s** e, em seguida, pressione Enter.

12. Para`Target column headername <default 'product'>`, pressione Enter.

    O nome padrão '`product`' é usado.

13. Para`‘product_sealed’ padding type: [n]one, [f]ixed, or [m]ax <default ’max’?>`, pressione Enter para escolher o padrão.

14. Para, `Byte-length beyond max length to pad cleartext to in ‘product_sealed’ <default ‘0’>?` pressione Enter para escolher o padrão.

    O esquema é gravado em um novo arquivo chamado`sales.json`.

15. Agora você está pronto para criptografar dados.

Etapa 5: criar uma chave secreta compartilhada

Para criptografar as tabelas de dados, os participantes da colaboração devem concordar e compartilhar com segurança uma chave secreta compartilhada.

A chave secreta compartilhada deve ter pelo menos 256 bits (32 bytes). Você pode especificar uma chave maior, mas ela não fornecerá nenhuma segurança adicional.

> **Important**
>
> Lembre-se de que a chave e o ID de colaboração usados para criptografia e descriptografia devem ser idênticos para todos os participantes da colaboração.

As seções a seguir fornecem exemplos de comandos do console para gerar uma chave secreta compartilhada salva como `secret.key` no diretório de trabalho atual do respectivo terminal.

Tópicos

- Exemplo: geração de chaves usando OpenSSL
- Exemplo: geração de chaves no Windows uso PowerShell

Exemplo: geração de chaves usando OpenSSL

Para uma biblioteca de criptografia de uso geral comum, execute o comando a seguir para criar uma chave secreta compartilhada.

```
openssl rand 32 > secret.key
```

Se você estiver usando Windows e não tiver OpenSSL instalado, poderá gerar chaves usando o exemplo descrito em Exemplo: geração de chaves ao Windows usar PowerShell.

Exemplo: geração de chaves no Windows uso PowerShell

ParaPowerShell, um aplicativo de terminal disponível emWindows, execute o comando a seguir para criar uma chave secreta compartilhada.

```
$bs = New-Object Byte[](32);
[Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($bs); Set-
Content 'secret.key' -Encoding Byte -Value $bs
```

Etapa 6: armazenar a chave secreta compartilhada em uma variável de ambiente

Uma variável de ambiente é uma maneira conveniente e extensível de os usuários fornecerem uma chave secreta de vários armazenamentos de chaves, como, AWS Secrets Manager e passá-la para o cliente de criptografia C3R.

O cliente de criptografia C3R pode usar chaves armazenadas Serviços da AWS se você usar o AWS CLI para armazenar essas chaves na variável de ambiente relevante. Por exemplo, o cliente de criptografia C3R pode usar uma chave de. AWS Secrets Manager Para obter mais informações, consulte Criar e gerenciar segredos AWS Secrets Manager no Guia do AWS Secrets Manager usuário.

> **Note**
>
> No entanto, antes de usar um AWS service (Serviço da AWS) como AWS Secrets Manager para armazenar suas chaves C3R, verifique se seu caso de uso permite isso. Certos casos de uso podem exigir que a chave seja retida AWS. Isso é para garantir que os dados criptografados e a chave nunca sejam mantidos pelo mesmo terceiro.

Os únicos requisitos para uma chave secreta compartilhada são que a chave secreta compartilhada seja base64 codificada e armazenada na variável de ambiente. `C3R_SHARED_SECRET`

As seções a seguir descrevem os comandos do console para converter um `secret.key` arquivo base64 e armazená-lo como uma variável de ambiente. O `secret.key` arquivo pode ter sido gerado a partir de qualquer um dos comandos listados em Etapa 5: criar uma chave secreta compartilhada e é apenas uma fonte de exemplo.

Armazene a chave em uma variável de ambiente ao Windows usar PowerShell

Para converter base64 e definir a variável de ambiente em Windows usoPowerShell, execute o comando a seguir.

```
$Bytes=[IO.File]::ReadAllBytes((Get-Location).ToString()+'\secret.key');
 $env:C3R_SHARED_SECRET=[Convert]::ToBase64String($Bytes)
```

Armazene a chave em uma variável de ambiente em Linux ou macOS

Para converter base64 e definir a variável de ambiente em Linux oumacOS, execute o comando a seguir.

```
export C3R_SHARED_SECRET="$(cat secret.key | base64)"
```

Etapa 7: criptografar dados

Para executar essa etapa, você deve adquirir o ID de AWS Clean Rooms colaboração e a chave secreta compartilhada. Para obter mais informações, consulte Prerequisites (Pré-requisitos).

No exemplo a seguir, executamos a criptografia usando o esquema que criamos chamado`ads.json`. `ads.csv`

Para criptografar dados

1. Armazene a chave secreta compartilhada para a colaboração emEtapa 6: armazenar a chave secreta compartilhada em uma variável de ambiente.
2. Na linha de comando, digite o seguinte comando.

   ```
   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. Para<name of input .csv file>, insira o nome do arquivo.csv de entrada.
4. Para`schema=`, insira o nome do arquivo do esquema de criptografia .json.
5. Para `id=`, insira o ID da colaboração.
6. Para `output=`, insira o nome do arquivo de saída (por exemplo, `ads-output.csv`).
7. Inclua qualquer um dos sinalizadores de linha de comando descritos em Parâmetros de computação criptográfica e. Sinalizadores opcionais em computação criptográfica para o Clean Rooms
8. Execute o comando.

No exemplo para`ads.csv`, executamos o seguinte comando.

java -jar c3r-cli.jar encrypt ***ads.csv*** --schema=***ads.json*** --id=***123e4567-e89b-42d3-a456-556642440000*** --output=***ads-output.csv***

No exemplo parasales.csv, executamos o seguinte comando.

java -jar c3r-cli.jar encrypt ***sales.csv*** --schema=***sales.json*** --id=***123e4567-e89b-42d3-a456-556642440000***

> **Note**
>
> Neste exemplo, não especificamos um nome de arquivo de saída (`--output=`*`sales-output.csv`*). Como resultado, o nome do arquivo de saída padrão `name-of-file.out.csv` foi gerado.

Agora você está pronto para verificar os dados criptografados.

Etapa 8: verificar a criptografia de dados

Para verificar se os dados foram criptografados

1. Visualize o arquivo de dados criptografado (por exemplo,`sales-output.csv`).
2. Verifique as seguintes colunas:
   a. Coluna 1 — Criptografada (por exemplo,`username_fingerprint`).

Para as fingerprint colunas (HMAC), após a versão e o prefixo de tipo (por exemplo,`01:hmac:`), há 44 caracteres de dados codificados em base64.

b. Coluna 2 — Não criptografada (por exemplo,`purchased`).

c. Coluna 3 — Criptografada (por exemplo,`product_sealed`).

Para colunas criptografadas (SELECT), o comprimento do cleartext mais qualquer preenchimento após a versão e o prefixo de tipo (por exemplo,`01:enc:`) é diretamente proporcional ao comprimento do cleartext que foi criptografado. Ou seja, o comprimento é o tamanho da entrada mais aproximadamente 33% de sobrecarga devido à codificação.

Agora está tudo pronto para:

1. Faça o upload dos dados criptografados para o S3.
2. Crie uma AWS Glue tabela.
3. Crie uma tabela configurada em AWS Clean Rooms.

O cliente de criptografia C3R criará arquivos temporários que não contêm dados não criptografados (a menos que esses dados também não sejam criptografados na saída final). No entanto, alguns valores criptografados podem não ser preenchidos corretamente. As colunas de impressão digital podem conter valores duplicados, mesmo que a configuração `allowRepeatedFingerprintValue` de colaboração seja. `false` Esse problema ocorre porque o arquivo temporário é gravado antes que os comprimentos adequados de preenchimento e as propriedades de remoção de duplicatas sejam verificados.

Se o cliente de criptografia C3R falhar ou for interrompido durante a criptografia, ele poderá parar depois de gravar o arquivo temporário, mas antes de verificar essas propriedades e excluir os arquivos temporários. Portanto, esses arquivos temporários ainda podem estar no disco. Se for esse o caso, o conteúdo desses arquivos não protege os dados de texto simples nos mesmos níveis da saída. Em particular, esses arquivos temporários podem revelar dados de texto simples para análises estatísticas que não funcionariam na saída final. O usuário deve excluir esses arquivos (especialmente um SQLite banco de dados) para evitar que eles caiam em mãos não autorizadas.

(Opcional) Crie um esquema (usuários avançados)

A criação manual de um esquema é para usuários avançados.

Veja a seguir uma descrição do formato de arquivo do esquema JSON para arquivos de entrada com ou sem cabeçalhos de coluna. Usuários avançados podem escrever ou modificar diretamente o esquema, se desejarem.

> **Note**
>
> O cliente de criptografia C3R pode ajudá-lo a criar um esquema por meio do processo interativo descrito em Exemplo: gerar um esquema de criptografia comsealed,fingerprint, e colunas cleartext ou por meio da criação de um modelo de stub.

Esquemas de tabelas mapeadas e posicionais

A seção a seguir descreve dois tipos de esquemas de tabela:

- Esquema de tabela mapeada — Esse esquema é usado para criptografar arquivos.csv com uma linha de cabeçalho e arquivos. Apache Parquet
- Esquema de tabela posicional — Esse esquema é usado para criptografar arquivos.csv sem uma linha de cabeçalho.

O cliente de criptografia C3R pode criptografar um arquivo tabular para uma colaboração. Para fazer isso, ele deve ter um arquivo de esquema correspondente que especifique como a saída criptografada deve ser derivada da entrada.

O cliente de criptografia C3R pode ajudar a gerar um esquema para um `INPUT` arquivo executando o comando esquema do cliente de criptografia C3R na linha de comando. Um exemplo de comando `éjava -jar c3r-cli.jar schema --interactive INPUT`.

O esquema especifica as seguintes informações:

1. Quais colunas de origem são mapeadas para quais colunas transformadas no arquivo de saída por meio de seus nomes de cabeçalho (esquemas mapeados) ou posição (esquemas posicionais)
2. Quais colunas-alvo devem permanecer cleartext
3. Quais colunas de destino devem ser criptografadas para SELECT consultas
4. Quais colunas de destino devem ser criptografadas para JOIN consultas

Essas informações são codificadas em um arquivo de esquema JSON específico da tabela, que consiste em um único objeto cujo `headerRow` campo é um valor booleano. O valor deve ser `true` para Parquet arquivos e arquivos.csv com uma linha de cabeçalho e `false` outros.

Esquema de tabela mapeada

O esquema mapeado tem a seguinte forma.

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": STRING,
      "targetHeader": STRING,
      "type": TYPE,
      "pad": PAD
    },
    ...
  ]
}
```

Se `headerRow` for`true`, o próximo campo no objeto será`columns`, que contém uma matriz de esquemas de colunas que mapeiam cabeçalhos de origem para cabeçalhos de destino (ou seja, objetos JSON descrevendo o que as colunas de saída devem conter).

- `sourceHeader`— O nome do `STRING` cabeçalho da coluna de origem da qual os dados são derivados.

  > **Note**
  >
  > A mesma coluna de origem pode ser usada para várias colunas de destino.
  > Uma coluna do arquivo de entrada não listada como em `sourceHeader` nenhum lugar do esquema não aparece no arquivo de saída.

- `targetHeader`— O nome do `STRING` cabeçalho da coluna correspondente no arquivo de saída.

  > **Note**
  >
  > Esse campo é opcional para esquemas mapeados. Se esse campo for omitido, o `sourceHeader` será reutilizado para o nome do cabeçalho na saída. `_fingerprint`Ou

`_sealed` é anexado se a coluna de saída for uma fingerprint coluna ou sealed coluna, respectivamente.

- `type`— A TYPE da coluna de destino no arquivo de saída. Ou seja, uma das `cleartext`, `sealed`, ou `fingerprint` dependendo de como a coluna será usada na colaboração.
- `pad`— Um campo de um objeto de esquema de coluna que só está presente quando o TYPE é`sealed`. Seu valor correspondente de PAD é um objeto que descreve como os dados devem ser preenchidos antes de serem criptografados.

```
{
  "type": PAD_TYPE,
  "length": INT
}
```

Para especificar o preenchimento de pré-criptografia, `type` e `length` são usados da seguinte forma:

- PAD_TYPEas `none` — Nenhum preenchimento será aplicado aos dados da coluna e o `length` campo não é aplicável (ou seja, omitido).
- PAD_TYPEas `fixed` — Os dados da coluna são `length` preenchidos com os bytes especificados.
- PAD_TYPEas `max` — Os dados da coluna são preenchidos até o tamanho do byte do valor mais longo, mais bytes adicionais. `length`

Veja a seguir um exemplo de esquema mapeado, com uma coluna de cada tipo.

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

Como um exemplo mais complexo, a seguir está um exemplo de arquivo.csv com cabeçalhos.

```
FirstName,LastName,Address,City,State,PhoneNumber,Title,Level,Notes
Jorge,Souza,12345 Mills Rd,Anytown,SC,703-555-1234,CEO,10,
Paulo,Santos,0 Street,Anytown,MD,404-555-111,CIO,9,This is a really long note that
 could really be a paragraph
Mateo,Jackson,1 Two St,Anytown,NY,304-555-1324,COO,9,""
Terry,Whitlock4 N St,Anytown,VA,407-555-8888,EA,7,Secret notes
Diego,Ramirez,9 Hollows Rd,Anytown,VA,407-555-1222,SDE I,4,null
John,Doe,8 Hollows Rd,Anytown,VA,407-555-4321,SDE I,4,Jane's younger brother
Jane,Doe,8 Hollows Rd,Anytown,VA,407-555-4322,SDE II,5,John's older sister
```

No exemplo de esquema mapeado a seguir, as colunas `FirstName` e `LastName` são `cleartext` colunas. A `State` coluna é criptografada como uma `fingerprint` coluna e como uma `sealed` coluna com um preenchimento denone. As colunas restantes são omitidas.

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

A seguir está o arquivo.csv que resulta do esquema mapeado.

```
givenname,surname,state_fingerprint,state
John,Doe,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv
+1Mk=,01:enc:FQ3n3Ahv9BQQNWQGcugeHzHYzEZE1vapHa2Uu4SRgSAtZ3qObjPA4TcsHt
+BOkMKBcnHWI13BeGG/SBqmj7vKpI=
Paulo,Santos,01:hmac:CHF4eIrtTNgAooU9v4h9Qjc
+txBnMidQTjdjWuaDTTA=,01:enc:KZ5n5GtaXACco65AXk48BQO2durDNR2ULc4YxmMC8NaZZKKJiksU1IwFadAvV4iBQ1
Mateo,Jackson,01:hmac:iIRnjfNBzryusIJ1w35lgNzeY1RQ1bSfq6PDHW8Xrbk=,01:enc:mLKpS5HIOSgphdEsrzhEd
eN9nBO2gAbIygt4OFn4LalYn9Xyj/XUWXlmn8zFe2T4kyDTD8kGOvpQEUGxAUFk=
Diego,Ramirez,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:rmZhT98Zm
+IIGw1UTjMIJP4IrW/AAltBLMXcHvnYfRgmWP623VFQ6aUnhsb2MDqEw4G5Uwg5rKKZepUxx5uKbfk=
Jorge,Souza,01:hmac:3BxJdXiFFyZ8HBbYNqqEhBVqhNOd7s2ZiKUe7QiTyo8=,01:enc:vVaqWC1VRbhvkf8gnuR7q0z
Terry,Whitlock01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:3c9VEWbODO/
xbQjdGuccLvI7oZTBdPU+SyrJIyr2kudfAxbuMQ2uRdU/q7rbgyJjxZS8M2U35ILJf/lDgTyg7cM=
Jane,Doe,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:9RWv46YLveykeNZ/
G0NdlYFg+AVdOnu05hHyAYTQkPLHnyX+0/jbzD/g9ZT8GCgVE9aB5bV4ooJIXHGBVMXcjrQ=
```

Esquema de tabela posicional

O esquema posicional tem a seguinte forma.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      },
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      }
    ],
    [],
    ...
  ]
}
```

Se `headerRow` for`false`, o próximo campo no objeto será`columns`, que contém uma matriz de entradas. Cada entrada em si é uma matriz de zero ou mais esquemas de colunas posicionais (sem `sourceHeader` campo), que são objetos JSON que descrevem o que a saída deve conter.

- `sourceHeader`— O nome do `STRING` cabeçalho da coluna de origem da qual os dados são derivados.

  > **Note**
  >
  > Esse campo deve ser omitido nos esquemas posicionais. Em esquemas posicionais, a coluna de origem é inferida pelo índice correspondente da coluna no arquivo do esquema.

- `targetHeader`— O nome do `STRING` cabeçalho da coluna correspondente no arquivo de saída.

> **Note**
>
> Esse campo é obrigatório para esquemas posicionais.

- `type`— A TYPE da coluna de destino no arquivo de saída. Ou seja, uma das `cleartextsealed`, ou `fingerprint` dependendo de como a coluna será usada na colaboração.
- `pad`— Um campo de um objeto de esquema de coluna que só está presente quando o TYPE é`sealed`. Seu valor correspondente de PAD é um objeto que descreve como os dados devem ser preenchidos antes de serem criptografados.

```
{
  "type": PAD_TYPE,
  "length": INT
}
```

Para especificar o preenchimento de pré-criptografia, `type` e `length` são usados da seguinte forma:

- PAD_TYPEas `none` — Nenhum preenchimento será aplicado aos dados da coluna e o `length` campo não é aplicável (ou seja, omitido).
- PAD_TYPEas `fixed` — Os dados da coluna são `length` preenchidos com os bytes especificados.
- PAD_TYPEas `max` — Os dados da coluna são preenchidos até o tamanho do byte do valor mais longo, mais bytes adicionais. `length`

> **Note**
>
> `fixed`é útil se você souber com antecedência um limite superior no tamanho do byte dos dados da coluna. Um erro é gerado se algum dado nessa coluna for maior que o especificado`length`.
> `max`é conveniente quando o tamanho exato dos dados de entrada é desconhecido, pois funciona independentemente do tamanho dos dados. No entanto, `max` requer tempo de processamento adicional porque criptografa os dados duas vezes. `max`criptografa os dados uma vez quando lidos no arquivo temporário e uma vez após a entrada de dados mais longa na coluna ser conhecida.
> Além disso, o comprimento do valor mais longo não é salvo entre as invocações do cliente. Se você planeja criptografar seus dados em lotes ou criptografar novos dados

periodicamente, esteja ciente de que os comprimentos de texto cifrado resultantes podem variar entre os lotes.

Veja a seguir um exemplo de um esquema posicional.

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

Como um exemplo complexo, a seguir está um exemplo de arquivo.csv se ele não tivesse a primeira linha com os cabeçalhos.

```
Jorge,Souza,12345 Mills Rd,Anytown,SC, 703 -555 -1234,CEO, 10,
Paulo,Santos, 0 Street,Anytown,MD, 404-555-111,CIO, 9,This is a really long note that
 could really be a paragraph
Mateo,Jackson, 1 Two St,Anytown,NY, 304-555-1324,COO, 9, ""
Terry,Whitlock, 4 N St,Anytown,VA, 407-555-8888,EA, 7,Secret notes
Diego,Ramirez, 9 Hollows Rd,Anytown,VA, 407-555-1222,SDE I, 4,null
John,Doe, 8 Hollows Rd,Anytown,VA, 407-555-4321,SDE I, 4,Jane's younger brother
Jane,Doe, 8 Hollows Rd,Anytown,VA, 407-555-4322,SDE II, 5,John's older sister
```

O esquema posicional tem o seguinte formato.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": "GivenName",
        "type": "cleartext"
      }
    ],
    [
      {
        "targetHeader": "Surname",
        "type": "cleartext"
      }
    ],
    [],
    [],
    [
      {
        "targetHeader": "State_Join",
        "type": "fingerprint"
      },
      {
        "targetHeader": "State",
        "type": "sealed",
        "pad": {
          "type": "none"
        }
      }
```

```
    ],
    [],
    [],
    [],
    []
  ]
}
```

O esquema anterior produz o seguinte arquivo de saída com uma linha de cabeçalho contendo os cabeçalhos de destino especificados.

```
givenname,surname,state_fingerprint,state
Mateo,Jackson,01:hmac:iIRnjfNBzryusIJ1w35lgNzeY1RQ1bSfq6PDHW8Xrbk=,01:enc:ENS6QD3cMVl9vQEGfe9MN
Q8m/Y5SA89dJwKpT5rGPp8e36h6klwDoslpFzGvU0=
Jorge,Souza,01:hmac:3BxJdXiFFyZ8HBbYNqqEhBVqhNOd7s2ZiKUe7QiTyo8=,01:enc:LKo0zirq2+
+XEIIIMNRjAsGMdyWUDwYaum0B+IFP+rUf1BNeZDJjtFe1Z+zbZfXQWwJy52Rt7HqvAb2WIK1oMmk=
Paulo,Santos,01:hmac:CHF4eIrtTNgAooU9v4h9Qjc
+txBnMidQTjdjWuaDTTA=,01:enc:MyQKyWxJ9kvK1xDQQtXlUNwv3F+yrBRr0xrUY/1BGg5KFgOn9pK+MZ7g
+ZNqZEPcPz4lht1u0t/wbTaqzOCLXFQ=
Jane,Doe,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:Pd8sbITBfb0/
ttUB4svVsgoYkDfnDvgkvxzeci0Yxq54rLSwccy1o3/B50C3cpkkn56dovCwzgmmPNwrmCmYtb4=
Terry,Whitlock01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv
+1Mk=,01:enc:Qmtzu3B3GAXKh2KkRYTiEAaMopYedsSdF2e/
ADUiBQ9kv2CxKPzWyYTD3ztmKPMka19dHre5VhUHNpO3O+j1AQ8=
Diego,Ramirez,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:ysdg
+GHKdeZrS/geBIooOEPLHG68MsWpx1dh3xjb+fG5rmFmqUcJLNuuYBHhHAlxchM2WVeV1fmHkBX3mvZNvkc=
John,Doe,01:hmac:UK8s8Cn/WR2JO/To2dTxWD73aDEe2ZUXeSHy3Tv+1Mk=,01:enc:9uX0wZuO7kAPAx
+Hf6uvQownkWqFSKtWS7gQIJSe5aXFquKWCK6yZN0X5Ea2N3bn03Uj1kh0agDWoiP9FRZGJA4=
```

Criar uma tabela configurada no AWS Clean Rooms

Uma tabela configurada é uma referência a uma tabela existente no AWS Glue Data Catalog. Ele contém uma regra de análise que determina como os dados podem ser consultados no AWS Clean Rooms. As tabelas configuradas podem ser associadas a uma ou mais colaborações. Para obter mais informações sobre AWS Glue, consulte o AWS Glue Developer Guide.

Use a geração de estatísticas fornecida por AWS Glue para calcular estatísticas em nível de coluna para tabelas. AWS Glue Data Catalog Depois de AWS Glue gerar estatísticas para tabelas no catálogo de dados, o Amazon Redshift Spectrum usa automaticamente essas estatísticas para otimizar o plano de consulta. Para obter mais informações sobre o uso de estatísticas em nível de coluna AWS Glue, consulte o Guia de trabalho com estatísticas de coluna.

Criar uma tabela configurada

Nesta etapa, você cria uma tabela configurada AWS Clean Rooms para usar na colaboração.

Para criar uma tabela configurada no AWS Clean Rooms

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. No canto superior direito, escolha Configurar nova tabela.
4. Em Configurar nova tabela, em Escolher tabela do AWS Glue :
   a. Escolha o Banco de dados que você deseja configurar na lista suspensa.
   b. Escolha a Tabela que deseja configurar na lista suspensa.

> **Note**
>
> Para verificar se essa é a tabela correta, faça um dos seguintes:
>
> - Escolha Exibir em AWS Glue.
> - Ative Exibir esquema para ver o esquema.

5. Em Colunas permitidas em colaborações, escolha Todas as colunas ou Lista personalizada.

Se você escolher...	Então…
Todas as colunas	Todas as colunas podem ser usadas em AWS Clean Rooms (sujeitas às regras de análise).
Lista personalizada	Escolha uma ou mais colunas que deseja permitir na lista suspensa Especificar colunas permitidas.

6. Para obter detalhes da tabela configurada,

   a. Insira um Nome para a tabela configurada.

      Você pode usar o nome padrão ou renomear essa tabela.

   b. Insira uma Descrição da tabela.

      A descrição ajuda a diferenciar outras tabelas configuradas com nomes semelhantes.

   c. Se quiser habilitar Tags para o recurso de tabela configurado, escolha Adicionar nova tag e, em seguida, insira o par Chave e Valor.

7. Escolha Configurar nova tabela.

Próximas etapas

Agora que você criou uma tabela configurada, você está pronto para:

- Configurar uma regra de análise para a tabela configurada
- Associar a tabela configurada a uma colaboração

Configurando uma regra de análise em uma tabela configurada

As seções a seguir descrevem como configurar uma regra de análise para sua tabela configurada. Ao definir as regras de análise, é possível autorizar o membro que pode consultar a executar consultas que correspondam a uma regra de análise específica compatível com o AWS Clean Rooms.

AWS Clean Rooms suporta os seguintes tipos de regras de análise: agregação, lista e customização.

Só pode haver uma regra de análise por tabela configurada.

> **Important**
>
> Se você estiver usando Computação Criptográfica Clean Rooms e tiver tabelas de dados criptografadas na colaboração, a regra de análise adicionada à tabela configurada criptografada deverá ser consistente com a forma como os dados foram criptografados. Por exemplo, se você criptografou os dados para SELECT (regra de análise de agregação), não deve adicionar a regra de análise para JOIN (regra de análise de lista).

Para obter uma compreensão dos tipos de regras de análise que estão disponíveis em AWS Clean Rooms, consulte Regras de análise em AWS Clean Rooms.

Para obter mais informações sobre a regra de análise de agregação, consulte Regra de análise de agregação.

Para obter mais informações sobre a regra de análise de lista, consulte Regra de análise de lista.

Para obter mais informações sobre a regra de análise personalizada, consulte Regra de análise personalizada em AWS Clean Rooms.

Depois de revisar e compreender essas seções, você pode executar os seguintes procedimentos:

Tópicos

- Configurando uma regra de análise de agregação em uma tabela (fluxo guiado)
- Configurando uma regra de análise de lista em uma tabela (fluxo guiado)
- Configurando uma regra de análise personalizada em uma tabela (fluxo guiado)

Configurando uma regra de análise de agregação em uma tabela (fluxo guiado)

A regra de análise de agregação permite consultas que agregam estatísticas sem revelar informações no nível de linha usando funções COUNT, SUM e AVG ao longo de dimensões opcionais.

Esse procedimento descreve o processo de adicionar uma regra de análise de agregação à sua tabela configurada usando a opção Fluxo guiado no console AWS Clean Rooms.

Para adicionar a regra de análise de agregação a uma tabela (fluxo guiado)

1. Faça login no AWS Management Console e abra o console AWS Clean Rooms com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. Escolha a tabela configurada.
4. Na página de detalhes da tabela configurada, escolha Configurar regra de análise.
5. Em Etapa 1: Escolha o tipo, em Tipo, deixe a opção Agregação selecionada por padrão.
6. Em Método de criação, selecione Fluxo guiado e escolha Avançar.
7. Na Etapa 2: Especifique os controles de consulta, para Funções agregadas:

    a. Escolha uma Função agregadas no menu suspenso:

        - CONTAGEM
        - CONTAGEM DISTINTA
        - SUM
        - SOMA DISTINTA
        - AVG

    b. Escolha quais colunas podem ser usadas na Função agregadas no menu suspenso Colunas.

    c. (Opcional) Escolha Adicionar outra função para adicionar outra função agregada e associar uma ou mais colunas a essa função.

> **Note**
>
> Pelo menos uma função agregada é necessária.

d. (Opcional) Escolha Remover para remover uma função agregada.

8. Para Controles de junção,

a. Escolha uma opção para Permitir que a tabela seja consultada sozinha:

Se você escolher...	Então…
Não, somente a sobreposição pode ser consultada	A tabela só pode ser consultada quando unida a uma tabela de propriedade do membro que pode consultar.
Sim	A tabela pode ser consultada sozinha ou quando unida a outras tabelas.

b. Em Especificar colunas de junção, escolha as colunas que você deseja permitir que sejam usadas na instrução INNER JOIN.

Isso é opcional se você tiver selecionado Sim na etapa anterior.

c. Em Especificar operadores permitidos para correspondência, escolha quais operadores, se houver, podem ser usados para correspondência em várias colunas de junção. Se você selecionar duas ou mais colunas JOIN, um desses operadores será necessário.

Se você escolher...	Então…
E	Você pode incluir `AND` nas condições de correspondência `INNER JOIN` a união de uma coluna a outra coluna entre as tabelas.
OU	Você pode incluir `OR` nas condições de correspondência `INNER JOIN` para combinar várias correspondências de colunas entre tabelas. Esse operador

Se você escolher...	Então…
	lógico é útil para obter uma taxa de correspondência mais alta.

9. (Opcional) Para Controles de dimensão, no menu suspenso Especificar colunas de dimensão, escolha quais colunas você deseja permitir que sejam usadas na instrução SELECT e as partes WHERE, GROUP, BY e ORDER BY da consulta.

> **Note**
>
> A função de agregação ou as colunas de junção não podem ser usadas como colunas de Dimensão.

10. Para Funções escalares, escolha uma opção para Quais funções escalares você deseja permitir?

Se você escolher...	Então…
Todos atualmente suportados por AWS Clean Rooms	Você permite todas as funções escalares atualmente suportadas pelo AWS Clean Rooms. • Você pode escolher Exibir lista para ver a lista completa de Funções escalares suportadas no AWS Clean Rooms.
Uma lista personalizada	Você pode personalizar quais funções escalares permitir. • Escolha uma ou mais opções no menu suspenso Especificar funções escalares permitidas.
Nenhum	Você não quer permitir nenhuma função escalar.

Para obter mais informações, consulte Funções escalares.

11. Escolha Next (Próximo).
12. Na Etapa 3: Especifique os controles dos resultados da consulta, para Restrições de agregação:
    a. Selecione a lista suspensa para cada nome de Coluna.
    b. Selecione a lista suspensa para cada Número mínimo de valores distintos que devem ser atendidos para que cada linha de saída seja retornada, depois que a função COUNT DISTINCT for aplicada a ela.
    c. Escolha Adicionar restrição para adicionar mais restrições de agregação.
    d. (Opcional) Escolha Remover para remover uma restrição de agregação.
13. Escolha Next (Próximo).
14. Em Etapa 4: revisar e configurar, revise as seleções feitas nas etapas anteriores, edite se necessário e escolha Configurar regra de análise.

Você vê uma mensagem de confirmação de que configurou com êxito uma regra de análise de agregação na tabela.

Configurando uma regra de análise de lista em uma tabela (fluxo guiado)

A regra de análise de lista permite consultas que geram listas em nível de linha da sobreposição entre a tabela associada e uma tabela do membro que pode consultar.

Esse procedimento descreve o processo de adicionar a regra de análise de lista à tabela configurada usando a opção Fluxo guiado no console AWS Clean Rooms.

Para adicionar uma regra de análise de lista a uma tabela (fluxo guiado)

1. Faça login no AWS Management Console e abra o console AWS Clean Rooms com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. Escolha a tabela configurada.
4. Na página de detalhes da tabela configurada, escolha Configurar regra de análise.
5. Em Etapa 1: Escolha o tipo, em Tipo, escolha a opção Lista.
6. Em Método de criação, selecione Fluxo guiado e escolha Avançar.
7. Em Etapa 2: Especificar controles de consulta, para controles de junção:

a. Em Especificar colunas de junção, escolha as colunas que você deseja permitir que sejam usadas na instrução INNER JOIN.

b. Em Especificar operadores permitidos para correspondência, escolha quais operadores, se houver, podem ser usados para correspondência em várias colunas de junção. Se você selecionar duas ou mais colunas JOIN, um desses operadores será necessário.

Se você escolher...	Então…
E	Você pode incluir `AND` nas condições de correspondência `INNER JOIN` a união de uma coluna a outra coluna entre as tabelas.
OU	Você pode incluir `OR` nas condições de correspondência `INNER JOIN` para combinar várias correspondências de colunas entre tabelas. Esse operador lógico é útil para obter uma taxa de correspondência mais alta.

8. (Opcional) Para Controles de lista, no menu suspenso Especificar colunas da lista, escolha quais colunas você deseja permitir que sejam usadas na saída da consulta (ou seja, usadas na instrução SELECT) ou usadas para filtrar resultados (ou seja, a instrução WHERE).
9. Escolha Next (Próximo).
10. Em Etapa 3: revisar e configurar, revise as seleções feitas nas etapas anteriores, edite se necessário e escolha Configurar regra de análise.

Você vê uma mensagem de confirmação de que configurou com êxito uma regra de análise de lista para a tabela.

Configurando uma regra de análise personalizada em uma tabela (fluxo guiado)

A regra de análise personalizada permite consultas SQL personalizadas em uma tabela configurada. A regra de análise personalizada é necessária se usar modelos de análise ou privacidade diferencial.

Esse procedimento descreve o processo de adicionar a regra de análise personalizada à tabela configurada usando a opção Fluxo guiado no console AWS Clean Rooms.

Para adicionar uma regra de análise personalizada a uma tabela (fluxo guiado)

1. Faça login no AWS Management Console e abra o console AWS Clean Rooms com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. Escolha a tabela configurada.
4. Na página de detalhes da tabela configurada, escolha Configurar regra de análise.
5. Em Etapa 1: Escolha o tipo, em Tipo, escolha a opção Personalizado.
6. Em Método de criação, selecione Fluxo guiado e escolha Avançar.
7. Em Etapa 2: definir privacidade diferencial, determine se você deseja que a privacidade diferencial seja ativada ou desativada. A privacidade diferencial é uma técnica matematicamente comprovada para proteger seus dados contra ataques de reidentificação.

   a. Em Privacidade diferencial:

Se você…	A seguir, escolha…
Tem dados no nível de usuário e deseja proteção contra tentativas de reidentif icação	Ativar
Não tem dados no nível de usuário ou não precisa de proteção contra tentativas de reidentificação	Desativar

   b. Se você optou por Ativar a privacidade diferencial, selecione a coluna Identificador de usuário que contém o identificador exclusivo dos usuários, como a coluna `user_id`, cuja privacidade você deseja proteger. Se quiser ativar a privacidade diferencial para duas ou mais tabelas em uma colaboração, você deve configurar a mesma coluna da coluna Identificador de usuário em ambas as regras de análise para manter uma definição consistente dos usuários nas tabelas. Em caso de configuração incorreta, o membro que pode consultar recebe uma mensagem de erro informando que há duas colunas a escolher para calcular o número de contribuições do usuário (por exemplo, o número de impressões de anúncios feitas por um usuário) enquanto executa a consulta.

c. Escolha Next (Próximo).

8. Em Etapa 3: especificar controles de consulta,

   a. Para o Tipo de controle:

Se você deseja ...	A seguir, escolha…
Revise cada novo modelo de análise antes de executá-lo na tabela configurada	Revise cada nova análise antes que ela possa ser executada nesta tabela
Permita que qualquer modelo de análise ou consulta direta seja executada em sua tabela configurada	Permita que qualquer consulta criada por colaboradores específicos seja executada sem revisão nesta tabela

   b. Escolha uma das seguintes opções:

Se você escolheu...	Então…
Revise cada nova análise antes que ela possa ser executada nesta tabela	Em Modelos de análise que podem ser executados, escolha Adicionar modelo de análise e, em seguida, escolha a Colaboração e o Modelo de análise apropriados nas listas suspensas.
Permita que qualquer consulta criada por colaboradores específicos seja executada sem revisão nesta tabela	Em Permitido criar qualquer consulta Contas da AWS, escolha Adicionar Conta da AWS e, em seguida, escolha o ID Conta da AWS apropriado.

9. Escolha Next (Próximo).
10. Em Etapa 4: revisar e configurar, revise as seleções feitas nas etapas anteriores, edite se necessário e escolha Configurar regra de análise.

Você verá uma mensagem de confirmação de que configurou com êxito uma regra de análise personalizada para a tabela.

Configurando a regra de análise em uma tabela (editor JSON)

O procedimento a seguir mostra como adicionar uma regra de análise a uma tabela usando a opção do Editor JSON no console AWS Clean Rooms.

Para configurar uma agregação, lista ou regra de análise personalizada em uma tabela (editor JSON)

1. Faça login no AWS Management Console e abra o console AWS Clean Rooms com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. Escolha a tabela configurada.
4. Na página de detalhes da tabela configurada, escolha Configurar regra de análise.
5. Em Etapa 1: Escolha o tipo, em Tipo, escolha a opção Agregação, Lista ou Personalizado.
6. Em Método de criação, selecione Editor JSON e escolha Avançar.
7. Em Etapa 2: Especificar controles, você pode optar por inserir uma estrutura de consulta (Inserir modelo) ou inserir um arquivo (Importar do arquivo).

Se você escolher...	Então…
Inserir modelo	1. Especifique os parâmetros para a regra de análise selecionada na definição da regra de análise. 2. Você pode pressionar Ctrl + Barra de espaço para ativar o preenchimento automático. Para obter mais informações sobre parâmetros de regra de análise de agregação, consulte Regra de análise de agregação - controles de consulta. Para obter mais informações sobre parâmetros de regra de análise de lista, consulte Regra de análise de lista - controles de consulta.

Se você escolher...	Então…
Importar do arquivo	1. Selecione seu arquivo JSON na sua unidade local. 2. Escolha Open (Abrir). A definição da regra de análise exibe a regra de análise do arquivo carregado.

8. Escolha Next (Próximo).
9. Em Etapa 3: revisar e configurar, revise as seleções feitas nas etapas anteriores, edite se necessário e escolha Configurar regra de análise.

Você receberá uma mensagem de confirmação de que configurou com êxito uma regra de análise para a tabela.

Próximas etapas

Agora que você configurou uma regra de análise em sua tabela configurada, você está pronto para:

- Associar uma tabela configurada a uma colaboração
- Consulte as tabelas de dados (como um membro que pode consultar)

Associar uma tabela configurada a uma colaboração

Depois de criar uma tabela configurada e adicionar uma regra de análise a ela, você pode associá-la a uma colaboração.

Important

Antes de associar as AWS Glue tabelas configuradas à colaboração, a localização da AWS Glue tabela deve apontar para uma pasta do Amazon Simple Storage Service (Amazon S3) e não para um único arquivo. Você pode verificar esse local visualizando a tabela no AWS Glue console em https://console.aws.amazon.com/glue/.

Note

Se você configurou a criptografia AWS Glue e criou uma função de serviço, deverá conceder a essa função acesso AWS KMS keys para uso na descriptografia AWS Glue de tabelas. Se você associou uma tabela configurada que é apoiada por um conjunto AWS KMS de dados criptografado do Amazon S3, você deve conceder à função acesso para usar a chave KMS para descriptografar dados do Amazon S3.
Para obter mais informações, consulte Configurar criptografia em AWS Glue no Guia do desenvolvedor do AWS Glue .

Os tópicos a seguir descrevem como associar uma tabela configurada a uma colaboração usando o AWS Clean Rooms console:

Tópicos

Para obter informações sobre como associar suas tabelas configuradas à colaboração usando os SDKs da AWS , consulte a Referência da API do AWS Clean Rooms .

Associar uma tabela configurada a partir da página de detalhes da tabela configurada

Para associar AWS Glue tabelas à colaboração a partir da página de detalhes da tabela configurada

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. Escolha a tabela configurada.
4. Na página de detalhes da tabela configurada, escolha Associar à colaboração.
5. Para a caixa de diálogo Associar tabela à colaboração, escolha a Colaboração na lista suspensa.
6. Escolha Escolher colaboração.

   Na página Associar tabela, o nome da tabela configurada que você escolheu aparece na seção Escolher tabela configurada.
7. Em Escolher tabela configurada, faça o seguinte:

Se você deseja...	Então...
Configurar uma tabela	Escolha Configurar tabela e siga as instruções na página Configurar tabela.
Exibir o esquema e a regra de análise da tabela configurada	Ative Exibir esquema e regra de análise.

8. Especifique as permissões de Acesso ao serviço selecionando Criar e usar um novo perfil de serviço ou Usar um perfil de serviço existente.

Se você escolher...	Então...
Criar e usar um novo perfil de serviço	• AWS Clean Rooms cria uma função de serviço com a política necessária para essa tabela. • O nome do perfil de serviço padrão é `cleanrooms-<timestamp>`

Se você escolher...	Então...
	• Você deve ter permissões para criar perfis e anexar políticas. • Se seus dados de entrada estiverem criptografados, você poderá seleciona r Esses dados são criptografados com uma chave KMS e, em seguida, inserir uma AWS KMS key que será usada para descriptografar sua entrada de dados.

Se você escolher...	Então...
Use um perfil de serviço existente	1. Escolha um nome do perfil de serviço existente na lista suspensa. A lista de perfis é exibida se você tiver permissões para listar funções. Se você não tiver permissões para listar perfis, insira o nome do recurso da Amazon (ARN) do perfil que você deseja usar. 2. Veja a função de serviço escolhendo o link externo Exibir no IAM. Se não houver perfis de serviço existente s, a opção de Usar um perfil de serviço existente não estará disponível. Por padrão, AWS Clean Rooms não tenta atualizar a política de perfil existente para adicionar as permissões necessárias. 3. (Opcional) Marque a caixa de seleção Adicionar uma política pré-configurada com as permissões necessárias para esse perfil para adicionar as permissõe s necessárias ao perfil. Você deve ter permissões para modificar funções e criar políticas.

> **Note**
>
> - AWS Clean Rooms requer permissões para consultar de acordo com as regras de análise. Para obter mais informações sobre permissões para AWS Clean Rooms, consulteAWS políticas gerenciadas para AWS Clean Rooms.

- Se a função não tiver permissões suficientes para AWS Clean Rooms, você receberá uma mensagem de erro informando que a função não tem permissões suficientes para AWS Clean Rooms. A política de perfil deve ser adicionada antes de continuar.
- Se você não conseguir modificar a política de perfil, receberá uma mensagem de erro informando que AWS Clean Rooms não conseguiu encontrar a política para o perfil de serviço.

9. Se quiser habilitar Tags para o recurso de associação de tabelas configurado, escolha Adicionar nova tag e, em seguida, insira o par de Chave e Valor.
10. Escolha Associar tabela.

Associar uma tabela configurada a partir da página de detalhes da colaboração

Para associar AWS Glue tabelas à colaboração a partir da página de detalhes da colaboração

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Na guia Tabelas, escolha Associar tabela.
5. Em Escolher tabela configurada, faça o seguinte:

Se você deseja...	Então...
Escolha uma tabela configurada existente	Escolha o Nome da tabela configurada que você deseja associar à colaboração na lista suspensa.
Configurar uma tabela	Escolha Configurar tabela e siga as instruçõe s na página Configurar tabela.
Exibir o esquema e a regra de análise da tabela configurada	Ative Exibir esquema e regra de análise.

6. Para obter detalhes da associação de tabelas,

   a. Insira um Nome para a tabela associada.

      Você pode usar o nome padrão ou renomear essa tabela.

   b. (Opcional) Insira uma Descrição da tabela.

      A descrição ajuda a escrever consultas.

7. Especifique as permissões de Acesso ao serviço selecionando Criar e usar um novo perfil de serviço ou Usar um perfil de serviço existente.

Se você escolher...	Então...
Criar e usar um novo perfil de serviço	• AWS Clean Rooms cria uma função de serviço com a política necessária para essa tabela. • O nome do perfil de serviço padrão é `cleanrooms-<timestamp>` . • Você deve ter permissões para criar perfis e anexar políticas. • Se seus dados de entrada estiverem criptografados, você poderá seleciona r Esses dados são criptografados com uma chave KMS e, em seguida, inserir uma AWS KMS key que será usada para descriptografar sua entrada de dados.
Use um perfil de serviço existente	1. Escolha um nome do perfil de serviço existente na lista suspensa. A lista de perfis é exibida se você tiver permissões para listar funções. Se você não tiver permissões para listar perfis, insira o nome do recurso da Amazon (ARN) do perfil que você deseja usar.

Se você escolher...	Então...
	2. Veja a função de serviço escolhendo o link externo Exibir no IAM. Se não houver perfis de serviço existente s, a opção de Usar um perfil de serviço existente não estará disponível. Por padrão, AWS Clean Rooms não tenta atualizar a política de função existente para adicionar as permissões necessárias. 3. (Opcional) Marque a caixa de seleção Adicionar uma política pré-configurada com as permissões necessárias para esse perfil para adicionar as permissõe s necessárias ao perfil. Você deve ter permissões para modificar funções e criar políticas.

> **Note**
>
> - AWS Clean Rooms requer permissões para consultar de acordo com as regras de análise. Para obter mais informações sobre permissões para AWS Clean Rooms, consulteAWS políticas gerenciadas para AWS Clean Rooms.
> - Se a função não tiver permissões suficientes para AWS Clean Rooms, você receberá uma mensagem de erro informando que a função não tem permissões suficientes para AWS Clean Rooms. A política de perfil deve ser adicionada antes de continuar.
> - Se você não conseguir modificar a política de perfil, receberá uma mensagem de erro informando que AWS Clean Rooms não conseguiu encontrar a política para o perfil de serviço.

8. Se quiser habilitar Tags para o recurso de associação de tabelas configurado, escolha Adicionar nova tag e, em seguida, insira o par de Chave e Valor.
9. Escolha Associar tabela.

Próximas etapas

Agora que você associou sua tabela de dados configurada à colaboração, você está pronto para:

- Edite a colaboração, se você for o criador da colaboração
- Consulte as tabelas de dados (como um membro que pode consultar)

Configurar a política de privacidade diferencial

Esse procedimento descreve o processo de configuração da política de privacidade diferencial em uma colaboração usando a opção Fluxo guiado no AWS Clean Rooms console. Essa é uma etapa única para todas as tabelas com proteção diferencial de privacidade.

Para definir as configurações de privacidade diferencial (fluxo guiado)

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Na guia Tabelas da página de colaboração, escolha Configurar política de privacidade diferencial.
5. Na página Configurar política de privacidade diferencial, escolha valores para as seguintes propriedades:

   - Orçamento de privacidade
   - Atualizar o orçamento de privacidade mensalmente
   - Ruído adicionado por consulta

   É possível usar os valores-padrão ou inserir valores personalizados que sejam compatíveis com seu caso de uso específico. Depois de escolher os valores para Orçamento de privacidade e Ruído adicionado por consulta, você pode visualizar o utilitário resultante em termos do número de agregações possíveis em todas as consultas nos dados.
6. Selecione Configurar.

Você verá uma mensagem de confirmação de que configurou com sucesso a política de privacidade diferencial para a colaboração.

Próximas etapas

Agora que você configurou a privacidade diferencial, está tudo pronto para:

- Consulte as tabelas de dados (como um membro que pode consultar)

- Gerenciar a colaboração (se você for o criador da colaboração)

Trabalhando com modelos de análise

Os modelos de análise funcionam com Regra de análise personalizada em AWS Clean Rooms. Com um modelo de análise, você pode definir parâmetros para ajudá-lo a reutilizar a mesma consulta. AWS Clean Rooms suporta um subconjunto de parametrização com valores literais.

Os modelos de análise são específicos para colaboração. Para cada colaboração, os membros só podem ver as consultas nessa colaboração. Se você planeja usar a privacidade diferencial em uma colaboração, os modelos de análise devem ser compatíveis com a estrutura de consulta de uso geral da privacidade diferencial do AWS Clean Rooms .

Tópicos

Criar um modelo de análise

Para obter informações sobre como criar um modelo de análise usando os AWS SDKs, consulte a Referência da AWS Clean Rooms API.

Para criar um modelo de análise usando o AWS Clean Rooms console

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com o Conta da AWS que funcionará como criador da colaboração.
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Na guia Modelos, vá para a seção Modelos de análise criados por você.
5. Escolha Criar modelo de análise.
6. Na página Criar modelo de análise, em Detalhes, insira um Nome e uma Descrição opcional.
7. Para Tabelas, visualize as tabelas configuradas associadas à colaboração.
8. Para Definição,

    a. Insira a definição para o modelo de análise.

b. Escolha Importar de para importar uma definição.

c. (Opcional) Especifique um parâmetro no editor SQL inserindo dois pontos (`:`) na frente do nome do parâmetro.

   Por exemplo: .

   ```
   WHERE table1.date + :date_period > table1.date
   ```

9. Se você adicionou parâmetros anteriormente, em Parâmetros – opcional, para cada Nome de parâmetro, escolha o Tipo e o Valor padrão (opcional).
10. Se quiser habilitar Tags para o recurso de tabela configurado, escolha Adicionar nova tag e, em seguida, insira o par Chave e Valor.
11. Escolha Criar.

Agora está tudo pronto para:

- Informe ao membro da colaboração que ele pode Revisar um modelo de análise. (Opcional se quiser consultar seus próprios dados.)

Revisão de um modelo de análise

Depois que um membro da colaboração tiver criado um modelo de análise, você poderá revisá-lo e aprová-lo. Depois que o modelo de análise for aprovado, ele poderá ser consultado em AWS Clean Rooms.

Para revisar um modelo de análise usando o AWS Clean Rooms console

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com o Conta da AWS que funcionará como criador da colaboração.
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Na guia Modelos, acesse a seção Modelos de análise criados por outros membros.
5. Escolha o modelo de análise que tem o status Pode ser executado de Não requer sua revisão.
6. Escolha Revisar.
7. Revise a visão geral, a definição e os parâmetros da regra de análise (se houver).
8. Revise as tabelas configuradas listadas em Tabelas referenciadas na definição.

O Status ao lado de cada tabela exibirá Modelo não permitido.

9. Escolha uma tabela.

Se você	A seguir, escolha…
Aprovar o modelo de análise	modelo na mesa. Confirme sua aprovação escolhendo.
Não aprove o modelo de análise	Proibir

Agora você está pronto para usar o modelo de análise para consultar as tabelas de dados (como um membro que pode consultar).

Consultando tabelas configuradas usando um modelo de análise

Esse procedimento demonstra como usar um modelo de análise no AWS Clean Rooms console para consultar tabelas configuradas com a regra de análise personalizada.

Para usar um modelo de análise para consultar tabelas configuradas com a regra de análise Personalizada

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que tem o status de Suas habilidades de membro como Consulta.
4. Na guia Consultas, em Tabelas, visualize as tabelas e o tipo de regra de análise associada (Regra de análise personalizada).

> **Note**
>
> Se não estiver vendo as tabelas que espera na lista, isso pode ser pelos seguintes motivos:
>
> - As tabelas não foram associadas.
> - As tabelas não têm uma regra de análise configurada.

5. Na seção Análise, selecione o modelo de análise na lista suspensa.
6. Insira o valor dos parâmetros do modelo de análise que você deseja usar na consulta. O valor deve estar no tipo de dados especificado pelo parâmetro. Você pode usar valores diferentes sempre que executar o modelo de análise. Não há suporte para NULL valores vazios ou para o parâmetro. O uso de parâmetros na LIMIT cláusula também não é suportado.
7. Escolha Executar.

> **Note**
>
> Você não poderá executar a consulta se o membro que pode receber os resultados não tiver definido as configurações dos resultados da consulta.

8. Continue ajustando os parâmetros e execute sua consulta novamente ou escolha o botão + para iniciar uma nova consulta em uma nova guia.

Consultar dados em uma colaboração

Como membro que pode consultar, você pode realizar uma das seguintes ações:

- Criar uma consulta SQL manualmente usando o editor de código SQL.
- Use a IU do Analysis Builder para criar uma consulta sem precisar escrever código SQL.
- Use um modelo de análise aprovado.

Quando o membro que pode consultar executa uma consulta SQL nas tabelas da colaboração, AWS Clean Rooms assume as funções relevantes para acessar as tabelas em seu nome. AWS Clean Rooms aplica as regras de análise conforme necessário à consulta de entrada e sua saída.

AWS Clean Rooms oferece suporte a consultas SQL que podem ser diferentes de outros mecanismos de consulta. Para obter as especificações, consulte a AWS Clean Rooms Referência SQL. Se você quiser executar consultas em tabelas de dados protegidas com privacidade diferencial, será necessário garantir que suas consultas sejam compatíveis com a estrutura de consulta de uso geral da privacidade diferencial do AWS Clean Rooms .

> **Note**
>
> Ao usar a Computação Criptográfica para o Clean Rooms, nem todas as operações SQL geram resultados válidos. Por exemplo, você pode conduzir um COUNT em uma coluna criptografada, mas conduzir um SUM em números criptografados leva a erros. Além disso, as consultas também podem gerar resultados incorretos. Por exemplo, consultas em SUM colunas seladas produzem erros. No entanto, uma GROUP BY consulta em colunas seladas parece ter sucesso, mas produz grupos diferentes daqueles produzidos por uma GROUP BY consulta em texto não criptografado.

Os tópicos a seguir explicam como consultar dados em uma colaboração usando o console AWS Clean Rooms .

Tópicos

- Visualizar consultas recentes
- Visualizar detalhes da consulta

Para obter informações sobre como consultar dados ou visualizar consultas chamando a operação da AWS Clean Rooms `StartProtectedQuery` API diretamente ou usando os AWS SDKs, consulte a Referência da AWS Clean Rooms API.

Para ter mais informações sobre o registro de consultas, consulte Login de consulta AWS Clean Rooms.

> **Note**
>
> Se você executar uma consulta em tabelas de dados criptografadas, os resultados das colunas criptografadas serão criptografados.

Para obter mais informações sobre resultados de consultas, veja Recebimento do resultados da consulta.

Usar o editor de código SQL

Como membro que pode consultar, você pode criar uma consulta manualmente escrevendo código SQL no editor de código SQL. O editor de código SQL está localizado na seção Análise da guia Consultas no AWS Clean Rooms console.

O editor de código SQL é exibido por padrão. Se quiser usar o criador de análises para criar consultas, consulte Usar o criador de análise.

> **Important**
>
> Se você começar a escrever uma consulta SQL no editor de código e depois ativar a Interface do usuário do construtor de análises, sua consulta não será salva.

AWS Clean Rooms oferece suporte a muitos comandos, funções e condições SQL. Para obter mais informações, consulte a Referência SQL do AWS Clean Rooms.

> **Tip**
>
> Se uma manutenção programada ocorrer enquanto uma consulta estiver sendo executada, a consulta será encerrada e revertida e será necessário reiniciá-la. Você deve reiniciar a consulta.

Para criar a consulta manualmente usando o editor de código SQL

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que tem o status de Suas habilidades de membro como Consulta.
4. Na guia Consultas, vá para a seção Análise.

   > **Note**
   >
   > A seção Análise só será exibida se o membro que pode receber os resultados e o membro responsável por pagar pelos custos de computação da consulta tiverem ingressado na colaboração como membro ativo.

5. Na guia Consultas, em Tabelas, visualize a lista de tabelas e o tipo de regra de análise associada (regra de análise de agregação, regra de análise de lista ou regra de análise personalizada).

   > **Note**
   >
   > Se não estiver vendo as tabelas que espera na lista, isso pode ser pelos seguintes motivos:
   >
   > - As tabelas não foram associadas.
   > - As tabelas não têm uma regra de análise configurada.

6. (Opcional) Para visualizar os controles do esquema e da regra de análise da tabela, expanda a tabela selecionando o ícone do sinal de adição (+).
7. Crie a consulta digitando a consulta no editor de código SQL.

(Opcional) Se você deseja usar um exemplo de consulta	(Opcional) Se você deseja inserir nomes ou funções de coluna
1. Clique nos três pontos verticais ao lado da tabela. 2. Em Inserir no editor, escolha Exemplo de consulta. **Note** A inserção de uma consulta de exemplo acrescenta a consulta que já está no editor. O exemplo de consulta é exibido. Todas as tabelas listadas em Tabelas estão incluídas na consulta. 3. Edite os valores do espaço reservado na consulta.	1. Selecione os três pontos verticais ao lado de uma coluna. 2. Em Inserir no editor, escolha Nome da coluna. 3. Para inserir manualmente uma função permitida em uma coluna, selecione os três pontos verticais ao lado de uma coluna, selecione Inserir no editor e, em seguida, selecione o nome da função permitida (como INNER JOIN, SUM, SUM DISTINCT ou COUNT). 4. Pressione Ctrl + Espaço para visualizar os esquemas da tabela no editor de código. **Note** Os membros que podem consultar podem visualizar e usar as colunas de partição em cada associação de tabela configurada. Certifique-se de que a coluna de partição esteja rotulada como uma coluna de partição na AWS Glue tabela

(Opcional) Se você deseja usar um exemplo de consulta	(Opcional) Se você deseja inserir nomes ou funções de coluna
	subjacente à tabela configurada. 5. Edite os valores do espaço reservado na consulta.

8. Escolha Executar.

> **Note**
>
> Você não poderá executar a consulta se o membro que pode receber os resultados não tiver definido as configurações dos resultados da consulta.

9. Continue ajustando os parâmetros e execute sua consulta novamente ou escolha o botão + para iniciar uma nova consulta em uma nova guia.

> **Note**
>
> AWS Clean Rooms visa fornecer mensagens de erro claras. Se uma mensagem de erro não tiver detalhes suficientes para ajudá-lo a solucionar o problema, entre em contato com a equipe da conta. Forneça a eles uma descrição de como o erro ocorreu e a mensagem de erro (incluindo quaisquer identificadores). Para ter mais informações, consulte Solução de problemas AWS Clean Rooms.

Usar o criador de análise

Você pode usar o criador de análises para criar consultas sem precisar escrever código SQL. Com o criador de análises, você pode criar uma consulta para uma colaboração que tenha:

- Uma única tabela que usa a regra de análise de agregação sem a necessidade de JOIN
- Duas tabelas (uma de cada membro) que usam a regra de análise de agregação
- Duas tabelas (uma de cada membro) que usam a regra de análise de lista

- Duas tabelas (uma de cada membro) que usam a regra de análise de agregação e duas tabelas (uma de cada membro) que usam a regra de análise de lista

Se quiser escrever consultas SQL manualmente, consulte Usar o editor de código SQL.

O criador de análises aparece como a opção de IU do Analysis builder na seção Análise da guia Consultas no console AWS Clean Rooms .

> **Important**
>
> Se você ativar a Interface do usuário do construtor de análises, começar a criar uma consulta no construtor de análises e, depois, desativar a Interface do usuário do construtor de análises, sua consulta não será salva.

> **Tip**
>
> Se uma manutenção programada ocorrer enquanto uma consulta estiver sendo executada, a consulta será encerrada e revertida. Você deve reiniciar a consulta.

Os tópicos a seguir explicam como usar o analysis builder (criador de análise).

Tópicos

- Use o analysis builder para consultar uma única tabela (agregação)
- Use o construtor de análise para consultar duas tabelas (agregação ou lista)

Use o analysis builder para consultar uma única tabela (agregação)

Esse procedimento demonstra como usar a interface do usuário do Analysis Builder no AWS Clean Rooms console para criar uma consulta. A consulta é para uma colaboração que tem uma única tabela que usa a regra de análise de agregação sem JOIN necessidade.

Para usar o analysis builder para consultar uma única tabela

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.

3. Escolha a colaboração que tem o status de Suas habilidades de membro como Consulta.
4. Na guia Consultas, em Tabelas, visualize a tabela e o tipo de regra de análise associada. (O tipo de regra de análise deve ser a regra de análise de agregação.)

> **Note**
>
> Se não estiver vendo a tabela que espera, isso pode ser pelos seguintes motivos:
>
> - A tabela não foi associada.
> - A tabela não tem uma regra de análise configurada.

5. Na seção Análise, ative a IU do Analysis Builder.
6. Crie uma consulta.

   Se quiser ver todas as métricas de agregação, vá para a etapa 9.

   a. Em Escolher métricas, revise as métricas agregadas que foram pré-selecionadas por padrão e remova qualquer métrica, se necessário.

   b. (Opcional) Em Adicionar segmentos – opcional, escolha um ou mais parâmetros.

   > **Note**
   >
   > Adicionar segmentos – opcional só é exibido se as dimensões forem especificadas para a tabela.

   c. (Opcional) Em Adicionar filtros – opcional, escolha Adicionar filtro e, em seguida, escolha um parâmetro, operador e valor.

   Para adicionar mais filtros, escolha Adicionar outro filtro.

   Para remover um filtro, selecione Remover.

   > **Note**
   >
   > ORDER BY não é compatível com consultas de agregação.
   > Somente o operador AND é compatível com filtros.

   d. (Opcional) Em Adicionar descrição – opcional, insira uma descrição para ajudar a identificar a consulta na lista de consultas.

7. Expanda Visualizar código SQL.

   a. Visualize o código SQL que é gerado a partir do criador de análise.

   b. Para copiar o código SQL, escolha Copiar.

   c. Para editar o código SQL, escolha Editar no editor de código SQL.

8. Escolha Executar.

> **Note**
>
> Você não poderá executar a consulta se o membro que pode receber os resultados não tiver definido as configurações dos resultados da consulta.

9. Continue ajustando os parâmetros e execute sua consulta novamente ou escolha o botão + para iniciar uma nova consulta em uma nova guia.

> **Note**
>
> AWS Clean Rooms visa fornecer mensagens de erro claras. Se uma mensagem de erro não tiver detalhes suficientes para ajudá-lo a solucionar o problema, entre em contato com a equipe da conta. Forneça a eles uma descrição de como o erro ocorreu e a mensagem de erro (incluindo quaisquer identificadores). Para ter mais informações, consulte Solução de problemas AWS Clean Rooms.

Use o construtor de análise para consultar duas tabelas (agregação ou lista)

Este procedimento descreve como usar o criador de análise no AWS Clean Rooms console para criar uma consulta para uma colaboração que tenha:

- Duas tabelas (uma de cada membro) que usam a regra de análise de agregação
- Duas tabelas (uma de cada membro) que usam a regra de análise de lista
- Duas tabelas (uma de cada membro) que usam a regra de análise de agregação e duas tabelas (uma de cada membro) que usam a regra de análise de lista

Para usar o analysis builder para consultar duas tabelas

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que tem o status de Suas habilidades de membro como Consulta.
4. Na guia Consultas, em Tabelas, visualize as duas tabelas e o tipo de regra de análise associada (regra de análise de agregação ou regra de análise de lista).

> **Note**
>
> Se não estiver vendo as tabelas que espera na lista, isso pode ser pelos seguintes motivos:
>
> - As tabelas não foram associadas.
> - As tabelas não têm uma regra de análise configurada.

5. Na seção Análise, ative a IU do Analysis Builder.
6. Crie uma consulta.

   Se a colaboração contiver duas tabelas que usam a regra de análise de agregação e duas tabelas que usam a regra de análise de lista, primeiro escolha Agregação ou Lista e, em seguida, siga as instruções com base na regra de análise selecionada.

Se as duas tabelas usarem a regra de análise de agregação	Se as duas tabelas usarem a regra de análise de lista
1. Em Escolher métricas, revise as métricas agregadas que foram pré-selecionadas por padrão e remova qualquer métrica, se necessário. 2. Para Match records, escolha um ou mais registros.	1. Em Escolher atributos, revise os atributos da lista que foram pré-selecionados por padrão e remova qualquer métrica, se necessário. 2. Para Match records, escolha um ou mais registros.

Se as duas tabelas usarem a regra de análise de agregação	Se as duas tabelas usarem a regra de análise de lista
Note Ao usar o criador de análise, você pode combinar somente em um único par de colunas.	**Note** Ao usar o criador de análise, você pode combinar somente em um único par de colunas.
3. (Opcional) Em Adicionar segmentos – opcional, escolha um ou mais parâmetros.	3. (Opcional) Em Adicionar filtros – opcional, escolha Adicionar filtro e escolha um parâmetro, operador e valor. Para adicionar mais filtros, escolha Adicionar outro filtro. Para remover um filtro, selecione Remover.
Note Adicionar segmentos – opcional só é exibido se as dimensões forem especificadas para a tabela.	**Note** LIMIT não é compatíve l com listas de consultas. Somente o operador AND é compatível com filtros.
4. (Opcional) Em Adicionar filtros – opcional, escolha Adicionar filtro e escolha um parâmetro, operador e valor. Para adicionar mais filtros, escolha Adicionar outro filtro. Para remover um filtro, selecione Remover.	4. (Opcional) Em Adicionar descrição – opcional, insira uma descrição para ajudar a identificar a consulta na lista de consultas recentes.
Note ORDER BY não é compatível com	

Se as duas tabelas usarem a regra de análise de agregação	Se as duas tabelas usarem a regra de análise de lista
consultas de agregação . Somente o operador AND é compatível com filtros. 5. (Opcional) Em Adicionar descrição – opcional, insira uma descrição para ajudar a identificar a consulta na lista de consultas recentes.	

7. Expanda Visualizar código SQL.
   a. Visualize o código SQL que é gerado a partir do criador de análise.
   b. Para copiar o código SQL, escolha Copiar.
   c. Para editar o código SQL, escolha Editar no editor de código SQL.
8. Escolha Executar.

> **Note**
>
> Você não poderá executar a consulta se o membro que pode receber os resultados não tiver definido as configurações dos resultados da consulta.

9. Continue ajustando os parâmetros e execute sua consulta novamente ou escolha o botão + para iniciar uma nova consulta em uma nova guia.

> **Note**
>
> AWS Clean Rooms visa fornecer mensagens de erro claras. Se uma mensagem de erro não tiver detalhes suficientes para ajudá-lo a solucionar o problema, entre em contato com a equipe da conta. Forneça a eles uma descrição de como o erro ocorreu e a mensagem de

erro (incluindo quaisquer identificadores). Para ter mais informações, consulte Solução de problemas AWS Clean Rooms.

Consultar dados com privacidade diferencial

Em geral, escrever e executar consultas não muda quando a privacidade diferencial é ativada. No entanto, você não poderá executar uma consulta se não houver orçamento de privacidade suficiente restante. Ao executar consultas e consumir o orçamento de privacidade, você pode ver aproximadamente quantas agregações podem ser executadas e como isso pode afetar futuras consultas.

Para ver o impacto da privacidade diferencial em uma colaboração

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração que tem o status Seus detalhes de membro de Executar consultas.
4. Na guia Consultas, em Tabelas, veja o orçamento de privacidade restante. Isso é exibido como o número estimado de funções de agregação restantes e Utilidade usada (renderizada como uma porcentagem).

   > **Note**
   >
   > O número estimado de funções agregadas restantes e a porcentagem de Utilidade usada exibidos somente para o membro que pode consultar.

5. Escolha Veja o impacto para ver quanto ruído é injetado nos resultados e aproximadamente quantas funções de agregação você pode executar.

Visualizar consultas recentes

Você pode ver as consultas que foram executadas nos últimos 90 dias na guia Consultas recentes.

> **Note**
>
> Se sua única habilidade de membro for Contribuir com dados e você não for o membro que pagará pelos custos de computação da consulta, a guia Consultas não aparecerá no console.

Para visualizar consultas recentes

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha uma colaboração.
4. Na guia Consultas, em Consultas, visualize as consultas que foram executadas nos últimos 90 dias.
5. Para classificar consultas recentes por status, selecione um status na lista suspensa Todos os status.

   Os status são: Enviado, Iniciado, Cancelado, Sucesso, Falha e Expirado.

Visualizar detalhes da consulta

Você pode ver os detalhes da consulta como o membro que pode executar consultas ou como um membro que pode receber resultados.

Para visualizar detalhes da consulta

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha uma colaboração.
4. Na guia Consultas, faça o seguinte:

   - Escolha o botão ao lado do host que você deseja visualizar e escolha Visualizar detalhes.
   - Escolha a ID de consulta protegida.
5. Na página de detalhes da consulta,

- Se você for o membro que pode executar consultas, visualize os detalhes da consulta, o texto SQL e os resultados.

  Você vê uma mensagem confirmando que os resultados da consulta foram entregues ao membro que pode receber os resultados.
- Se você for o membro que pode receber os resultados, veja os detalhes da consulta e os resultados.

Recebimento do resultados da consulta

Como membro que pode receber resultados, você pode receber a saída da consulta AWS Clean Rooms no bucket do Amazon S3 que você especificou quando ingressou na colaboração.

Os tópicos a seguir explicam como receber resultados da consulta usando o console AWS Clean Rooms.

Tópicos

- Receber resultados da consulta
- Editar valores padrão para as configurações dos resultados da consulta
- Usar a saída da consulta em outros Serviços da AWS

Para obter informações sobre como consultar dados ou visualizar consultas chamando a AWS Clean Rooms API diretamente ou usando os SDKs AWS, consulte a AWS Clean Rooms Referência da API.

Para ter mais informações sobre o registro em log de consultas, consulte Login de consulta AWS Clean Rooms.

> **Note**
>
> Se você executar uma consulta em tabelas de dados criptografadas, os resultados das colunas criptografadas serão criptografados.

Receber resultados da consulta

Os resultados da consulta estão localizados na seção Padrões de configurações de resultados da consulta e na seção Consultas da guia Consultas no console AWS Clean Rooms.

Para receber resultados da consulta

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que tem o status de Suas habilidades de membro de Receber resultados.

4. Para receber os resultados da consulta diretamente de AWS Clean Rooms, na guia Consultas, em Consultas, na coluna ID da consulta protegida, selecione a consulta.
5. Na página Detalhes da consulta, em Resultados, faça o seguinte:

Se você deseja…	A seguir, escolha…
Copie os resultados.	Copiar
Fazer download dos resultados.	Baixar **Note** Por padrão, o nome do arquivo baixado é o correspondente a `Query id` exibido quando a consulta foi executada em AWS Clean Rooms.
Visualizar os resultados no Amazon S3.	Exibir no Amazon S3 O console do Amazon S3 é aberto em uma guia separada.

6. Se você estiver usando dados criptografados, agora você pode descriptografar as tabelas de dados.

   Para obter mais informações, consulte Descriptografando tabelas de dados com o cliente de criptografia C3R.

Editar valores padrão para as configurações dos resultados da consulta

Como membro que pode receber resultados, você pode editar os valores padrão das configurações dos resultados da consulta no console AWS Clean Rooms.

Para editar os valores padrão para as configurações dos resultados da consulta

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que tem o status de Suas habilidades de membro de Receber resultados.
4. Na guia Consultas, em Configurações de resultados da consulta, escolha Editar.
5. Na página Editar padrões das configurações dos resultados da consulta, modifique qualquer um dos itens a seguir, conforme necessário:

   a. Em Configurações de resultados da consulta, modifique o destino dos resultados no Amazon S3 ou o formato do Resultado.
   b. Em Acesso ao serviço, modifique o Método para autorizar AWS Clean Rooms a gravação no bucket e no formato do Amazon S3 que você especificou.

   As configurações dos resultados da consulta atualizadas aparecem na página de detalhes da colaboração.

Usar a saída da consulta em outros Serviços da AWS

A saída da consulta AWS Clean Rooms está disponível no console (se o console for usado para executar consultas) e é baixada em um bucket específico do Amazon S3. A partir daí, você pode usar a saída da consulta em outros Serviços da AWS, como o Amazon QuickSight e o Amazon SageMaker, dependendo de como esses serviços usam dados do Amazon S3.

Para obter mais informações sobre o Amazon QuickSight, consulte a documentação do Amazon QuickSight.

Para mais informações sobre o Amazon SageMaker, consulte a documentação do Amazon SageMaker.

Descriptografando tabelas de dados com o cliente de criptografia C3R

Siga este procedimento para colaborações que usam Computação Criptográfica Clean Rooms e o cliente de criptografia C3R para criptografar tabelas de dados. Use esse procedimento depois de consultar os dados na colaboração.

A chave secreta compartilhada e o ID de colaboração são necessários para esse procedimento.

O membro que pode receber os resultados decodifica os dados usando a mesma chave secreta compartilhada e ID de colaboração que foram usadas para criptografar os dados da colaboração.

> **Note**
>
> As colaborações AWS Clean Rooms já limitam quem pode realizar e visualizar os resultados da consulta. Para realizar a descriptografia, quem tem acesso a esses resultados precisa da mesma chave secreta compartilhada e ID de colaboração que foram usadas para criptografar os dados.

Para descriptografar uma tabela de dados criptografados

1. (Opcional) Visualize os comandos disponíveis no cliente de criptografia C3R.
2. (Opcional) Navegue até o diretório desejado e execute `ls` (macOS) ou `dir` (Windows).
   - Verifique se o arquivo c3r-cli.jar e o arquivo de dados criptografados dos resultados da consulta estão no diretório desejado.

     > **Note**
     >
     > Se os resultados da consulta forem baixados da interface do console AWS Clean Rooms, provavelmente estão na pasta Downloads da sua conta de usuário. (Por exemplo, a pasta Downloads em seu diretório de usuário em Windows e macOS.) Recomendamos que você mova o arquivo de resultados da consulta para a mesma pasta do c3r-cli.jar.

3. Armazene a chave secreta compartilhada na variável do ambiente `C3R_SHARED_SECRET`. Para obter mais informações, consulte Etapa 6: armazenar a chave secreta compartilhada em uma variável de ambiente.
4. A partir de AWS Command Line Interface (AWS CLI), execute o seguinte comando.

   java -jar c3r-cli.jar decrypt ***<name of input .csv file>*** --id=***<collaboration id>*** --output=***<output file name>***
5. Substitua cada *espaço reservado de entrada do usuário* por suas próprias informações:

   a. Para `id=`, insira o ID da colaboração.

   b. Para `output=`, insira o nome do arquivo de saída (por exemplo, `results-decrypted.csv`).

      Se você não especificar um nome de saída, um nome padrão será exibido no terminal.

   c. Visualize os dados descriptografados no arquivo de saída especificado usando seu CSV ou aplicativo de visualização Parquet preferido (como um editor de texto Microsoft Excel ou outro aplicativo).

Gerenciando AWS Clean Rooms

Os tópicos a seguir descrevem como gerenciar uma colaboração, membros e tabelas configuradas AWS Clean Rooms usando o AWS Clean Rooms console.

Para obter informações sobre como gerenciar o AWS Clean Rooms uso dos AWS SDKs, consulte a Referência da AWS Clean Rooms API.

Tópicos

Gerenciando colaborações no AWS Clean Rooms

Os tópicos a seguir descrevem como o criador da colaboração pode gerenciar uma colaboração AWS Clean Rooms usando o console AWS Clean Rooms.

Para obter informações sobre como gerenciar uma colaboração usando os SDKs AWS, consulte a AWS Clean Rooms Referência da API.

Tópicos

- Excluir uma política de privacidade diferencial
- Visualizar os parâmetros de privacidade diferencial calculados

Editar colaborações

Saiba como editar as diferentes partes de uma colaboração.

Tópicos

- Editar nome e descrição da colaboração
- Editar tags de colaboração
- Editar tags de associação
- Editar tags de tabela associadas
- Editar tags do modelo de análise
- Editar tags de política de privacidade diferencial

Editar nome e descrição da colaboração

Depois de criar a colaboração, você só pode editar o nome e a descrição da colaboração.

> **Note**
>
> Se você habilitou os Logs de consultas, você pode editar se os logs de consulta estão armazenados na sua conta do Amazon CloudWatch Logs.

Para editar o nome e a descrição da colaboração

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que você criou.
4. Na página de detalhes da colaboração, escolha Ações e, em seguida, escolha Editar colaboração.
5. Para Detalhes, edite o nome e a descrição da colaboração.

6. Escolha Salvar alterações.

Editar tags de colaboração

Como criador de colaboração, depois de criar uma colaboração, você pode gerenciar as tags no recurso de colaboração.

Para editar as tags de colaboração

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que você criou.
4. Escolha uma das seguintes opções:

Se você é...	Então ...
Um membro da colaboração	Escolha a guia Detalhes.
O criador da colaboração, mas não um membro da colaboração	Role para baixo até a seção Tags da página.

5. Para obter detalhes da colaboração, escolha Gerenciar tags.
6. Na página Gerenciar tags é possível fazer o seguinte:

   - Para remover uma tag, selecione Remover.
   - Para adicionar uma tag, escolha Adicionar nova tag.
   - Para salvar suas alterações, escolha Salvar alterações

Editar tags de associação

Como criador de colaboração, depois de criar uma colaboração, você pode gerenciar as tags no recurso de associação.

Para editar as tags de associação

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).

2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que você criou.
4. Escolha a guia Detalhes.
5. Em Detalhes da associação, selecione Gerenciar tags.
6. Na página Gerenciar tags é possível fazer o seguinte:

   - Para remover uma tag, selecione Remover.
   - Para adicionar uma tag, escolha Adicionar nova tag.
   - Para salvar suas alterações, escolha Salvar alterações.

Editar tags de tabela associadas

Como criador de colaboração, depois de associar tabelas a uma colaboração, você pode gerenciar as tags no recurso de tabela associado.

Para editar as tags de tabela associadas

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que você criou.
4. Escolha a guia Tabelas.
5. Para Tabelas associadas por você, escolha uma tabela.
6. Na página de detalhes da tabela configurada, em Tags, escolha Gerenciar tags.

   Na página Gerenciar tags é possível fazer o seguinte:

   - Para remover uma tag, selecione Remover.
   - Para adicionar uma tag, escolha Adicionar nova tag.
   - Para salvar suas alterações, escolha Salvar alterações.

Editar tags do modelo de análise

Como criador de colaboração, depois de criar uma colaboração, você pode gerenciar as tags no atributo do modelo de análise.

Para editar as tags de associação

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que você criou.
4. Escolha a guia Modelos.
5. Na seção Modelos de análise criados por você, escolha o modelo de análise.
6. Na página de detalhes da tabela do modelo de análise, role para baixo até a seção Tags.
7. Selecione Gerenciar tags.
8. Na página Gerenciar tags é possível fazer o seguinte:
   - Para remover uma tag, selecione Remover.
   - Para adicionar uma tag, escolha Adicionar nova tag.
   - Para salvar suas alterações, escolha Salvar alterações.

Editar tags de política de privacidade diferencial

Como criador de colaboração, depois de criar uma colaboração, você pode gerenciar as tags no atributo do modelo de análise.

Para editar as tags de associação

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração que contém a política de privacidade diferencial que você deseja editar.
4. Escolha a guia Tabelas.
5. Na guia Tabelas, selecione Gerenciar tags.
6. Na página Gerenciar tags é possível fazer o seguinte:
   - Para remover uma tag, selecione Remover.
   - Para adicionar uma tag, escolha Adicionar nova tag.
   - Para salvar suas alterações, escolha Salvar alterações.

Excluindo colaborações

Como criador de colaborações, você pode excluir uma colaboração que você criou.

> **Note**
>
> Ao excluir uma colaboração, você e todos os membros não poderão executar consultas, receber resultados ou contribuir com dados. Cada membro da colaboração continua a ter acesso aos seus próprios dados como parte de sua associação.

Para excluir uma colaboração

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que você deseja atualizar ou excluir.
4. Em Ações, escolha Excluir colaboração.
5. Confirme a exclusão e escolha Excluir.

Visualizando colaborações

Como criador de colaborações, você pode ver todas as colaborações que criou.

Para ver as colaborações

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Na página Colaborações, em Última utilização, veja as últimas 5 colaborações usadas.
4. Na guia Com associação ativa, veja a lista de colaborações com associação ativa.

   Você pode classificar por nome, data de criação da associação e detalhes do seu membro.

   É possível usar a barra de Pesquisa para procurar uma colaboração.
5. Na guia Disponível para participar, veja a lista de colaborações disponíveis para participar.

6. Na guia Não mais disponível, visualize a lista de colaborações excluídas e associações para colaborações que não estão mais disponíveis (associações removidas).

Visualização de tabelas e regras de análise

Para visualizar tabelas associadas às regras de colaboração e análise

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Escolha a guia Tabelas.
5. Escolha uma das seguintes opções:
    a. Para visualizar suas tabelas associadas na colaboração, em Tabelas associadas por você, escolha uma tabela (texto azul).
    b. Para visualizar outras tabelas associadas à colaboração, em Tabelas associadas por colaboradores, escolha uma tabela (texto azul).
6. Veja os detalhes da tabela e as regras de análise na página de detalhes da tabela.

Visualizar logs de uso de privacidade diferencial

Como membro da colaboração que protege dados com privacidade diferencial, depois de criar uma colaboração com privacidade diferencial, você pode monitorar o uso do orçamento de privacidade.

Para ver quantas agregações foram executadas e quanto do orçamento de privacidade foi usado

1. Faça login no AWS Management Console e abra o console AWS Clean Rooms com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Escolha a guia Tabelas.
5. Escolha Visualizar logs de uso (texto em azul).
6. Veja os detalhes de uso, incluindo o orçamento de privacidade e a quantidade de utilitário fornecida.

Monitorar o status do membro

Como criador da colaboração, depois de criar uma colaboração, você pode monitorar o status de todos os membros na guia Membros.

Para verificar o status de um membro

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que você criou.
4. Escolha a guia Membros.
5. Veja o status de membro de cada membro.

Remoção de um membro de uma colaboração

> **Note**
>
> A remoção de um membro também remove todos os conjuntos de dados associados da colaboração.

Como remover um membro de uma colaboração

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, selecione Colaborações.
3. Escolha a colaboração que você criou.
4. Escolha a guia Membros.
5. Selecione o botão de opção ao lado do membro a ser removido.

   > **Note**
   >
   > Um criador de colaboração não pode escolher seu próprio ID de conta.

6. Escolha Remover.

7. Na caixa de diálogo, confirme a decisão de remover o membro digitando **`confirm`** no campo de entrada de texto.

> **Note**
>
> Se você remover o membro que está pagando pelos custos de computação da consulta, nenhuma outra consulta poderá ser executada na colaboração.

Saindo de uma colaboração

Como membro da colaboração, você pode sair de uma colaboração excluindo sua associação. Se você for o criador da colaboração, só poderá sair de uma colaboração excluindo a colaboração.

> **Note**
>
> Ao excluir sua associação, você sai da colaboração e não pode voltar a participar dela. Se você for o membro que está pagando pelos custos de computação da consulta e excluir sua associação, não será permitida a execução de mais consultas.

Para deixar uma colaboração

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Em Com associação ativa, escolha a colaboração da qual você é membro.
4. Escolha Ações.
5. Escolha Excluir associação.
6. Na caixa de diálogo, confirme a decisão de sair da colaboração digitando no campo de entrada de texto e, **`confirm`** em seguida, escolha Esvaziar e excluir associação.

   Você vê uma mensagem no console indicando que a associação foi excluída.

   O criador da colaboração vê o status do Membro como Saiu.

Editar associações de tabelas configuradas

Como membro da colaboração, você pode editar as associações de tabelas configuradas que você criou.

Para editar associações de tabelas configuradas

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Escolha a guia Tabelas.
5. Para Tabelas associadas por você, escolha uma tabela.
6. Na página de detalhes da tabela, role para baixo para ver os detalhes da associação da tabela.
7. Selecione a opção Editar.
8. Na página Editar associações de tabelas configuradas, atualize a Descrição ou as informações de acesso ao serviço.
9. Escolha Salvar alterações.

Desassociação de tabelas configuradas

Como membro da colaboração, você pode desassociar uma tabela configurada da colaboração. Essa ação impede que o membro que pode consultar consulte a tabela.

Como desassociar uma tabela configurada

1. Faça logon no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Escolha a guia Tabelas.
5. Em Tabelas associadas por você, selecione o botão de opção ao lado da tabela que você deseja desassociar.
6. Escolha Desassociar.

7. Na caixa de diálogo, confirme a decisão de desassociar a tabela configurada e impedir o membro que pode consultar a tabela escolhendo Desassociar.

Editar uma política de privacidade diferencial

A qualquer momento após configurar a política de privacidade diferencial, você pode atualizá-la para refletir melhor suas necessidades de privacidade.

Para editar a política de privacidade diferencial

1. Faça login no AWS Management Console e abra o console AWS Clean Rooms com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Na guia Tabelas da página de colaboração, em Tabelas associadas por você, escolha Editar.
5. Na página Editar privacidade diferencial, escolha novos valores para as seguintes propriedades:

   - Orçamento de privacidade: mova a barra deslizante para aumentar ou diminuir o orçamento a qualquer momento durante uma colaboração. Você não poderá diminuir o orçamento depois que o membro que pode consultar tiver começado a consultar seus dados. Se o Orçamento de privacidade for aumentado, o AWS Clean Rooms continuará usando o orçamento existente até que seja totalmente consumido antes de utilizar o orçamento de privacidade recém-adicionado.
   - Ruído adicionado por consulta: mova a barra deslizante para aumentar ou diminuir o ruído adicionado por consulta a qualquer momento durante uma colaboração.

   > **Note**
   >
   > É possível escolher exemplos interativos para explorar como os diferentes valores de Orçamento de privacidade e Ruído adicionado por consulta afetam o número de funções agregadas que você pode executar.

   Não é possível alterar o valor da Atualização do orçamento de privacidade. Para alterar a seleção, você deverá excluir a política de privacidade diferencial e criar outra.
6. Escolha Save changes (Salvar alterações).

Você verá uma mensagem de confirmação de que editou com sucesso a política de privacidade diferencial.

Excluir uma política de privacidade diferencial

É possível excluir a política de privacidade diferencial na guia Tabelas de uma colaboração.

Para excluir a política de privacidade diferencial

1. Faça login no AWS Management Console e abra o console AWS Clean Rooms com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Na guia Tabelas da página de colaboração, ao lado de Política de privacidade diferencial, selecione Excluir.
5. Se você tiver certeza de que deseja excluir a política de privacidade diferencial, escolha Excluir.

Depois de excluir uma política de privacidade diferencial, você não poderá acessar os logs de uso do orçamento de privacidade dessa política. Tabelas com privacidade diferencial ativada não poderão ser consultadas se a política de privacidade diferencial for excluída.

Visualizar os parâmetros de privacidade diferencial calculados

Para usuários com experiência em privacidade diferencial, você pode visualizar os parâmetros de privacidade diferencial calculados na guia Consultas de uma colaboração.

Para visualizar os parâmetros de privacidade diferencial calculados

1. Faça login no AWS Management Console e abra o console AWS Clean Rooms com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação à esquerda, escolha Colaborações.
3. Escolha a colaboração.
4. Na guia Consultas, na seção Resultados, selecione Visualizar parâmetros de privacidade diferencial calculados.

Na tabela de Parâmetros de privacidade diferencial calculados, você pode ver os valores de sensibilidade das funções agregadas, que são definidos como o valor máximo pelo qual o resultado

de uma função pode mudar se os registros de um único usuário forem adicionados, removidos ou modificados. A lista inclui os seguintes parâmetros de privacidade diferencial:

- O Limite de contribuição do usuário (UCL) é o número máximo de linhas contribuídas por um usuário em uma consulta SQL. Por exemplo, se você quiser contar o número total de impressões correspondentes em uma campanha específica em que cada usuário pode ter várias impressões, a privacidade diferencial do AWS Clean Rooms precisa limitar o número de impressões de um único usuário para garantir que o cálculo da privacidade diferencial seja preciso. Em outras palavras, se algum usuário tiver mais impressões do que o limite, o AWS Clean Rooms pegará automaticamente uma amostra aleatória uniforme das impressões desse usuário de acordo com o valor calculado de UCL e excluirá as impressões restantes desse usuário ao executar a consulta. O valor de UCL será igual a 1 se você estiver contando o número de usuários exclusivos. Isso ocorre porque adicionar, remover ou modificar um único usuário pode alterar a contagem de usuários distintos em no máximo 1.
- Valor mínimo é o limite inferior de uma expressão usada em uma função agregada, como `sum()`. Por exemplo, se a expressão for uma coluna conhecida como `purchase_value`, o valor mínimo será o limite inferior da coluna.
- Valor máximo é o limite superior de uma expressão usada em uma função agregada, como `sum()`. Por exemplo, se a expressão for uma coluna conhecida como `purchase_value`, o valor máximo será o limite superior da coluna.

Na tabela Parâmetros de privacidade diferencial calculados, você pode usar esses parâmetros para entender melhor a quantidade total de ruído nos resultados da consulta. Por exemplo, quando o Ruído adicionado por consulta configurado é de 30 usuários e uma consulta `COUNT DISTINCT (user_id)` é executada, a privacidade diferencial do AWS Clean Rooms adiciona um ruído aleatório que fica entre -30 e 30 com alta probabilidade porque a sensibilidade de `COUNT DISTINCT` é 1. No caso de uma consulta `COUNT` com a mesma configuração, a privacidade diferencial AWS Clean Rooms adiciona ruído estatístico que é escalado pelo limite de contribuição do usuário, pois um único usuário pode contribuir com várias linhas para o resultado da consulta. No caso de uma consulta `SUM` como `SUM (purchase_value)` em que todos os valores da coluna são positivos, o ruído total é escalado pelo limite de contribuição do usuário multiplicado pelo valor máximo. AWS Clean Rooms A privacidade diferencial calcula automaticamente os parâmetros de sensibilidade para realizar a adição de ruído no tempo de execução da consulta e esgota o orçamento de privacidade. O esgotamento do orçamento de privacidade é necessário porque os parâmetros de sensibilidade dependem dos dados.

Gerenciando tabelas configuradas no AWS Clean Rooms

Os tópicos a seguir descrevem como gerenciar tabelas configuradas AWS Clean Rooms usando o AWS Clean Rooms console.

Para obter informações sobre como gerenciar tabelas configuradas usando os AWS SDKs, consulte a Referência da AWS Clean Rooms API.

Tópicos

Editar detalhes da tabela configurada

Como membro da colaboração, você pode editar os detalhes da tabela configurada.

Para editar detalhes da tabela configurada

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. Selecione a tabela configurada que você criou.
4. Na página de detalhes da tabela configurada, role para baixo até Detalhes da tabela configurada.
5. Selecione a opção Editar.
6. Atualize o Nome ou a Descrição da tabela configurada.
7. Escolha Salvar alterações.

Editar tags de tabela configuradas

Como membro da colaboração, depois de criar uma tabela configurada, você pode gerenciar as tags no recurso de tabela configurada na guia Tabelas configuradas.

Para editar as tags de tabela configurada

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. Selecione a tabela configurada que você criou.
4. Na página de detalhes da tabela configurada, role para baixo até a seção Tags.
5. Selecione Gerenciar tags.
6. Na página Gerenciar tags é possível fazer o seguinte:
   - Para remover uma tag, selecione Remover.
   - Para adicionar uma tag, escolha Adicionar nova tag.
   - Para salvar suas alterações, escolha Salvar alterações.

Editar a regra de análise de tabela configurada

Para editar a regra de análise de tabela configurada

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. Selecione a tabela configurada que você criou.
4. Na página de detalhes da tabela configurada, role para baixo até a seção Regra de análise de agregação, Regra de análise de lista ou Regra de análise personalizada. (Sua escolha depende do tipo de regra de análise que você escolheu para a tabela configurada.)
5. Selecione a opção Editar.
6. Na página Editar regra de análise, você pode:
   - Modificar a definição da regra de análise da seguinte forma:
     - Modificar o editor de JSON.
     - Escolha Importar do arquivo para carregar uma nova definição de regra de análise.
   - Visualize o que os membros verão em uma colaboração selecionando uma das seguintes opções:
     - Visualização da tabela

- JSON
- Consulta de exemplo

7. Escolha Salvar alterações para salvar suas alterações.

Excluir a regra de análise de tabela configurada

> **Warning**
>
> Essa ação não pode ser desfeita e afeta todos os recursos relacionados.

Para excluir a regra de análise de tabela configurada

1. Faça login no AWS Management Console e abra o AWS Clean Rooms console com seu Conta da AWS (se ainda não tiver feito isso).
2. No painel de navegação esquerdo, escolha Tabelas configuradas.
3. Selecione a tabela configurada que você criou.
4. Na página de detalhes da tabela configurada, role para baixo até a seção Regra de análise de agregação, Regra de análise de lista ou Regra de análise personalizada. (Sua escolha depende do tipo de regra de análise que você escolheu para a tabela configurada.)
5. Escolha Excluir.
6. Se você tiver certeza de que deseja excluir a regra de análise, escolha Excluir.

Solução de problemas AWS Clean Rooms

Esta seção descreve alguns problemas comuns que podem surgir durante o uso AWS Clean Rooms e como corrigi-los.

Problemas

Uma ou mais tabelas referenciadas pela consulta não podem ser acessadas pelo perfil de serviço associado. O proprietário da tabela/perfil deve conceder acesso de perfil de serviço à tabela.

- Verifique se as permissões para o perfil de serviço estão configuradas conforme necessário. Para obter mais informações, consulte Conf AWS Clean Rooms iguração.

Um dos conjuntos de dados subjacentes tem um formato de arquivo incompatível.

- Certifique-se de que seu conjunto de dados esteja em um dos formatos de arquivo compatíveis:
  - Parquet
  - RCFile
  - TextFile
  - SequenceFile
  - RegexSerde
  - OpenCSV
  - AVRO
  - JSON

Para ter mais informações, consulte Formatos de dados para AWS Clean Rooms.

Os resultados de consulta não são os esperados ao usar a computação criptográfica para o Clean Rooms.

Se você estiver usando Computação Criptográfica para o Clean Rooms (C3R), verifique se sua consulta usa colunas criptografadas corretamente:

- As colunas sealed são usadas somente em cláusulas SELECT.
- As colunas fingerprint são usadas somente em cláusulas JOIN (e cláusulas GROUP BY sob certas condições).
- Que você só tem colunas JOINing fingerprint com o mesmo nome se as configurações de colaboração exigirem isso.

Para ter mais informações, consulte Computação criptográfica e the section called “Tipos de coluna”.

Segurança em AWS Clean Rooms

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam AWS Clean Rooms, consulte Serviços da AWS no escopo do programa de conformidade .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e os regulamentos aplicáveis

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Clean Rooms. Ele mostra como configurar para atender AWS Clean Rooms aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS Clean Rooms recursos.

Conteúdo

Proteção de dados em AWS Clean Rooms

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Clean Rooms. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS LGPD e Modelo de Responsabilidade Compartilhada no AWS Blog de Segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS Clean Rooms ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico.

Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em repouso

AWS Clean Rooms sempre criptografa todos os metadados do serviço em repouso sem exigir nenhuma configuração adicional. Essa criptografia é automática quando você usa AWS Clean Rooms.

O Clean Rooms ML criptografa todos os dados armazenados no serviço em repouso. AWS KMS Se você optar por fornecer sua própria chave do KMS, o conteúdo de seus modelos de semelhanças e trabalhos de geração de segmentos de semelhanças será criptografado em repouso com sua chave do KMS.

> **Note**
>
> Você pode usar as opções de criptografia do Amazon S3 para proteger seus dados em repouso.
> Para obter mais informações, consulte Especificar a criptografia do Amazon S3 no Guia do usuário do Amazon S3.

Criptografia em trânsito

AWS Clean Rooms usa Transport Layer Security (TLS) e criptografia do lado do cliente para criptografia em trânsito. A comunicação com AWS Clean Rooms é sempre feita por HTTPS para que seus dados sejam sempre criptografados em trânsito. Isso inclui todos os dados em trânsito ao usar o Clean Rooms ML.

Criptografia de dados subjacentes

Para obter mais informações sobre como criptografar seus dados subjacentes, consulte Computação criptográfica para o Clean Rooms.

Retenção de dados em AWS Clean Rooms

Quando você cria um modelo semelhante, o Clean Rooms ML lê seus dados de treinamento, os transforma em um formato adequado ao nosso modelo de ML e armazena os parâmetros do

modelo treinado dentro do Clean Rooms ML. O Clean Rooms ML não retém uma cópia dos seus dados de treinamento. AWS Clean Rooms As consultas SQL não retêm nenhum dos seus dados após a execução da consulta. O Clean Rooms ML então usa o modelo treinado para resumir o comportamento de todos os seus usuários. O Clean Rooms ML armazena um conjunto de dados em nível de usuário para cada usuário em seus dados enquanto seu modelo semelhante estiver ativo.

Quando você inicia um trabalho de geração de segmentos semelhantes, o Clean Rooms ML lê os dados iniciais, lê os resumos de comportamento do modelo semelhante associado e cria um segmento semelhante que é armazenado no serviço. AWS Clean Rooms O Clean Rooms ML não retém uma cópia dos seus dados iniciais. O Clean Rooms ML armazena a saída em nível de usuário da tarefa, desde que a tarefa esteja ativa.

Se você quiser remover seus dados de trabalho de geração de modelos ou segmentos de semelhanças, use a API para excluí-los. O Clean Rooms ML exclui de forma assíncrona todos os dados associados ao modelo ou ao trabalho. Quando esse processo é concluído, o Clean Rooms ML exclui os metadados do modelo ou do trabalho e eles não ficam mais visíveis na API. O Clean Rooms ML retém os dados excluídos por 3 dias para prevenção de recuperação de desastres. Depois que o trabalho ou modelo não estiver mais visível na API e passarem três dias, todos os dados associados ao modelo ou ao trabalho serão excluídos permanentemente.

Melhores práticas para colaborações de dados em AWS Clean Rooms

Este tópico descreve as melhores práticas para conduzir colaborações de dados no AWS Clean Rooms.

AWS Clean Rooms segue o Modelo de Responsabilidade AWS Compartilhada. AWS Clean Rooms oferece regras de análise que você pode configurar para fortalecer sua capacidade de proteger dados confidenciais em uma colaboração. As regras de análise que você configura AWS Clean Rooms aplicarão as restrições (controles de consulta e controles de saída de consulta) que você configurou. Você é responsável por determinar as restrições e configurar as regras de análise adequadamente.

As colaborações de dados podem envolver mais do que apenas o uso de AWS Clean Rooms. Para ajudá-lo a maximizar os benefícios das colaborações de dados, recomendamos que você execute as seguintes melhores práticas com o uso AWS Clean Rooms e especificamente com as regras de análise.

Tópicos

Melhores práticas com AWS Clean Rooms

Você é responsável por avaliar o risco de cada colaboração de dados e compará-lo aos seus requisitos de privacidade, como políticas e programas de conformidade externos e internos. Recomendamos que você tome medidas adicionais com o uso do AWS Clean Rooms. Essas ações podem ajudar a gerenciar ainda mais os riscos e a evitar tentativas de terceiros de reidentificar seus dados (por exemplo, ataques diferenciados ou ataques de canal lateral).

Por exemplo, considere realizar a devida diligência com seus outros colaboradores e firmar acordos legais com eles antes de iniciar uma colaboração. Para monitorar o uso de seus dados, considere também adotar outros mecanismos de auditoria com o uso do AWS Clean Rooms.

Melhores práticas para usar regras de análise em AWS Clean Rooms

As regras de análise AWS Clean Rooms permitem restringir as consultas que podem ser executadas definindo controles de consulta em uma tabela configurada. Por exemplo, você pode definir um controle de consulta sobre como uma tabela configurada pode ser unida e quais colunas podem ser selecionadas. Você também pode restringir a saída da consulta definindo controles de resultados de consulta, como limites de agregação nas linhas de saída. O serviço rejeita qualquer consulta e remove as linhas que não estão em conformidade com as regras de análise definidas pelos membros em suas tabelas configuradas na consulta.

Recomendamos as 10 melhores práticas a seguir para usar as regras de análise em sua tabela configurada:

- Crie tabelas configuradas separadas para casos de uso de consultas separados (por exemplo, planejamento ou atribuição de público). Você pode criar várias tabelas configuradas com a mesma tabela AWS Glue subjacente.
- Especifique as colunas na regra de análise (por exemplo, colunas de dimensão, colunas de lista, colunas de união) que são necessárias para consultas em uma colaboração. Isso pode ajudar a reduzir o risco de ataques diferenciados ou permitir que outros membros façam engenharia reversa em seus dados. Use o atributo de colunas da lista de permissões para observar outras colunas que talvez você queira tornar consultáveis no futuro. Para personalizar as colunas que

podem ser usadas para uma determinada colaboração, crie tabelas configuradas adicionais com a mesma AWS Glue tabela subjacente.

- Especifique as funções na regra de análise que são necessárias para análise na colaboração. Isso pode ajudar a reduzir o risco de erros de função raros que podem apresentar informações em um ponto de dados individual. Para personalizar as funções que podem ser usadas para uma determinada colaboração, crie tabelas configuradas adicionais com a mesma tabela AWS Glue subjacente.
- Adicione restrições de agregação em todas as colunas cujos valores em nível de linha sejam confidenciais. Isso inclui colunas em sua tabela configurada que também existem nas tabelas e regras de análise de outros membros da colaboração como uma restrição de agregação. Isso também inclui colunas na tabela configurada que não podem ser consultadas, ou seja, colunas que estão na tabela configurada, mas não estão na regra de análise. As restrições de agregação podem ajudar a reduzir o risco de correlacionar os resultados de consulta com dados fora da colaboração.
- Crie colaborações de teste e regras de análise para testar restrições criadas com regras de análise especificadas.
- Analise as tabelas configuradas pelo colaborador e as regras de análise dos membros nas tabelas configuradas para verificar se elas correspondem ao que foi acordado para a colaboração. Isso pode ajudar a reduzir o risco de outros membros criarem seus próprios dados para executar consultas que não foram acordadas.
- Revise a consulta de exemplo fornecida (somente console) que está ativada na tabela configurada após a configuração da regra de análise.

> **Note**
>
> Além da consulta de exemplo fornecida, outras consultas são possíveis com base na regra de análise e em outras tabelas e regras de análise de membros da colaboração.

- Você pode adicionar ou atualizar uma regra de análise para uma tabela configurada em uma colaboração. Ao fazer isso, revise todas as colaborações às quais a tabela configurada está associada e o impacto resultante. Isso ajuda a garantir que nenhuma colaboração use regras de análise obsoletas.
- Analise as consultas executadas na colaboração para verificar se elas correspondem aos casos de uso ou às consultas que foram acordadas para a colaboração. (As consultas estão disponíveis nos logs de consultas quando o atributo de registro de consultas está ativado.) Isso pode ajudar a

reduzir o risco de membros realizarem análises que não foram acordadas e de possíveis ataques, como ataques por canais laterais.

- Revise as colunas configuradas da tabela usadas nas regras de análise dos membros da colaboração e nas consultas para verificar se elas correspondem ao que foi acordado na colaboração. (As consultas estão disponíveis nos logs de consultas quando esse atributo está ativado.) Isso pode ajudar a reduzir o risco de outros membros criarem seus próprios dados para fazer consultas que não foram acordadas.

Identity and Access Management para AWS Clean Rooms

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Clean Rooms os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS Clean Rooms.

Usuário do serviço — Se você usar o AWS Clean Rooms serviço para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa

mais AWS Clean Rooms recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no AWS Clean Rooms, consulte Solução de problemas AWS Clean Rooms de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS Clean Rooms recursos da sua empresa, provavelmente tem acesso total AWS Clean Rooms a. É seu trabalho determinar quais AWS Clean Rooms recursos e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS Clean Rooms, consulteComo AWS Clean Rooms funciona com o IAM.

Administrador do IAM: Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar acesso ao AWS Clean Rooms. Para ver exemplos de políticas AWS Clean Rooms baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para AWS Clean Rooms

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (IAM Identity Center) ou a autenticação de login único da sua empresa são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre o uso do método recomendado para você assinar as

solicitações por conta própria, consulte Signature Version 4 signing process (Processo de assinatura do Signature Versão 4) no Referência geral da AWS.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Utilizar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade, chamada usuário raiz da Conta da AWS , é acessada por login com o endereço de e-mail e a senha usada para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte credenciais Usuário raiz da conta da AWS e identidades do IAM na Referência geral da AWS.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte “O que é o Centro de Identidade do IAM?” no Guia do usuário AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a

autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário AWS IAM Identity Center .

- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

Cada entidade do IAM (usuário ou função) começa sem permissões. Por padrão, os usuários não podem fazer nada, nem mesmo alterar sua própria senha. Para dar permissão a um usuário para fazer algo, um administrador deve anexar uma política de permissões ao usuário. Ou o administrador pode adicionar o usuário a um grupo que tenha as permissões pretendidas. Quando um administrador concede permissões a um grupo, todos os usuários desse grupo recebem essas permissões.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade da entidade

e seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) no Guia do usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do Usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS Clean Rooms funciona com o IAM

Antes de usar o IAM para gerenciar o acesso AWS Clean Rooms, saiba com quais recursos do IAM estão disponíveis para uso AWS Clean Rooms.

Recursos do IAM que você pode usar com AWS Clean Rooms

Atributo do IAM	AWS Clean Rooms apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Parcial
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Parcial
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Perfis vinculados ao serviço	Não

Para ter uma visão de alto nível de como AWS Clean Rooms e outros Serviços da AWS funcionam com a maioria dos recursos do IAM, consulte Serviços da AWS esse trabalho com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para AWS Clean Rooms

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições.

Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para AWS Clean Rooms

Para ver exemplos de políticas AWS Clean Rooms baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Clean Rooms

Políticas baseadas em recursos dentro AWS Clean Rooms

Oferece compatibilidade com políticas baseadas em recursos	Parcial

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso

conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

O AWS Clean Rooms serviço oferece suporte a apenas um tipo de política baseada em recursos, chamada política de recursos gerenciados de modelo semelhante configurado, que é anexada a um modelo semelhante configurado. Essa política define quais diretores podem realizar ações no modelo semelhante configurado.

Para saber como anexar uma política baseada em recursos a um modelo semelhante configurado, consulte. Comportamentos do IAM para AWS Clean Rooms ML

Ações políticas para AWS Clean Rooms

Oferece compatibilidade com ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de AWS Clean Rooms ações, consulte Ações definidas por AWS Clean Rooms na Referência de Autorização de Serviço.

As ações de política AWS Clean Rooms usam o seguinte prefixo antes da ação.

```
cleanrooms
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "cleanrooms:action1",
      "cleanrooms:action2"
         ]
```

Para ver exemplos de políticas AWS Clean Rooms baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Clean Rooms

Recursos políticos para AWS Clean Rooms

Oferece compatibilidade com recursos de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de AWS Clean Rooms recursos e seus ARNs, consulte Recursos definidos por AWS Clean Rooms na Referência de Autorização de Serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Clean Rooms.

Para ver exemplos de políticas AWS Clean Rooms baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Clean Rooms

Chaves de condição de política para AWS Clean Rooms

Suporta chaves de condição de política específicas do serviço	Parcial

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para saber como o AWS Clean Rooms ML usa chaves de condição de política, consulte Comportamentos do IAM para AWS Clean Rooms ML.

ACLs em AWS Clean Rooms

Oferece compatibilidade com ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS Clean Rooms

Oferece compatibilidade com ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com AWS Clean Rooms

Oferece compatibilidade com credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS trabalhar com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para AWS Clean Rooms

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.

Funções de serviço para AWS Clean Rooms

Oferece compatibilidade com funções de serviço	Sim

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper AWS Clean Rooms a funcionalidade. Edite as funções de serviço somente quando AWS Clean Rooms fornecer orientação para fazer isso.

Funções vinculadas a serviços para AWS Clean Rooms

Oferece suporte a perfis vinculados ao serviço	Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para AWS Clean Rooms

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS Clean Rooms . Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por AWS Clean Rooms, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição AWS Clean Rooms na Referência de Autorização de Serviço.

Tópicos

- Melhores práticas de política
- Usar o console do AWS Clean Rooms
- Permitir que usuários visualizem suas próprias permissões

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS Clean Rooms recursos em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do Usuário do IAM.
- Aplique permissões de privilégio mínimo –- ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do Usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso –- você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: Condição no Guia do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Usar o console do AWS Clean Rooms

Para acessar o AWS Clean Rooms console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS Clean Rooms recursos em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o AWS Clean Rooms console, anexe também a política AWS Clean Rooms `FullAccess` ou a política `ReadOnly` AWS gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

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

AWS políticas gerenciadas para AWS Clean Rooms

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

AWS política gerenciada: **`AWSCleanRoomsReadOnlyAccess`**

Você pode conectar `AWSCleanRoomsReadOnlyAccess` às suas entidades principais do IAM.

Essa política concede permissões somente leitura aos recursos e metadados em uma colaboração `AWSCleanRoomsReadOnlyAccess`.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `CleanRoomsRead` – Permite que as entidades principais tenham acesso somente leitura ao serviço.
- `ConsoleDisplayTables`— Permite que os diretores tenham acesso somente para leitura aos AWS Glue metadados necessários para mostrar dados sobre as AWS Glue tabelas subjacentes no console.
- `ConsoleLogSummaryQueryLogs` – Permite que as entidades principais vejam os logs de consultas.
- `ConsoleLogSummaryObtainLogs` – Permite que as entidades principais recuperem os resultados do log.

```
{
 "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 política gerenciada: **AWSCleanRoomsFullAccess**

Você pode conectar `AWSCleanRoomsFullAccess` às suas entidades principais do IAM.

Essa política concede permissões administrativas que permitem acesso total (leitura, gravação e atualização) aos recursos e metadados em uma AWS Clean Rooms colaboração. Essa política inclui acesso para realizar consultas.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `CleanRoomsAccess`— Concede acesso total a todas as ações em todos os recursos do AWS Clean Rooms.
- `PassServiceRole` – Concede acesso para passar um perfil de serviço somente para o serviço (condição `PassedToService`) que tem "cleanrooms" em seu nome.
- `ListRolesToPickServiceRole`— Permite que os diretores listem todas as suas funções para escolher uma função de serviço ao usar AWS Clean Rooms.
- `GetRoleAndListRolePoliciesToInspectServiceRole` – Permite que as entidades principais vejam o perfil de serviço e a política correspondente no IAM.
- `ListPoliciesToInspectServiceRolePolicy` – Permite que as entidades principais vejam o perfil de serviço e a política correspondente no IAM.
- `GetPolicyToInspectServiceRolePolicy` – Permite que as entidades principais vejam o perfil de serviço e a política correspondente no IAM.
- `ConsoleDisplayTables`— Permite que os diretores tenham acesso somente para leitura aos AWS Glue metadados necessários para mostrar dados sobre as AWS Glue tabelas subjacentes no console.
- `ConsolePickQueryResultsBucketListAll` – Permite que as entidades principais escolham um bucket do Amazon S3 em uma lista de todos os buckets do S3 disponíveis nos quais seus resultados de consulta são gravados.
- `SetQueryResultsBucket` – Permite que as entidades principais escolham um bucket do S3 no qual os resultados de consulta são gravados.
- `ConsoleDisplayQueryResults` – Permite que as entidades principais mostrem ao cliente os resultados de consulta, lidos do bucket do S3.
- `WriteQueryResults` – Permite que as entidades principais gravem os resultados de consulta em um bucket S3 de propriedade do cliente.

- `EstablishLogDeliveries`— Permite que os diretores entreguem registros de consulta ao grupo de CloudWatch registros Amazon Logs de um cliente.
- `SetupLogGroupsDescribe`— Permite que os diretores usem o processo de criação de grupos de CloudWatch logs do Amazon Logs.
- `SetupLogGroupsCreate`— Permite que os diretores criem um grupo de CloudWatch logs do Amazon Logs.
- `SetupLogGroupsResourcePolicy`— Permite que os diretores configurem uma política de recursos no grupo de CloudWatch registros do Amazon Logs.
- `ConsoleLogSummaryQueryLogs` – Permite que as entidades principais vejam os logs de consultas.
- `ConsoleLogSummaryObtainLogs` – Permite que as entidades principais recuperem os resultados do log.

```
{
 "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 política gerenciada: **AWSCleanRoomsFullAccessNoQuerying**

Você pode conectar `AWSCleanRoomsFullAccessNoQuerying` às suas IAM principals.

Essa política concede permissões administrativas que permitem acesso total (leitura, gravação e atualização) aos recursos e metadados em uma AWS Clean Rooms colaboração. Essa política exclui o acesso para realizar consultas.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `CleanRoomsAccess`— Concede acesso total a todas as ações em todos os recursos AWS Clean Rooms, exceto para consultas em colaborações.
- `CleanRoomsNoQuerying` – Nega explicitamente `StartProtectedQuery` e `UpdateProtectedQuery` para evitar consultas.
- `PassServiceRole` – Concede acesso para passar um perfil de serviço somente para o serviço (condição `PassedToService`) que tem "cleanrooms" em seu nome.
- `ListRolesToPickServiceRole`— Permite que os diretores listem todas as suas funções para escolher uma função de serviço ao usar AWS Clean Rooms.
- `GetRoleAndListRolePoliciesToInspectServiceRole` – Permite que as entidades principais vejam o perfil de serviço e a política correspondente no IAM.
- `ListPoliciesToInspectServiceRolePolicy` – Permite que as entidades principais vejam o perfil de serviço e a política correspondente no IAM.
- `GetPolicyToInspectServiceRolePolicy` – Permite que as entidades principais vejam o perfil de serviço e a política correspondente no IAM.
- `ConsoleDisplayTables`— Permite que os diretores tenham acesso somente para leitura aos AWS Glue metadados necessários para mostrar dados sobre as AWS Glue tabelas subjacentes no console.
- `EstablishLogDeliveries`— Permite que os diretores entreguem registros de consulta ao grupo de CloudWatch registros Amazon Logs de um cliente.
- `SetupLogGroupsDescribe`— Permite que os diretores usem o processo de criação de grupos de CloudWatch logs do Amazon Logs.
- `SetupLogGroupsCreate`— Permite que os diretores criem um grupo de CloudWatch logs do Amazon Logs.
- `SetupLogGroupsResourcePolicy`— Permite que os diretores configurem uma política de recursos no grupo de CloudWatch registros do Amazon Logs.
- `ConsoleLogSummaryQueryLogs` – Permite que as entidades principais vejam os logs de consultas.
- `ConsoleLogSummaryObtainLogs` – Permite que as entidades principais recuperem os resultados do log.
- `cleanrooms`— gerencie colaborações, modelos de análise, tabelas configuradas, associações e recursos associados dentro do AWS Clean Rooms serviço. Execute várias operações, como criar, atualizar, excluir, listar e recuperar informações sobre esses recursos.

- `iam`— Passe funções de serviço com nomes contendo `cleanrooms` "" para o AWS Clean Rooms serviço. Liste funções, políticas e inspecione funções de serviço e políticas relacionadas ao AWS Clean Rooms serviço.
- `glue`— recupere informações sobre bancos de dados, tabelas, partições e esquemas do. AWS Glue Isso é necessário para que o AWS Clean Rooms serviço exiba e interaja com as fontes de dados subjacentes.
- `logs`— Gerencie entregas de registros, grupos de registros e políticas de recursos para o CloudWatch Logs. Consulte e recupere registros relacionados ao AWS Clean Rooms serviço. Essas permissões são necessárias para fins de monitoramento, auditoria e solução de problemas no serviço.

A política também nega explicitamente as ações `cleanrooms:StartProtectedQuery` e `cleanrooms:UpdateProtectedQuery` impede que os usuários executem ou atualizem diretamente as consultas protegidas, o que deve ser feito por meio dos mecanismos controlados. AWS Clean Rooms

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CleanRoomsAccess",
   "Effect": "Allow",
   "Action": [
    "cleanrooms:BatchGetCollaborationAnalysisTemplate",
    "cleanrooms:BatchGetSchema",
    "cleanrooms:BatchGetSchemaAnalysisRule",
    "cleanrooms:CreateAnalysisTemplate",
    "cleanrooms:CreateCollaboration",
    "cleanrooms:CreateConfiguredTable",
    "cleanrooms:CreateConfiguredTableAnalysisRule",
    "cleanrooms:CreateConfiguredTableAssociation",
    "cleanrooms:CreateMembership",
    "cleanrooms:DeleteAnalysisTemplate",
    "cleanrooms:DeleteCollaboration",
    "cleanrooms:DeleteConfiguredTable",
    "cleanrooms:DeleteConfiguredTableAnalysisRule",
    "cleanrooms:DeleteConfiguredTableAssociation",
    "cleanrooms:DeleteMember",
    "cleanrooms:DeleteMembership",
    "cleanrooms:GetAnalysisTemplate",
```

```
    "cleanrooms:GetCollaboration",
    "cleanrooms:GetCollaborationAnalysisTemplate",
    "cleanrooms:GetConfiguredTable",
    "cleanrooms:GetConfiguredTableAnalysisRule",
    "cleanrooms:GetConfiguredTableAssociation",
    "cleanrooms:GetMembership",
    "cleanrooms:GetProtectedQuery",
    "cleanrooms:GetSchema",
    "cleanrooms:GetSchemaAnalysisRule",
    "cleanrooms:ListAnalysisTemplates",
    "cleanrooms:ListCollaborationAnalysisTemplates",
    "cleanrooms:ListCollaborations",
    "cleanrooms:ListConfiguredTableAssociations",
    "cleanrooms:ListConfiguredTables",
    "cleanrooms:ListMembers",
    "cleanrooms:ListMemberships",
    "cleanrooms:ListProtectedQueries",
    "cleanrooms:ListSchemas",
    "cleanrooms:UpdateAnalysisTemplate",
    "cleanrooms:UpdateCollaboration",
    "cleanrooms:UpdateConfiguredTable",
    "cleanrooms:UpdateConfiguredTableAnalysisRule",
    "cleanrooms:UpdateConfiguredTableAssociation",
    "cleanrooms:UpdateMembership",
    "cleanrooms:ListTagsForResource",
    "cleanrooms:UntagResource",
    "cleanrooms:TagResource"
   ],
   "Resource": "*"
  },
  {
   "Sid": "CleanRoomsNoQuerying",
   "Effect": "Deny",
   "Action": [
    "cleanrooms:StartProtectedQuery",
    "cleanrooms:UpdateProtectedQuery"
   ],
   "Resource": "*"
  },
  {
   "Sid": "PassServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
```

```
    ],
    "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*",
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "ListRolesToPickServiceRole",
    "Effect": "Allow",
    "Action": [
     "iam:ListRoles"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GetRoleAndListRolePoliciesToInspectServiceRole",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:ListRolePolicies",
     "iam:ListAttachedRolePolicies"
    ],
    "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*"
   },
   {
    "Sid": "ListPoliciesToInspectServiceRolePolicy",
    "Effect": "Allow",
    "Action": [
     "iam:ListPolicies"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GetPolicyToInspectServiceRolePolicy",
    "Effect": "Allow",
    "Action": [
     "iam:GetPolicy",
     "iam:GetPolicyVersion"
    ],
    "Resource": "arn:aws:iam::*:policy/*cleanrooms*"
   },
   {
```

```
    "Sid": "ConsoleDisplayTables",
    "Effect": "Allow",
    "Action": [
     "glue:GetDatabase",
     "glue:GetDatabases",
     "glue:GetTable",
     "glue:GetTables",
     "glue:GetPartition",
     "glue:GetPartitions",
     "glue:GetSchema",
     "glue:GetSchemaVersion",
     "glue:BatchGetPartition"
    ],
    "Resource": "*"
   },
   {
    "Sid": "EstablishLogDeliveries",
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogDelivery",
     "logs:GetLogDelivery",
     "logs:UpdateLogDelivery",
     "logs:DeleteLogDelivery",
     "logs:ListLogDeliveries"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "SetupLogGroupsDescribe",
    "Effect": "Allow",
    "Action": [
     "logs:DescribeLogGroups"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
```

```
  },
  {
   "Sid": "SetupLogGroupsCreate",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogGroup"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "SetupLogGroupsResourcePolicy",
   "Effect": "Allow",
   "Action": [
     "logs:DescribeResourcePolicies",
    "logs:PutResourcePolicy"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ConsoleLogSummaryQueryLogs",
   "Effect": "Allow",
   "Action": [
    "logs:StartQuery"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
   "Sid": "ConsoleLogSummaryObtainLogs",
   "Effect": "Allow",
   "Action": [
    "logs:GetQueryResults"
   ],
   "Resource": "*"
  }
```

```
 ]
}
```

AWS política gerenciada: **AWSCleanRoomsMLReadOnlyAccess**

Você pode conectar `AWSCleanRoomsMLReadOnlyAccess` às suas entidades principais do IAM.

Essa política concede permissões somente leitura aos recursos e metadados em uma colaboração `AWSCleanRoomsMLReadOnlyAccess`.

Esta política inclui as seguintes permissões:

- `CleanRoomsConsoleNavigation`— Concede acesso para visualizar as telas do AWS Clean Rooms console.
- `CleanRoomsMLRead`— Permite que os diretores tenham acesso somente para leitura ao serviço 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 política gerenciada: **AWSCleanRoomsMLFullAccess**

Você pode conectar `AWSCleanRoomsMLFullAcces` às suas entidades principais do IAM. Essa política concede permissões administrativas que permitem acesso total (leitura, gravação e atualização) aos recursos e metadados necessários ao Clean Rooms ML.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `CleanRoomsMLFullAccess`— Concede acesso a todas as ações do Clean Rooms ML.
- `PassServiceRole` – Concede acesso para passar um perfil de serviço somente para o serviço (condição `PassedToService`) que tem "cleanrooms-ml" em seu nome.
- `CleanRoomsConsoleNavigation`— Concede acesso para visualizar as telas do AWS Clean Rooms console.
- `CollaborationMembershipCheck`— Quando você inicia um trabalho de geração de público (segmento semelhante) em uma colaboração, o serviço Clean Rooms ML liga `ListMembers` para verificar se a colaboração é válida, se o chamador é um membro ativo e se o proprietário do modelo de público configurado é um membro ativo. Essa permissão é sempre necessária; o SID de navegação do console só é necessário para usuários do console.
- `AssociateModels`— Permite que os diretores associem um modelo de ML de salas limpas à sua colaboração.
- `TagAssociations`: permite que as entidades principais adicionem tags à associação entre um modelo de semelhanças e uma colaboração.
- `ListRolesToPickServiceRole`— Permite que os diretores listem todas as suas funções para escolher uma função de serviço ao usar AWS Clean Rooms.

- `GetRoleAndListRolePoliciesToInspectServiceRole` – Permite que as entidades principais vejam o perfil de serviço e a política correspondente no IAM.
- `ListPoliciesToInspectServiceRolePolicy` – Permite que as entidades principais vejam o perfil de serviço e a política correspondente no IAM.
- `GetPolicyToInspectServiceRolePolicy` – Permite que as entidades principais vejam o perfil de serviço e a política correspondente no IAM.
- `ConsoleDisplayTables`— Permite que os diretores tenham acesso somente para leitura aos AWS Glue metadados necessários para mostrar dados sobre as AWS Glue tabelas subjacentes no console.
- `ConsolePickOutputBucket`: permite que as entidades principais selecionem buckets do Amazon S3 para saídas configuradas do modelo de público.
- `ConsolePickS3Location`: permite que as entidades principais selecionem o local em um bucket para saídas configuradas do modelo de público.

```
{
    "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 atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Clean Rooms desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS Clean Rooms documento.

Alteração	Descrição	Data
AWSCleanRoomsFullAccessNoQuerying: atualizar para uma política existente.	adicionado a .cleanrooms:BatchGetSchemaAnalysisRuleCleanRoomsAccess	13 de maio de 2024
AWSCleanRoomsFullAccess: atualizar para uma política existente.	A ID da declaração foi atualizada AWSCleanRoomsFullAccess de ConsolePickQueryResultsBucket para SetQueryResultsBucket nesta política para representar melhor as permissões, pois as permissões são necessárias para definir o intervalo de resultados da consulta com e sem o console.	21 de março de 2024
AWSCleanRoomsMLReadOnlyAccess – Nova política AWSCleanRoomsMLFullAccess – Nova política	Adição de AWSCleanRoomsMLReadOnlyAccess e AWSCleanRoomsMLFullAccess para compatibilidade com o AWS Clean Rooms ML.	29 de novembro de 2023
AWSCleanRoomsFullAccessNoQuerying: atualizar para uma política existente.	Adicionados cleanrooms:CreateAnalysisTemplatecleanrooms:GetAnalysisTemplate,,cleanrooms:UpdateAnalysisTemplate, cleanrooms:DeleteAnalysisTemplate,cleanrooms:ListAnalysisTemplates,cleanrooms:GetCollaborationAnalysisTemplate,cleanrooms:BatchGetCollaborationAnalysisTemplate, e cleanrooms:ListCollaborationAnalysisTemplates para CleanRoomsAccess habilitar o novo recurso de modelos de análise.	31 de julho de 2023
AWSCleanRoomsFullAccessNoQuerying: atualizar para uma política existente.	Adicionado cleanrooms:ListTagsForResource, cleanrooms:UntagResource e cleanrooms:TagResource	21 de março de 2023

Alteração	Descrição	Data
	para CleanRoomsAccess habilitar a marcação de recursos.	
AWS Clean Rooms começou a rastrear alterações	AWS Clean Rooms começou a rastrear as mudanças em suas políticas AWS gerenciadas.	12 de janeiro de 2023

Solução de problemas AWS Clean Rooms de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Clean Rooms um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AWS Clean Rooms
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Clean Rooms recursos

Não estou autorizado a realizar uma ação em AWS Clean Rooms

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para exibir detalhes sobre um recurso do *`my-example-widget`* fictício, mas não tem as permissões fictícias do `cleanrooms:`*`GetWidget`*.

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

Nesse caso, a política de Mateo deve ser atualizada para permitir que ele tenha acesso ao recurso *`my-example-widget`* usando a ação `cleanrooms:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Clean Rooms.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS Clean Rooms. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Clean Rooms recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil.

Para saber mais, consulte:

- Para saber se é AWS Clean Rooms compatível com esses recursos, consulteComo AWS Clean Rooms funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Prevenção do problema do substituto confuso entre serviços

O problema de "confused deputy" é uma questão de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar em um problema confuso de delegado. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição global `aws:SourceArn` nas políticas de recursos para limitar as permissões que o AWS Clean Rooms concede outro serviço ao recurso. Use `aws:SourceArn` se quiser que apenas um recurso seja associado ao acesso entre serviços.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Em AWSClean Rooms, você também precisa comparar com a chave de `sts:ExternalId` condição.

O valor de `aws:SourceArn` deve ser definido como o ARN da associação da função assumida.

O exemplo a seguir mostra como você pode usar a chave de contexto da condição global `aws:SourceArn` no AWS Clean Rooms para evitar o problema confused deputy.

> **Note**
>
> O exemplo de política se aplica à política de confiança do perfil de serviço que o AWS Clean Rooms usa para acessar os dados do cliente.

O valor de *membershipID* é seu ID de membro do AWS Clean Rooms na colaboração.

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

Comportamentos do IAM para AWS Clean Rooms ML

Trabalhos entre contas

O Clean Rooms ML permite que determinados recursos criados por um Conta da AWS sejam acessados com segurança em sua conta por outro. Conta da AWS Quando um cliente em A chama

Conta da AWS `StartAudienceGenerationJob` um `ConfiguredAudienceModel` recurso de propriedade de Conta da AWS B, o Clean Rooms ML cria dois ARNs para o trabalho. Um ARN em Conta da AWS A e outro em B. Conta da AWS Os ARNs são idênticos, exceto por seus. Conta da AWS

O Clean Rooms ML cria dois ARNs para o trabalho para garantir que ambas as contas possam aplicar suas próprias políticas de IAM aos trabalhos. Por exemplo, ambas as contas podem usar o controle de acesso baseado em tags e aplicar políticas de sua AWS organização. O trabalho processa dados de ambas as contas, para que elas possam excluir o trabalho e os dados associados. Nenhuma conta pode impedir que a outra exclua o trabalho.

Há apenas uma execução de trabalho e ambas as contas podem ver o trabalho quando chamam `ListAudienceGenerationJobs`. Ambas as contas podem chamar as `Export` APIs `GetDelete`,, e no trabalho usando o ARN com seu próprio Conta da AWS ID.

Nenhum deles Conta da AWS pode acessar o trabalho usando um ARN com o outro Conta da AWS ID.

O nome do trabalho deve ser exclusivo em uma Conta da AWS. O nome em Conta da AWS B é *`$accounta-$name`*. O nome escolhido por Conta da AWS A é prefixado com Conta da AWS A quando o trabalho é visualizado em B. Conta da AWS

Para que uma conta cruzada `StartAudienceGenerationJob` seja bem-sucedida, Conta da AWS B deve permitir essa ação no novo trabalho em Conta da AWS B e `ConfiguredAudienceModel` no Conta da AWS B usando uma política de recursos semelhante ao exemplo a seguir:

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

Se você usa a API de AWS Clean Rooms ML para criar um modelo semelhante configurado com `manageResourcePolicies` set como true, AWS Clean Rooms cria essa política para você.

Além disso, a política de identidade do chamador em A precisa Conta da AWS de `StartAudienceGenerationJob` permissão ativada`arn:aws:cleanrooms-ml:us-west-1:AccountA:audience-generation-job/*`. Portanto, há três recursos do IAM para ação`StartAudienceGenerationJob`: o Conta da AWS trabalho A, o trabalho Conta da AWS Conta da AWS B e o `ConfiguredAudienceModel` B.

> **Warning**
>
> A Conta da AWS pessoa que iniciou o trabalho recebe um evento AWS CloudTrail de registro de auditoria sobre o trabalho. A Conta da AWS proprietária de `ConfiguredAudienceModel` não recebe um evento de logs de auditoria do AWS CloudTrail .

Marcação de trabalhos

Quando você define o parâmetro `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` de `CreateConfiguredAudienceModel`, todos os trabalhos de geração de segmentos de semelhanças em sua conta que são criados com base nesse modelo de semelhanças configurado têm como padrão as mesmas tags do modelo de semelhanças configurado. O modelo de semelhanças configurado é o pai e o trabalho de geração do segmento de semelhanças é o filho.

Se você estiver criando um trabalho em sua própria conta, as tags de solicitação do trabalho substituirão as tags pais. Os trabalhos criados por outras contas nunca criam tags em sua conta. Se você definir `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` e outra conta criar

um trabalho, haverá duas cópias do trabalho. A cópia na sua conta tem as tags do recurso pai e a cópia na conta do remetente do trabalho tem as tags da solicitação.

Validar colaboradores

Ao conceder permissões a outros membros de uma AWS Clean Rooms colaboração, a política de recursos deve incluir a chave `cleanrooms-ml:CollaborationId` de condição. Isso garante que o `collaborationId` parâmetro seja incluído na StartAudienceGenerationJobsolicitação. Quando o `collaborationId` parâmetro é incluído na solicitação, o Clean Rooms ML valida que a colaboração existe, o remetente do trabalho é um membro ativo da colaboração e o proprietário do modelo semelhante configurado é um membro ativo da colaboração.

Quando AWS Clean Rooms gerencia sua política de recursos de modelo semelhante configurada (o `manageResourcePolicies` parâmetro está sendo `TRUE` CreateConfiguredAudienceModelAssociation solicitado), essa chave de condição será definida na política de recursos. Portanto, você deve especificar a `collaborationId` entrada StartAudienceGenerationJob.

Acesso entre contas

Só `StartAudienceGenerationJob` pode ser chamado em várias contas. Todas as outras APIs de ML do Clean Rooms só podem ser usadas com recursos em sua própria conta. Isso garante que seus dados de treinamento, configuração de modelo de semelhanças e outras informações permaneçam privadas.

O Clean Rooms ML nunca revela o Amazon S3 ou AWS Glue localizações em todas as contas. O local dos dados de treinamento, o local de saída do modelo de semelhanças configurado e o local de seed do trabalho de geração de segmentos de semelhanças nunca são visíveis em todas as contas. Se você usar `Get` em um trabalho de geração de público enviado por outra conta, o serviço não mostrará o local de seed.

Validação de conformidade para AWS Clean Rooms

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentos aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS Clean Rooms

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenters tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança da infraestrutura em AWS Clean Rooms

Como serviço gerenciado, AWS Clean Rooms é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS Clean Rooms pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Segurança de rede

Ao AWS Clean Rooms ler seu bucket do S3 durante a execução da consulta, o tráfego entre AWS Clean Rooms e o Amazon S3 é roteado com segurança pela rede privada. AWS O tráfego em trânsito é assinado usando o protocolo Amazon Signature versão 4 (SIGv4) e criptografado usando HTTPS. Esse tráfego é autorizado com base no perfil de serviço do IAM que você configurou para sua tabela configurada.

Você pode se conectar programaticamente AWS Clean Rooms por meio de um endpoint. Para obter uma lista de pontos de extremidade de serviço, consulte endpoints AWS Clean Rooms e cotas no Referência geral da AWS.

Todos os endpoints de serviço são somente HTTPS. Você pode usar endpoints da Amazon Virtual Private Cloud (VPC) caso queira se conectar a partir da AWS Clean Rooms sua VPC e não queira ter conectividade com a Internet. Para obter mais informações, consulte Acesse os AWS serviços AWS PrivateLink no AWS PrivateLink Guia.

Você pode atribuir políticas do IAM aos seus diretores do IAM, que usam as chaves de SourceVpce contexto aws: para restringir seu principal do IAM a fim de poder fazer chamadas apenas AWS Clean Rooms por meio de um endpoint VPC e não pela Internet.

Access AWS Clean Rooms ou AWS Clean Rooms ML usando um endpoint de interface ()AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre sua nuvem privada virtual (VPC) AWS Clean Rooms e/ou AWS Clean Rooms ML. Você pode acessar AWS Clean Rooms nosso AWS Clean Rooms ML como se estivesse em sua VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias na sua VPC não precisam de endereços IP públicos para acessar o AWS Clean Rooms.

Você estabelece essa conectividade privada criando um endpoint de interface, desenvolvido pelo AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Estas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao AWS Clean Rooms.

Para obter mais informações, consulte Acessar os Serviços da AWS pelo AWS PrivateLink no Guia do AWS PrivateLink .

Considerações para AWS Clean Rooms

Antes de configurar um endpoint de interface para AWS Clean Rooms, consulte as Considerações no AWS PrivateLink Guia.

AWS Clean Rooms e o AWS Clean Rooms ML oferecem suporte para fazer chamadas para todas as ações de API por meio do endpoint da interface.

As políticas de VPC endpoint não são compatíveis com nem ML. AWS Clean Rooms AWS Clean Rooms Por padrão, o acesso total ao AWS Clean Rooms AWS Clean Rooms ML é permitido por meio do endpoint da interface. Como alternativa, você pode associar um grupo de segurança às interfaces de rede do endpoint para controlar o tráfego AWS Clean Rooms ou o AWS Clean Rooms ML por meio do endpoint da interface.

Crie um endpoint de interface para AWS Clean Rooms

Você pode criar um endpoint de interface para AWS Clean Rooms ou AWS Clean Rooms ML usando o console Amazon VPC ou AWS Command Line Interface o AWS CLI(). Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink .

Crie um endpoint de interface para AWS Clean Rooms usar o seguinte nome de serviço.

```
com.amazonaws.region.cleanrooms
```

Crie um endpoint de interface para AWS Clean Rooms ML usando o nome do serviço a seguir.

```
com.amazonaws.region.cleanrooms-ml
```

Se você habilitar o DNS privado para o endpoint da interface, poderá fazer solicitações de API a AWS Clean Rooms usando seu nome DNS regional padrão. Por exemplo, `cleanrooms-ml.us-east-1.amazonaws.com`.

Monitoramento AWS Clean Rooms

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Clean Rooms suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar AWS Clean Rooms, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- O Amazon CloudWatch Logs permite que você monitore, armazene e acesse seus arquivos de log a partir de instâncias do Amazon EC2 e de outras fontes. AWS CloudTrail O Amazon CloudWatch Logs pode monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.

  O Clean Rooms ML permite trabalhos entre contas para determinadas ações de API. Conta da AWS Aquele que iniciou o trabalho recebe o evento de registro de AWS CloudTrail auditoria do trabalho. Para mais informações, consulte Comportamentos do IAM para AWS Clean Rooms ML.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por você ou em seu nome Conta da AWS e entrega os arquivos de log em um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário da AWS CloudTrail.

Registrar em log chamadas de API do AWS Clean Rooms usando o AWS CloudTrail

AWS Clean Rooms está integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um AWS service (Serviço da AWS) em AWS Clean Rooms. O CloudTrail captura as chamadas de API do AWS Clean Rooms como eventos. As chamadas capturadas incluem as chamadas do console do AWS Clean Rooms e as chamadas de código para as operações da API do AWS Clean Rooms. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o AWS Clean Rooms. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o AWS Clean Rooms, o

endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações do AWS Clean Rooms no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade em AWS Clean Rooms, essa atividade é registrada em um evento do CloudTrail junto com outros eventos AWS service (Serviço da AWS) em Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Viewing events with CloudTrail Event history (Como visualizar eventos com o histórico de eventos do CloudTrail).

Para obter um registro contínuo de eventos na sua Conta da AWS, incluindo eventos para o AWS Clean Rooms, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros Serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte as informações a seguir.

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Recebimento de arquivos de log do CloudTrail de várias regiões
- Recebimento de arquivos de log do CloudTrail de várias contas

Todas as ações do AWS Clean Rooms são registradas pelo CloudTrail e são documentadas na Referência de API do AWS Clean Rooms.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou de usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.

- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do AWS Clean Rooms

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

Exemplos de eventos do CloudTrail AWS Clean Rooms

Os exemplos a seguir demonstram eventos do CloudTrail para:

Tópicos

- StartProtectedQuery (êxito)
- StartProtectedQuery (falha)

StartProtectedQuery (êxito)

```
{
    "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 (falha)

```
{
    "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"
}
```

Criando AWS Clean Rooms recursos com AWS CloudFormation

AWS Clean Rooms é integrado com AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus AWS recursos. Como resultado desta integração, você pode gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os AWS recursos que você deseja e AWS CloudFormation provisiona e configura esses recursos para você. Exemplos de recursos incluem colaborações, tabelas configuradas, associações de tabelas configuradas e associações.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar seus AWS Clean Rooms recursos de forma consistente e repetida. Descreva seus recursos uma vez e, em seguida, provisione os mesmos recursos repetidamente em vários Contas da AWS Regiões da AWS e.

AWS Clean Rooms e AWS CloudFormation modelos

Para provisionar e configurar recursos AWS Clean Rooms e serviços relacionados, você deve entender AWS CloudFormation os modelos. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation Para obter mais informações, consulte O que é o Designer AWS CloudFormation ? no Manual do usuário do AWS CloudFormation .

AWS Clean Rooms suporta a criação de colaborações, tabelas configuradas, associações de tabelas configuradas e associações em. AWS CloudFormation Para obter mais informações, incluindo exemplos de modelos JSON e YAML para colaborações, tabelas configuradas, associações de tabelas configuradas e associações, consulte a Referência de tipo recurso AWS Clean Rooms no Guia do usuário AWS CloudFormation .

Os seguintes modelos estão disponíveis:

- Modelo de análise

  Especifique um modelo de AWS Clean Rooms análise, incluindo nome, descrição, formato, fonte, parâmetros e tags.

Para obter mais informações, consulte os tópicos a seguir.

AWS::CleanRooms::AnalysisTemplate no AWS Clean Rooms Guia do usuário

CreateAnalysisTemplate na Referência de API do AWS Clean Rooms

- Colaboração

  Especifique uma AWS Clean Rooms colaboração, incluindo nome, descrição, tipo, parâmetros e tags.

  Para obter mais informações, consulte os tópicos a seguir.

  AWS::CleanRooms::Collaboration no AWS CloudFormation Guia do usuário

  CreateCollaboration na Referência de API do AWS Clean Rooms

- Tabela configurada

  Especifique uma tabela configurada em AWS Clean Rooms, incluindo colunas permitidas, método de análise, descrição, nome, referência da tabela, orçamento de privacidade e tags. As tabelas configuradas representam uma referência a uma tabela existente no AWS Glue Data Catalog que foi configurada para uso em AWS Clean Rooms. Uma tabela configurada contém uma regra de análise que determina como os dados podem ser usados.

  Para obter mais informações, consulte os tópicos a seguir.

  AWS::CleanRooms::ConfiguredTable no AWS CloudFormation Guia do usuário

  CreateConfiguredTable na Referência de API do AWS Clean Rooms

- Associação de tabela configurada

  Especifique uma associação de tabela configurada em AWS Clean Rooms, incluindo ID, descrição, ID de associação, nome, função, Amazon Resource Name (ARN) e tags. Uma associação de tabela configurada vincula uma tabela configurada a uma colaboração.

  Para obter mais informações, consulte os tópicos a seguir.

  AWS::CleanRooms::ConfiguredTableAssociation no AWS CloudFormation Guia do usuário

  CreateConfiguredTableAssociation na Referência de API do AWS Clean Rooms

- Associação

Especifique a associação para um identificador de colaboração específico e ingresse na colaboração no formato AWS Clean Rooms.

Para obter mais informações, consulte os tópicos a seguir.

AWS::CleanRooms::Membership no AWS CloudFormation Guia do usuário

CreateMembership na Referência de API do AWS Clean Rooms

- Modelo de orçamento de privacidade

  Especifique um modelo AWS Clean Rooms de orçamento de privacidade, incluindo um orçamento de privacidade, ruído adicionado por consulta e atualização mensal do orçamento de privacidade.

  Para obter mais informações, consulte os tópicos a seguir.

  AWS::CleanRooms::PrivacyBudgetTemplate no AWS CloudFormation Guia do usuário

  CreatePrivacyBudgetTemplate na Referência de API do AWS Clean Rooms
- Crie um conjunto de dados de treinamento

  Especifique um conjunto de dados de treinamento para um modelo de ML de salas limpas a partir de uma AWS Glue tabela.

  Para obter mais informações, consulte os tópicos a seguir.

  AWS::CleanRoomsML::TrainingDataset no AWS CloudFormation Guia do usuário

  CreateTrainingDatasetna referência da API Clean Rooms ML

Saiba mais sobre AWS CloudFormation

Para saber mais sobre isso AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- AWS CloudFormation Guia do usuário
- AWS CloudFormation API Reference
- Guia do Usuário da Interface de Linha de Comando AWS CloudFormation

Cotas para AWS Clean Rooms

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada um. AWS service (Serviço da AWS) Salvo indicação em contrário, cada cota é específica para um Região da AWS. Você pode solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas.

Para ver as cotas de AWS Clean Rooms, abra o console Service Quotas. No painel de navegação, escolha Serviços AWS e selecione AWS Clean Rooms.

Para solicitar o aumento da cota, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível nas Cotas de Serviço, use o formulário de aumento do limite de serviço.

Você Conta da AWS tem as seguintes cotas relacionadas a. AWS Clean Rooms

Recurso	Padrão	Descrição
Membros convidados por colaboração	5	Número máximo de membros convidados por colaboração
Assinaturas por conta	100	Número máximo de assinaturas para uma conta
Colaborações criadas por conta	10	Número máximo de colaborações criadas por conta
Tabelas configuradas por conta	60	Número máximo de tabelas configuradas que podem ser criadas por uma conta
Tabelas de associações por associação	25	Número máximo de tabelas associadas por associação ativa
Consultas contínuas simultâneas por associação	5	Número máximo de consultas simultâneas por associação
Lista de permissões de colunas por tabela configurada	100	Número máximo de colunas que podem ser listadas

Recurso	Padrão	Descrição
		como permitidas por tabela configurada
Tabelas configuradas por consulta protegida	15	Número máximo de tabelas configuradas em uma consulta protegida
Modelos de análise por associação	25	Número máximo de modelos de análise por associação
Associações configuradas de modelo de semelhanç as (modelo de público) por associação	5	Número máximo de associaçõ es de modelos de semelhanç as configuradas por associaçã o.

Limites de parâmetros de recursos

Recurso	Padrão	Descrição
Tamanho da regra de análise	100 KB	Tamanho máximo do JSON para uma regra de análise
Comprimento do texto da consulta	90 KB (8 KB para consultas de privacidade diferencial)	Tamanho máximo do texto para uma instrução de consulta SQL
Tempo de execução da consulta	12 horas	Duração máxima em que uma consulta é executada antes do tempo limite
Tamanho de saída do arquivo de dados de consulta	6,2 GB	Tamanho máximo de um arquivo de saída de uma consulta protegida

Você Conta da AWS tem as seguintes cotas de transação de API por segundo (TPS) por conta por endpoint.

Cotas de controle de utilização da API

Recurso	Limite de taxa	Descrição
Taxa de solicitações `BatchGetCollaborationAnalysisTemplate`	5 TPS	Número máximo de chamadas de API `BatchGetCollaborationAnalysisTemplate` por segundo
Taxa de solicitações `BatchGetSchema`	5 TPS	Número máximo de chamadas de API `BatchGetSchema` por segundo
Taxa de solicitações `CreateAnalysisTemplate`	5 TPS	Número máximo de chamadas de API `CreateAnalysisTemplate` por segundo
Taxa de solicitações `CreateCollaboration`	5 TPS	Número máximo de chamadas de API `CreateCollaboration` por segundo
Taxa de solicitações `CreateConfiguredAudienceModelAssociation`	5 TPS	Número máximo de `CreateConfiguredAudienceModelAssociation` chamadas por segundo
Taxa de solicitações `CreateConfiguredTable`	5 TPS	Número máximo de `CreateConfiguredTable` chamadas por segundo
Taxa de solicitações `CreateConfiguredTableAnalysisRule`	5 TPS	Número máximo de `CreateConfiguredTableAnalysisRule` chamadas por segundo

Recurso	Limite de taxa	Descrição
Taxa de solicitações `CreateConfiguredTableAssociation`	5 TPS	Número máximo de `CreateConfiguredTableAssociation` chamadas por segundo
Taxa de solicitações `CreateMembership`	5 TPS	Número máximo de `CreateMembership` chamadas por segundo
Taxa de solicitações `CreatePrivacyBudgetTempate`	5 TPS	Número máximo de `CreatePrivacyBudgetTemplate` chamadas por segundo
Taxa de solicitações `DeleteAnalysisTemplate`	5 TPS	Número máximo de `DeleteAnalysisTemplate` chamadas por segundo
Taxa de solicitações `DeleteCollaboration`	5 TPS	Número máximo de `DeleteCollaboration` chamadas por segundo
Taxa de solicitações `DeleteConfiguredAudienceModelAssociation`	5 TPS	Número máximo de `DeleteConfiguredAudienceModelAssociation` chamadas por segundo
Taxa de solicitações `DeleteConfiguredTable`	5 TPS	Número máximo de `DeleteConfiguredTable` chamadas por segundo

Recurso	Limite de taxa	Descrição
Taxa de solicitações `DeleteConfiguredTableAnalysisRule`	5 TPS	Número máximo de `DeleteConfiguredTableAnalysisRule` chamadas por segundo
Taxa de solicitações `DeleteConfiguredTableAssociation`	5 TPS	Número máximo de `DeleteConfiguredTableAssociation` chamadas por segundo
Taxa de solicitações `DeleteMember`	5 TPS	Número máximo de `DeleteMember` chamadas por segundo
Taxa de solicitações `DeleteMembership`	5 TPS	Número máximo de `DeleteMembership` chamadas por segundo
Taxa de solicitações `DeletePrivacyBudgetTemplate`	5 TPS	Número máximo de `DeletePrivacyBudgetTemplate` chamadas por segundo
Taxa de solicitações `GetAnalysisTemplate`	5 TPS	Número máximo de `GetAnalysisTemplate` chamadas por segundo
Taxa de solicitações `GetCollaboration`	5 TPS	Número máximo de `GetCollaboration` chamadas por segundo
Taxa de solicitações `GetCollaborationConfiguredAudienceModelAssociation`	5 TPS	Número máximo de `GetCollaborationConfiguredAudienceModelAssociation` chamadas por segundo

Recurso	Limite de taxa	Descrição
Taxa de solicitações `GetCollaborationPrivacyBudgetTemplate`	5 TPS	Número máximo de `GetCollaborationPrivacyBudgetTemplate` chamadas por segundo
Taxa de solicitações `GetConfiguredAudienceModelAssociation`	5 TPS	Número máximo de `GetConfiguredAudienceModelAssociation` chamadas por segundo
Taxa de solicitações `GetConfiguredTable`	5 TPS	Número máximo de `GetConfiguredTable` chamadas por segundo
Taxa de solicitações `GetConfiguredTableAnalysisRule`	5 TPS	Número máximo de `GetConfiguredTableAnalysisRule` chamadas por segundo
Taxa de solicitações `GetConfiguredTableAssociation`	20 TPS	Número máximo de `GetConfiguredTableAssociation` chamadas por segundo
Taxa de solicitações `GetMembership`	5 TPS	Número máximo de `GetMembership` chamadas por segundo
Taxa de solicitações `GetPrivacyBudgetTemplate`	5 TPS	Número máximo de `GetPrivacyBudgetTemplate` chamadas por segundo
Taxa de solicitações `GetProtectedQuery`	20 TPS	Número máximo de `GetProtectedQuery` chamadas por segundo

Recurso	Limite de taxa	Descrição
Taxa de solicitações `GetSchema`	5 TPS	Número máximo de `GetSchema` chamadas por segundo
Taxa de solicitações `GetSchemaAnalysisRule`	5 TPS	Número máximo de `GetSchemaAnalysisRule` chamadas por segundo
Taxa de solicitações `ListAnalysisTemplates`	5 TPS	Número máximo de `ListAnalysisTemplates` chamadas por segundo
Taxa de solicitações `ListCollaborationConfiguredAudienceModelAssociations`	5 TPS	Número máximo de `ListCollaborationConfiguredAudienceModelAssociations` chamadas por segundo
Taxa de solicitações `ListCollaborationPrivacyBudgets`	5 TPS	Número máximo de `ListCollaborationPrivacyBudgets` chamadas por segundo
Taxa de solicitações `ListCollaborationPrivacyBudgetTemplates`	5 TPS	Número máximo de `ListCollaborationPrivacyBudgetTemplates` chamadas por segundo
Taxa de solicitações `ListCollaborations`	5 TPS	Número máximo de `ListCollaborations` chamadas por segundo
Taxa de solicitações `ListConfiguredAudienceModelAssociations`	5 TPS	Número máximo de `ListConfiguredAudienceModelAssociations` chamadas por segundo

Recurso	Limite de taxa	Descrição
Taxa de solicitações `ListConfiguredTableAssociations`	5 TPS	Número máximo de `ListConfiguredTableAssociations` chamadas por segundo
Taxa de solicitações `ListConfiguredTables`	5 TPS	Número máximo de `ListConfiguredTables` chamadas por segundo
Taxa de solicitações `ListMembers`	5 TPS	Número máximo de `ListMembers` chamadas por segundo
Taxa de solicitações `ListMemberships`	5 TPS	Número máximo de `ListMemberships` chamadas por segundo
Taxa de solicitações `ListPrivacyBudgets`	5 TPS	Número máximo de `ListPrivacyBudgets` chamadas por segundo
Taxa de solicitações `ListPrivacyBudgetTemplates`	5 TPS	Número máximo de `ListPrivacyBudgetTemplates` chamadas por segundo
Taxa de solicitações `ListProtectedQueries`	5 TPS	Número máximo de `ListProtectedQueries` chamadas por segundo
Taxa de solicitações `ListSchemas`	5 TPS	Número máximo de `ListSchemas` chamadas por segundo

Recurso	Limite de taxa	Descrição
Taxa de solicitações `StartProtectedQuery`	5 TPS	Número máximo de `StartProtectedQuery` chamadas por segundo
Taxa de solicitações `UpdateAnalysisTemplate`	5 TPS	Número máximo de `UpdateAnalysisTemplate` chamadas por segundo
Taxa de solicitações `UpdateCollaboration`	5 TPS	Número máximo de `UpdateCollaboration` chamadas por segundo
Taxa de solicitações `UpdateConfiguredAudienceModelAssociation`	5 TPS	Número máximo de `UpdateConfiguredAudienceModelAssociation` chamadas por segundo
Taxa de solicitações `UpdateConfiguredTable`	5 TPS	Número máximo de `UpdateConfiguredTable` chamadas por segundo
Taxa de solicitações `UpdateConfiguredTableAnalysisRule`	5 TPS	Número máximo de `UpdateConfiguredTableAnalysisRule` chamadas por segundo
Taxa de solicitações `UpdateConfiguredTableAssociation`	5 TPS	Número máximo de `UpdateConfiguredTableAssociation` chamadas por segundo

Recurso	Limite de taxa	Descrição
Taxa de solicitações `UpdatePrivacyBudgetTemplate`	5 TPS	Número máximo de `UpdatePrivacyBudgetTemplate` chamadas por segundo

AWS Clean Rooms Cotas de limitação da API ML

Recurso	Limite de taxa	Descrição
Taxa de solicitações de `CreateAudienceModel`	Taxa de 1 TPS, intermitência de 3 TPS	Número máximo de chamadas de API `CreateAudienceModel` por segundo
Taxa de solicitações `CreateConfiguredAudienceModel`	10 TPS	Número máximo de chamadas de API `CreateConfiguredAudienceModel` por segundo
Taxa de solicitações `CreateTrainingDataset`	10 TPS	Número máximo de chamadas de API `CreateTrainingDataset` por segundo
Taxa de solicitações `DeleteAudienceGenerationJob`	Taxa de 2 TPS, intermitência de 10 TPS	Número máximo de chamadas de API `DeleteAudienceGenerationJob` por segundo
Taxa de solicitações `DeleteAudienceModel`	Taxa de 2 TPS, intermitência de 10 TPS	Número máximo de chamadas de API `DeleteAudienceModel` por segundo
Taxa de solicitações `DeleteConfiguredAudienceModel`	10 TPS	Número máximo de chamadas de API `DeleteCon`

Recurso	Limite de taxa	Descrição
		figuredAudienceModel por segundo
Taxa de solicitações DeleteConfiguredAudienceModelPolicy	25 TPS	Número máximo de chamadas de API DeleteConfiguredAudienceModelPolicy por segundo
Taxa de solicitações DeleteTrainingDataset	10 TPS	Número máximo de chamadas de API DeleteTrainingDataset por segundo
Taxa de solicitações GetAudienceGenerationJob	50 TPS	Número máximo de chamadas de API GetAudienceGenerationJob por segundo
Taxa de solicitações GetAudienceModel	50 TPS	Número máximo de chamadas de API GetAudienceModel por segundo
Taxa de solicitações GetConfiguredAudienceModel	50 TPS	Número máximo de chamadas de API GetConfiguredAudienceModel por segundo
Taxa de solicitações GetConfiguredAudienceModelPolicy	50 TPS	Número máximo de chamadas de API GetConfiguredAudienceModelPolicy por segundo
Taxa de solicitações GetTrainingDataset	50 TPS	Número máximo de chamadas de API GetTrainingDataset por segundo

Recurso	Limite de taxa	Descrição
Taxa de solicitações `ListAudienceExportJobs`	50 TPS	Número máximo de chamadas de API `ListAudienceExportJobs` por segundo
Taxa de solicitações `ListAudienceGenerationJobs`	50 TPS	Número máximo de chamadas de API `ListAudienceGenerationJobs` por segundo
Taxa de solicitações `ListAudienceModels`	50 TPS	Número máximo de chamadas de API `ListAudienceModels` por segundo
Taxa de solicitações `ListConfiguredAudienceModels`	50 TPS	Número máximo de chamadas de API `ListConfiguredAudienceModels` por segundo
Taxa de solicitações `ListTagsForResource`	50 TPS	Número máximo de chamadas de API `ListTagsForResource` por segundo
Taxa de solicitações `ListTrainingDatasets`	50 TPS	Número máximo de chamadas de API `ListTrainingDatasets` por segundo
Taxa de solicitações `PutConfiguredAudienceModelPolicy`	25 TPS	Número máximo de chamadas de API `PutConfiguredAudienceModelPolicy` por segundo
Taxa de solicitações `StartAudienceExportJob`	Taxa de 1 TPS, intermitência de 3 TPS	Número máximo de chamadas de API `StartAudienceExportJob` por segundo

Recurso	Limite de taxa	Descrição
Taxa de solicitações `StartAudienceGenerationJob`	Taxa de 1 TPS, intermitência de 5 TPS	Número máximo de chamadas de API `StartAudienceGenerationJob` por segundo
Taxa de solicitações `TagResource`	10 TPS	Número máximo de chamadas de API `TagResource` por segundo
Taxa de solicitações `UntagResource`	50 TPS	Número máximo de chamadas de API `UntagResource` por segundo
Taxa de solicitações `UpdateConfiguredAudienceModel`	10 TPS	Número máximo de chamadas de API `UpdateConfiguredAudienceModel` por segundo

Nome	Padrão	Ajustá	Descrição
Trabalhos de exportação de público ativo por trabalho de geração de público	Cada região compatível: 25	Não	O número máximo de trabalhos ativos de exportação de público para um trabalho de geração de público
Trabalhos de exportação de público pendentes/em andamento por cliente	Cada região compatível: 20	Não	O número máximo de trabalhos de exportação de público pendentes/em andamento por cliente
Trabalhos de geração de público pendentes/em andamento por cliente	Cada região compatível: 10	Sim	O número máximo de trabalhos de geração de público pendentes/em andamento por cliente

Nome	Padrão	Ajustá	Descrição
Modelos de público pendentes/em andamento por cliente	Cada região compatível: 2	Sim	O número máximo de trabalhos de treinamento de modelo de público pendentes/em andamento por cliente

Cotas de ML para salas limpas

Recurso	Padrão	Descrição
Conjuntos de dados	por trabalho	
Número máximo de interações	20 bilhões	Número máximo de interações permitidas nos dados de treinamento. Entradas maiores têm a amostra reduzida.
Número mínimo de interações	1 milhão	
Número máximo de usuários distintos para treinamento de modelos de semelhanças	1 milhão	Se forem incluídos mais, somente os 100 milhões principais serão usados, classificados por número de interações.
Número mínimo de usuários distintos para treinamento de modelos de semelhanças	100.000	
Número máximo de usuários para exportar trabalho em segmento semelhante (público)	10.000	

Recurso	Padrão	Descrição
Número máximo de itens distintos usados para treinamento de modelos.	1 milhão	É possível incluir até 50 milhões de itens, mas somente o milhão mais popular será usado.
Número máximo de colunas de atributos no conjunto de dados de treinamento.	10	
Número mínimo de itens distintos por usuário	2	AWS Clean Rooms O ML exige que cada linha ou usuário tenha dois ou mais itens, incluindo itens repetidos.
Tamanho máximo do público inicial	500.000	
Tamanho mínimo do público inicial	500	O provedor de dados de treinamento pode definir esse valor como tão baixo quanto 25.
APIs	por cliente	
Número total de conjuntos de dados de treinamento ativos	500	
Número total de modelos de semelhanças ativos (modelos de público)	500	
Número total de modelos de semelhanças ativos configura dos (modelos de público)	10.000	

Recurso	Padrão	Descrição
Número total de trabalhos de geração de segmentos de semelhanças concluídos (público)	Sem limite	
Número total de trabalhos de exportação de segmentos de semelhanças concluídos (público)	Sem limite	
Duração máxima de um trabalho de geração de modelo de semelhanças (modelo de público)	1 dia (24 horas)	
Duração máxima de um trabalho de geração de segmento de semelhanças (público)	10 horas	Depois de fornecer uma semente, o Clean Rooms ML leva no máximo 10 horas para gerar um segmento semelhante.
Porcentagem mínima para um compartimento de tamanho de segmento (público)	1%	
Porcentagem máxima para um compartimento de tamanho de segmento (público)	20%	
Tamanho absoluto mínimo para um compartimento de tamanho de segmento (público)	1% do número de usuários distintos	

Recurso	Padrão	Descrição
Tamanho absoluto máximo para um compartimento de tamanho de segmento (público)	20% do número de usuários distintos	

Histórico de documentos para o Guia AWS Clean Rooms do usuário

A tabela a seguir descreve as versões de documentação do AWS Clean Rooms.

Para receber notificações sobre atualizações dessa documentação, você pode se inscrever em o feed RSS. Para assinar as atualizações de RSS, você deve ter um plug-in de RSS habilitado para o navegador que está usando.

Alteração	Descrição	Data
Atualizar a política existente	A seguinte nova permissão foi adicionada à política gerenciada `AWSCleanRoomsFullAccessNoQuerying` : `cleanrooms:BatchGetSchemaAnalysisRule` .	13 de maio de 2024
AWS Clean Rooms O ML agora está totalmente disponível	AWS Clean Rooms O ML fornece um método de aprimoramento de privacidade para duas partes identificarem usuários semelhantes em seus dados sem a necessida de de compartilhar seus dados entre si.	3 de abril de 2024
Atualizar a política existente	O ID da declaração na política `AWSCleanRoomsFullAccess` gerenciada foi atualizado de ConsolePickQueryResultsBucket para SetQueryResultsBucket para melhor representar	21 de março de 2024

	as permissões desde as permissões.	
Novas políticas gerenciadas para AWS Clean Rooms ML	Duas novas políticas gerenciadas foram adicionadas: `AWSCleanRoomsMLReadOnlyAccess` e `AWSCleanRoomsMLFullAccess`.	29 de novembro de 2023
AWS Clean Rooms ML (versão prévia)	AWS Clean Rooms O ML fornece um método de aprimoramento de privacidade para duas partes identificarem usuários semelhantes em seus dados sem a necessidade de compartilhar seus dados entre si.	29 de novembro de 2023
AWS Clean Rooms Privacidade diferencial (versão prévia)	Agora, os clientes podem usar a Privacidade AWS Clean Rooms Diferencial para ajudar a proteger a privacidade de seus usuários.	29 de novembro de 2023
Configuração de pagamento	O criador da colaboração agora pode configurar o membro que pode executar consultas ou um membro diferente na colaboração para ser cobrado pelos custos de computação da consulta.	14 de novembro de 2023
Tempo de execução da consulta: atualização	A duração máxima em que uma consulta é executada antes de o tempo limite ser atualizado de 4 horas para 12 horas.	6 de outubro de 2023

AWS CloudFormation recursos - atualização	AWS Clean Rooms adicionou os seguintes novos recursos: `AWS::CleanRooms::Membership` `ProtectedQueryOutputConfiguration` `AWS::CleanRooms::Membership` `ProtectedQueryResultConfiguration` , `AWS::CleanRooms::Membership` `ProtectedQueryS3OutputConfiguration` e.	7 de setembro de 2023
AWS CloudFormation recursos - atualização	AWS Clean Rooms adicionou os seguintes novos recursos: `AWS::CleanRooms::AnalysisTemplate` `AWS::CleanRooms::ConfiguredTable` `AnalysisRuleCustom` e.	31 de agosto de 2023
Habilidades separadas dos membros	Agora, o criador da colaboração pode designar um membro como aquele que pode consultar e outro membro como aquele pode receber os resultados. Isso dá ao criador da colaboração a capacidade de garantir que o membro que pode consultar não tenha acesso aos resultados da consulta.	30 de agosto de 2023

AWS Clean Rooms Glossário	Atualização somente de documentação para adicionar um glossário de termos. AWS Clean Rooms	30 de agosto de 2023
Suporte para tabelas do Apache Iceberg (prévia)	AWS Clean Rooms agora suporta Apache Iceberg tabelas (pré-visualização).	25 de agosto de 2023
Atualização de cotas	A seção Cotas foi atualizada para refletir a nova cota padrão para associações por conta.	9 de agosto de 2023
Atualizar a política existente	As seguintes novas permissões foram adicionadas à política gerenciada `AWSCleanRoomsFullAccessNoQuerying`: `cleanrooms:CreateAnalysisTemplate`, `cleanrooms:GetAnalysisTemplate`, `cleanrooms:UpdateAnalysisTemplate`, `cleanrooms:DeleteAnalysisTemplate`, `cleanrooms:ListAnalysisTemplates`, `cleanrooms:GetCollaborationAnalysisTemplate`, `cleanrooms:BatchGetCollaborationAnalysisTemplate` e `cleanrooms:ListCollaborationAnalysisTemplates`.	31 de julho de 2023

Modelos de análise e regra de análise personalizada	AWS Clean Rooms agora suporta modelos de análise e a regra de análise personalizada. Os modelos de análise permitem que os colaboradores criem ou importem sua própria consulta SQL personalizada para usar na colaboração. Com a regra de análise Personalizada, o proprietário da tabela pode aprovar consultas SQL personalizadas nas tabelas configuradas.	31 de julho de 2023
As regras de análise são compatíveis com a condição lógica `OR`	AWS Clean Rooms as regras de análise agora suportam a condição `OR` lógica na JOIN cláusula.	29 de junho de 2023
CloudFormation integração	AWS Clean Rooms agora se integra com AWS CloudFormation.	15 de junho de 2023
Construtor de análises	Os membros que podem consultar e receber resultados agora podem executar consultas em algumas tabelas sem escrever código SQL usando a Interface do usuário do construtor de análises.	15 de junho de 2023
Funções SQL	Atualização somente da documentação para esclarecer as funções SQL compatíveis.	5 de maio de 2023

Solução de problemas	Atualização somente da documentação para adicionar uma seção de Solução de problemas comuns.	27 de abril de 2023
Tipos de dados compatíveis para AWS Clean Rooms	Atualização somente de documentação para adicionar uma nova seção que lista os tipos de dados compatíveis AWS Glue Data Catalog .	26 de abril de 2023
Exemplos de AWS CloudTrail eventos	Atualização somente de documentação para adicionar exemplos de CloudTrai l eventos para StartProt ectedQuery (bem-sucedido) e StartProtectedQuery (falhado).	20 de abril de 2023
Atualizar a política existente	As seguintes novas permissõe s foram adicionadas à política gerenciada `AWSCleanR oomsFullAccessNoQu erying` : `cleanroom s:ListTagsForResou rce` , `cleanroom s:UntagResource` e `cleanrooms:TagReso urce` . Para obter mais informações, consulte Políticas gerenciadas pela AWS.	21 de março de 2023
Disponibilidade geral	AWS Clean Rooms agora está disponível ao público em geral.	21 de março de 2023

Versão de visualização	Versão prévia do Guia AWS Clean Rooms do usuário	12 de janeiro de 2023

AWS Clean Rooms Glossário

Consulte este glossário para se familiarizar com a terminologia usada para o AWS Clean Rooms.

Regra de análise de agregação

A restrição de consulta que permite consultas que agregam análises usando COUNT, SUM, ou AVG funções ao longo de dimensões opcionais. Essas consultas não revelarão informações em nível de linha.

Oferece suporte a casos de uso como planejamento de campanhas, alcance de mídia, frequência e medição de conversão.

Outros tipos de regras de análise são personalizadas e listadas.

Regras de análise

‘As restrições de consulta que autorizam um tipo específico de consulta.

O tipo de regra de análise determina que tipo de análise pode ser executada na tabela configurada. Cada tipo tem uma estrutura de consulta predefinida. Você controla como as colunas da tabela podem ser usadas na estrutura por meio dos controles de consulta.

Os tipos de regras de análise são agregação, lista e personalização.

Modelo de análise

Uma consulta pré-aprovada específica para colaboração que pode ser reutilizada.

Oferece suporte a consultas SQL personalizadas suportadas em AWS Clean Rooms.

Pode conter parâmetros sempre que um valor literal normalmente apareça em uma consulta SQL. Para obter mais informações sobre os tipos de parâmetros compatíveis, consulte Tipos de dados na Referência AWS Clean Rooms SQL.

Os modelos de análise só funcionam com a regra de análise personalizada.

Cliente de criptografia do C3R

O cliente de criptografia Cryptographic Computing para o Clean Rooms (C3R).

Usado para criptografar e descriptografar dados, o C3R é um SDK de criptografia do lado do cliente com uma interface de linha de comando.

Coluna de texto não criptografado

Uma coluna que não está protegida criptograficamente para uma JOIN ou SELECT estrutura SQL.

As colunas de texto não criptografado podem ser usadas em qualquer parte da consulta SQL.

Colaboração

Um limite lógico seguro AWS Clean Rooms no qual os membros podem realizar consultas SQL em tabelas configuradas.

As colaborações são criadas pelo criador da colaboração.

Somente membros que foram convidados para a colaboração podem participar da colaboração.

Uma colaboração pode ter apenas um membro que pode consultar dados, um membro que pode receber resultados e um membro pagando pelos custos de computação da consulta.

Todos os membros podem ver a lista de participantes convidados na colaboração antes de entrarem na colaboração.

Criador de colaboração

O membro que cria uma colaboração.

Há apenas um criador de colaboração por colaboração.

Somente o criador da colaboração pode remover membros da colaboração ou excluir a colaboração.

Tabela configurada

Cada tabela configurada representa uma referência a uma tabela existente no AWS Glue Data Catalog que foi configurada para uso em AWS Clean Rooms. Uma tabela configurada contém uma regra de análise que determina como os dados podem ser usados.

Atualmente, AWS Clean Rooms oferece suporte à associação de dados armazenados no Amazon Simple Storage Service (Amazon S3) que são catalogados por meio de. AWS Glue

Para obter mais informações sobre AWS Glue, consulte o Guia do AWS Glue desenvolvedor.

As tabelas configuradas podem ser associadas a uma ou mais colaborações.

> **Note**
>
> AWS Clean Rooms atualmente não oferece suporte a locais de bucket do Amazon S3 registrados no. AWS Lake Formation

Regra de análise personalizada

A restrição de consulta que permite um conjunto específico de consultas pré-aprovadas (modelos de análise) ou permite um conjunto específico de contas que pode fornecer consultas que usam seus dados.

Oferece suporte a casos de uso como atribuição de primeiro toque, análises incrementais e análises de descoberta de público.

Compatível com a privacidade diferencial.

Descriptografia

O processo de transformar dados criptografados de volta à sua forma original. Só será possível realizar se você tiver acesso à chave secreta.

Privacidade diferencial

Uma técnica matematicamente rigorosa que protege os dados de colaboração do membro que pode receber resultados aprendendo sobre um indivíduo específico.

Criptografia

O processo de codificação de dados em um formato que parece aleatório usando um valor secreto chamado chave. É impossível determinar o texto sem formatação original sem acesso à chave.

Coluna de impressão digital

Uma coluna protegida criptograficamente para uma JOIN estrutura SQL.

Regra de análise de lista

A restrição de consulta que permite consultas que geram uma análise de atributos em nível de linha da sobreposição entre essa tabela e as tabelas do membro que pode consultar.

Oferece suporte a casos de uso como enriquecimento e criação ou supressão de público.

Membro

Um AWS cliente que participa de uma colaboração.

Um membro é identificado usando sua Conta da AWS.

Todos os membros podem contribuir com dados.

Membro que pode consultar

O membro que pode consultar dados na colaboração.

Há apenas um membro que pode consultar por colaboração, e esse membro é imutável.

Um usuário administrativo pode usar permissões AWS Identity and Access Management (IAM) para controlar quais de seus diretores do IAM (como usuários ou funções) podem consultar dados na colaboração. Para ter mais informações, consulte Criar um perfil de serviço para ler dados.

Membro que pode receber resultados

O membro que pode receber os resultados de consulta. O membro que pode receber os resultados especifica as configurações dos resultados de consulta para o destino do Amazon S3 e o formato do resultado da consulta.

Há apenas um membro que pode receber resultados por colaboração, e esse membro é imutável.

Membro pagando pelos custos de computação da consulta

O membro responsável pelo pagamento dos custos de computação da consulta.

Há apenas um membro responsável por pagar pelos custos de computação de consulta por colaboração, e esse membro é imutável.

Se o criador da colaboração não tiver especificado ninguém como membro pagando pelos custos de computação da consulta, o membro que pode consultar é o pagador padrão.

O membro que paga pelos custos de computação da consulta recebe uma fatura pelas consultas que foram executadas na colaboração.

Associação

Um recurso criado quando um membro se junta a uma colaboração.

Todos os recursos que o membro associa a uma colaboração fazem parte da associação ou estão associados à associação.

Somente o membro que possui a associação pode adicionar, remover ou editar recursos nessa associação.

Coluna selada

Uma coluna protegida criptograficamente para uma SELECT estrutura SQL.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.