Guía del usuario

AWS Clean Rooms

AWS Clean Rooms: Guía del usuario

Table of Contents

¿Qué es AWS Clean Rooms?

AWS Clean Rooms le ayuda a usted y a sus socios a analizar y colaborar en sus conjuntos de datos colectivos para obtener nuevos conocimientos sin revelarse los datos subyacentes entre sí. Puede utilizar AWS Clean Rooms un espacio de trabajo de colaboración seguro para crear sus propias salas limpias en cuestión de minutos y empezar a analizar sus conjuntos de datos colectivos con solo unos pocos pasos. Puede elegir los socios con los que desea colaborar, seleccionar sus conjuntos de datos y configurar restricciones para los participantes.

Con AWS Clean Roomsél, puede colaborar con miles de empresas que ya lo utilizan AWS. La colaboración no requiere mover los datos de otra plataforma AWS ni cargarlos en ella. Al ejecutar consultas, AWS Clean Rooms lee los datos de su ubicación original y aplica reglas de análisis integradas para ayudarle a mantener el control sobre sus datos.

AWS Clean Rooms proporciona controles de acceso a los datos y controles de soporte de auditoría integrados que puede configurar. Estos controles incluyen:

- Reglas de análisis para restringir las consultas SQL y proporcionar restricciones de salida.
- Computación criptográfica para Clean Rooms mantener los datos cifrados, incluso mientras se procesan las consultas, con el fin de cumplir estrictas políticas de manejo de datos.
- Registros de consultas para revisar las consultas y respaldar las auditorías.
- Privacidad diferencial para proteger a los usuarios de los intentos de identificación. AWS Clean Rooms La privacidad diferencial es una capacidad totalmente gestionada que protege la privacidad de sus usuarios con técnicas respaldadas matemáticamente y controles intuitivos que puede aplicar con unos pocos clics.
- AWS Clean Rooms El aprendizaje automático permite a dos partes identificar a usuarios similares en sus datos sin necesidad de compartir sus datos entre sí. La primera parte crea y configura un modelo similar a partir de sus datos de entrenamiento. La segunda parte aporta sus datos iniciales a una colaboración y crea un segmento similar que se parece a los datos de entrenamiento.

En el siguiente vídeo se explica más sobre AWS Clean Rooms.

AWS Clean Rooms

¿Es la primera vez que lo usa AWS Clean Rooms ?

Si es la primera vez que lo utiliza AWS Clean Rooms, le recomendamos que comience leyendo las siguientes secciones:

- ¿Cómo funciona AWS Clean Rooms
- Acceder AWS Clean Rooms
- Con AWS Clean Rooms figuración
- AWS Clean Rooms Glosario

¿Cómo funciona AWS Clean Rooms

El siguiente flujo de trabajo presupone que:

- El miembro de la colaboración ya ha cargado sus tablas de datos a Amazon S3 y creado una tabla de AWS Glue.
- (Opcional) Solo para las tablas de datos cifrados, el miembro de la colaboración ya ha preparado las tablas de datos cifrados con el cliente de cifrado de C3R.

En resumen, el flujo de trabajo AWS Clean Rooms es el siguiente:

1. El creador de la colaboración realiza las siguientes tareas:
   - Crea una colaboración.
   - Invita a uno o más miembros a la colaboración.
   - Asigna capacidades a los miembros (como miembro que puede realizar consultas y miembro que puede recibir los resultados).

     Si el creador de la colaboración es también el miembro que puede recibir los resultados, especificará el destino y el formato de los resultados de las consultas. También proporcionará un nombre de recurso de Amazon (ARN) del rol de servicio para escribir los resultados en el destino de resultados de las consultas.
   - Configura qué miembro es responsable de pagar los costos de computación de las consultas en la colaboración.
2. El miembro invitado se une a la colaboración creando un recurso de pertenencia.

Si el miembro invitado es el miembro que puede recibir los resultados, especificará el destino y el formato de los resultados de las consultas. También proporcionará un ARN de rol de servicio para escribir en el destino de los resultados de las consultas.

Si el miembro invitado es el responsable de pagar los costos de computación de las consultas, deberá aceptar sus responsabilidades de pago antes de unirse a la colaboración.

3. El miembro configura una AWS Glue tabla existente para usarla en AWS Clean Rooms. (este paso se puede realizar antes o después de unirse a una colaboración, a menos que se utilice la computación criptográfica para Clean Rooms).

> **Note**
>
> AWS Clean Rooms admite AWS Glue tablas. Para obtener más información acerca de cómo obtener sus datos en AWS Glue, consulte Paso 3: cargar la tabla de datos en Amazon S3.

   1. El miembro asigna un nombre a la tabla configurada y elige qué columnas usar en la colaboración.
   2. El miembro configura una de las siguientes reglas de análisis en la tabla configurada:
      - Regla de análisis de agregación o regla de análisis de lista: para controlar el tipo de análisis que se pueden ejecutar en la tabla.
      - Regla de análisis personalizada: para permitir un conjunto específico de consultas preaprobadas o un conjunto específico de cuentas que puedan proporcionar consultas que utilicen sus datos. Permite al miembro activar la privacidad diferencial para protegerse de los intentos de identificación del usuario.

   > **Note**
   >
   > El miembro puede configurar la regla de análisis en cualquier momento antes de asociar sus tablas configuradas a la colaboración.

4. El miembro asocia sus tablas configuradas a la colaboración y asigna AWS Clean Rooms un rol de servicio para acceder a sus AWS Glue tablas.

> **Note**
>
> Este rol de servicio tiene permisos relacionados con las tablas. La función de servicio solo se puede asumir si se ejecutan las consultas permitidas en nombre del miembro que puede realizar la consulta. AWS Clean Rooms Ningún miembro de la colaboración (salvo el propietario de los datos) tiene acceso a las tablas subyacentes de la colaboración. El propietario de los datos puede activar la privacidad diferencial para que sus tablas estén disponibles para que otros miembros las consulten.

5. El miembro que puede realizar consultas ejecuta las consultas SQL en las tablas configuradas.

   Las consultas solo se pueden ejecutar si el miembro responsable de pagar los costos de computación de las consultas se ha unido a la colaboración como miembro activo.

   Las reglas de análisis y las restricciones de salida se aplican automáticamente. AWS Clean Rooms solo devuelve los resultados que cumplen con las reglas de análisis definidas en el paso 3.b.

   En el caso de las consultas sobre datos cifrados, el miembro que puede recibir los resultados recibe los datos cifrados AWS Clean Rooms que deben descifrarse (consulte el paso 8).
6. El miembro que puede recibir los resultados los revisa en la AWS Clean Rooms consola o en el bucket de Amazon S3 que especificó.
7. Las consultas ejecutadas en la colaboración se cobran al miembro que paga los costos de computación de las consultas.
8. (Opcional) Solo en el caso de las tablas de datos cifrados, el miembro que puede recibir los resultados descifra los resultados de la consulta ejecutando el cliente de cifrado de C3R en modo de descifrado.

Servicios relacionados

Los siguientes Servicios de AWS aspectos están relacionados con AWS Clean Rooms:

- Amazon S3

  Los miembros de Collaboration pueden almacenar los datos que introduzcan AWS Clean Rooms en Amazon S3.

Para obtener más información, consulte los temas siguientes:

Preparación de tablas de datos para consultas en AWS Clean Rooms

¿Qué es Amazon S3 en la Guía del usuario de Amazon Simple Storage Service

- AWS Glue

  Los miembros de Collaboration pueden crear AWS Glue tablas a partir de sus datos en Amazon S3 para usarlas en ellas AWS Clean Rooms.

  Para obtener más información, consulte los temas siguientes:

  Preparación de tablas de datos para consultas en AWS Clean Rooms

  ¿Qué es AWS Glue? en la Guía para desarrolladores de AWS Glue

- AWS CloudFormation

  Cree los siguientes recursos en AWS CloudFormation: colaboraciones, tablas configuradas, asociaciones de tablas configuradas y membresías

  Para obtener más información, consulte Creación de AWS Clean Rooms recursos con AWS CloudFormation.

- AWS CloudTrail

  AWS Clean Rooms Utilízalo con CloudTrail los registros para mejorar el análisis de la Servicio de AWS actividad.

  Para obtener más información, consulte Registrar llamadas a la API de AWS Clean Rooms mediante AWS CloudTrail.

Acceder AWS Clean Rooms

Puede acceder a AWS Clean Rooms través de las siguientes opciones:

- Directamente a través de la AWS Clean Rooms consola en https://console.aws.amazon.com/cleanrooms/.
- Programáticamente a través de la AWS Clean Rooms API. Para obtener más información, consulte la Referencia de la API de AWS Clean Rooms .

Precios para AWS Clean Rooms

Para obtener información acerca de los precios, consulte Precios de AWS Clean Rooms.

Facturación para AWS Clean Rooms

AWS Clean Rooms permite al creador de la colaboración configurar qué miembro paga los costes de procesamiento de consultas de la colaboración.

En la mayoría de los casos, el miembro que puede realizar consultas es también el miembro que paga los costos de computación de las consultas. No obstante, si el miembro que puede realizar consultas y el miembro que paga los costos de computación de las consultas son diferentes, cuando el miembro que puede realizar consultas ejecuta las consultas en su propio recurso de pertenencia, se factura al recurso de pertenencia del miembro que paga los costos de computación de las consultas.

El miembro que paga los costes de cálculo de las consultas no ve ningún evento relacionado con las consultas que se estén ejecutando en su historial de CloudTrail eventos porque el pagador no es quien ejecuta las consultas ni es el propietario del recurso con el que se ejecutan las consultas. No obstante, el pagador ve las facturas generadas en su recurso de pertenencia para todas las consultas ejecutadas por el miembro que puede realizar consultas en la colaboración.

Para obtener más información acerca de cómo crear una colaboración y configurar el miembro que paga los costos de computación de las consultas, consulte Creación de una colaboración.

Reglas de análisis en AWS Clean Rooms

Como parte de la habilitación de una tabla para utilizarla en AWS Clean Rooms el análisis de la colaboración, el miembro de la colaboración debe configurar una regla de análisis.

Una regla de análisis es un control que mejora la privacidad y que cada propietario de datos define en una tabla configurada. Una regla de análisis determina cómo se puede analizar la tabla configurada.

La regla de análisis es un control de nivel de cuenta en la tabla configurada (un recurso de nivel de cuenta) y que se aplica a cualquier colaboración a la que esté asociada la tabla configurada. Si no hay ninguna regla de análisis configurada, la tabla configurada se puede asociar a colaboraciones, pero no se puede consultar. Las consultas solo pueden hacer referencia a tablas configuradas con el mismo tipo de regla de análisis.

Para configurar una regla de análisis, primero debe seleccionar un tipo de análisis y, a continuación, especificar la regla de análisis. En ambos pasos, debe tener en cuenta el caso de uso que desea habilitar y cómo desea proteger los datos subyacentes.

AWS Clean Rooms aplica los controles más restrictivos en todas las tablas configuradas a las que se hace referencia en una consulta.

En los siguientes ejemplos se ilustran los controles restrictivos.

Example Control restrictivo: restricción de salida

- El colaborador A tiene una restricción de salida de 100 en la columna de identificador.
- El colaborador B tiene una restricción de salida de 150 en la columna de identificador.

  Una consulta de agregación que haga referencia a ambas tablas configuradas requiere al menos 150 valores diferenciados de identificador dentro de una fila de salida para que se muestre en el resultado de la consulta. El resultado de la consulta no indica que los resultados se eliminan debido a la restricción de salida.

Example Control restrictivo: plantilla de análisis no aprobada

- El colaborador A ha permitido una plantilla de análisis con una consulta que hace referencia a tablas configuradas de los colaboradores A y B en su regla de análisis personalizada.
- El colaborador B no ha permitido la plantilla de análisis.

Como el colaborador B no ha permitido la plantilla de análisis, el miembro que puede realizar la consulta no puede ejecutar esa plantilla de análisis.

Tipos de regla de análisis

Existen tres tipos de reglas de análisis: de agregación, de lista y personalizadas. En las siguientes tablas se comparan los tipos de reglas de análisis. Cada tipo tiene dedicada una sección independiente en la que se describe la especificación de la regla de análisis.

Las siguientes tablas muestran un resumen comparativo de los tipos de reglas de análisis.

Casos de uso admitidos

En las siguientes tablas se muestra un resumen comparativo de los casos de uso admitidos para cada tipo de regla de análisis.

Caso de uso	Agregación	Lista	Personalizada
Análisis admitidos	Consultas que agregan estadísticas mediante las funciones COUNT, SUM y AVG en dimensiones opcionales	Consultas que generan listas de nivel de fila de la superposición entre varias tablas	Cualquier análisis personalizado, siempre que la plantilla de análisis o el creador del análisis se hayan revisado y permitido
Casos de uso comunes	Análisis de segmentos, medición y atribución	Enriquecimiento, creación de segmentos	Atribución de primer toque, análisis

Caso de uso	Agregación	Lista	Personalizada
			incrementales, detección de audiencias
Constructos SQL	• Declaraciones JOIN: INNER JOIN • Funciones de agregado: COUNT/ COUNT DISTINCT, SUM/ SUM DISTINCT y AVG • Funciones escalares : subconjunto limitado	• Declaraciones JOIN: INNER JOIN • Funciones escalares : ninguna	La mayoría de las funciones SQL y constructos SQL están disponibles con el comando SELECT
Subconsultas y expresiones de tabla comunes (CTE)	No	No	Sí

Caso de uso	Agregación	Lista	Personalizada
Plantillas de análisis	No	No	Sí

Controles admitidos

Las siguientes tablas muestran un resumen comparativo de cómo cada tipo de regla de análisis protege los datos subyacentes.

Controlar	Agregación	Lista	Personalizada
Mecanismo de control	Controle cómo se pueden usar los datos de la tabla en una consulta (por ejemplo, permitir COUNT y SUM de la columna hashed_email).	Controle cómo se pueden usar los datos de la tabla en una consulta (por ejemplo, permitir el uso de la columna hashed_email solo en combinaciones).	Controle qué consultas pueden ejecutarse en la tabla (por ejemplo, permitir solo las consultas definidas en las plantillas de análisis "Consulta personalizada 1").
Técnicas de mejora de la	• Coincidencia ciega	• Coincidencia ciega	Privacidad diferencial

Controlar	Agregación	Lista	Personalizada
privacidad integrada	• Agregación obligatoria • Umbral de agregación mín. >= • 2 Estructura de consulta predefinida	• Solapamiento obligatorio • Estructura de consulta predefinida	
Revisar la consulta antes de que pueda ejecutarse	No	No	Sí, con plantillas de análisis

Para obtener más información sobre las reglas de análisis disponibles en AWS Clean Rooms, consulte los siguientes temas.

- Regla de análisis de agregación
- Regla de análisis de lista
- Regla de análisis personalizada en AWS Clean Rooms

Regla de análisis de agregación

En AWS Clean Rooms, una regla de análisis de agregación genera estadísticas agregadas utilizando las funciones COUNT, SUM y/o AVG en dimensiones opcionales. Cuando la regla de análisis de

agregación se agrega a una tabla configurada, permite al miembro que puede realizar la consulta ejecutar consultas en la tabla configurada.

La regla de análisis de agregación admite casos de uso tales como la planificación de campañas, el alcance mediático, la medición de la frecuencia y la atribución.

La estructura y sintaxis de consulta admitidas se definen en Estructura y sintaxis de consultas de agregación.

Los parámetros de la regla de análisis, definidos en Regla de análisis de agregación: controles de consulta, incluyen los controles de consulta y los controles de resultados de las consultas. Sus controles de consulta incluyen la posibilidad de imponer como requisito que una tabla configurada se una a al menos una tabla configurada propiedad del miembro que puede realizar la consulta, ya sea de forma directa o transitiva. Este requisito le permite asegurarse de que la consulta se ejecute en la intersección (INNER JOIN) entre su tabla y la de ellos.

Estructura y sintaxis de consultas de agregación

Las consultas en tablas que tienen una regla de análisis de agregación deben respetar la siguiente sintaxis.

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

En la siguiente tabla se explica cada una de las expresiones enumeradas en la sintaxis anterior.

Expression	Definición	Ejemplos
select_aggregate_function_expression	Una lista separada por comas que contiene las siguientes expresiones: • `select_aggregation_function_expression` • `select_aggregate_expression` **Note** Debe haber al menos una `select_aggregation_function_expression` en la `select_aggregate_expression` .	`SELECT SUM(PRICE), user_segment`

select_aggregation_function_expression	Una o más funciones de agregación admitidas aplicadas a una o más columnas. Solo se permiten columnas como argumentos de las funciones de agregación.	`AVG(PRICE)`
		
		`COUNT(DISTINCT user_id)`

Expression	Definición	Ejemplos
	Note Debe haber al menos una `select_aggregation_function_expression` en la `select_aggregate_expression` .	

Expression	Definición	Ejemplos

select_grouping_column_expression	Expresión que puede contener cualquier expresión que utilice lo siguiente:
	• Nombres de columna de la tabla
	• Funciones escalares admitidas
	• Literales de cadena
	• Literales numéricos
	
	Note
	`select_aggregate_expression` puede asignar un alias a las columnas con o sin el parámetro `AS`. Para obtener más información, consulte Referencia de SQL de AWS Clean Rooms.
		`TRUNC(timestampColumn)`
		
		`UPPER(campaignName)`

Expression	Definición	Ejemplos
table_expression	Una tabla o combinación de tablas que conecta expresion es condicionales de unión con `join_condition` . `join_condition` devuelve un valor booleano. La `table_expression` admite: • Un tipo JOIN específico (INNER JOIN) • La condición de comparación de igualdad dentro de una `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`

Expression	Definición	Ejemplos

where_expression	Una expresión condicional que devuelve un valor booleano. Puede constar de lo siguiente:
	• Nombres de columna de la tabla
	• Funciones escalares admitidas
	• Operadores matemáticos
	• Literales de cadena
	• Literales numéricos
	
	Las condiciones de comparación admitidas son (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Los operadores lógicos admitidos son (`AND, OR`).
	
	La `where_expression` es opcional.
		`WHERE where_condition`
		
		`WHERE price > 100`
		
		`WHERE TRUNC(timestampColumn) = '1/1/2022'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

group_by_expression	Lista separada por comas de expresiones que cumplen con los requisitos de `select_grouping_column_expression` .	`GROUP BY TRUNC(timestampColumn), UPPER(campaignName), segment`

Expression	Definición	Ejemplos
having_expression	Una expresión condicion al que devuelve un valor booleano. Tienen una función de agregación admitida aplicada a una sola columna (por ejemplo, `SUM(price)`) y se comparan con un literal numérico. Las condiciones admitidas son (`=, >, <, <=, >=, <>, !=`). Los operadores lógicos admitidos son (`AND, OR`). La `having_expression` es opcional.	`HAVING SUM(SALES) > 500`

Expression	Definición	Ejemplos
order_by_expression	Lista de expresiones separadas por comas que es compatible con los mismos requisitos definidos anteriormente en `select_aggregate_expression` . La `order_by_expression` es opcional. **Note** `order_by_expression` admite los parámetros `ASC` y `DESC`. Para obtener más información, consulte los parámetros ASC DESC en Referencia de SQL de AWS Clean Rooms.	`ORDER BY SUM(SALES), UPPER(campaignName)`

En cuanto a la estructura y sintaxis de las consultas de agregación, tenga en cuenta lo siguiente:

- No se admiten comandos SQL distintos de SELECT.
- No se admiten subconsultas ni expresiones de tabla comunes (por ejemplo, WITH).
- No se admiten operadores que combinen varias consultas (por ejemplo, UNION).
- No se admiten los parámetros TOP, LIMIT ni OFFSET.

Regla de análisis de agregación: controles de consulta

Los controles de consulta de agregación permiten controlar cómo se utilizan las columnas de la tabla para consultarla. Por ejemplo, puede controlar qué columna se usa para combinar, qué columna se puede contar o qué columna se puede usar en instrucciones WHERE.

En las secciones siguientes se explica cada uno de los controles.

Temas

Controles de agregación

El uso de controles de agregación permite definir qué funciones de agregación se van a permitir y a qué columnas se deben aplicar. Las funciones de agregación se pueden usar en las expresiones SELECT, HAVING y ORDER BY.

Control	Definición	Uso
`aggregateColumns`	Columnas de tablas configuradas que se permite utilizar en las funciones de agregación.	`aggregateColumns` se puede usar dentro de una función de agregación en las expresiones SELECT, HAVING y ORDER BY. Algunas `aggregateColumns` también se pueden categorizar como `joinColumn` (definición disponible más adelante). La `aggregateColumn` dada no se puede categorizar también como `dimension`

Control	Definición	Uso
		`Column` (definición disponible más adelante).
`function`	Las funciones COUNT, SUM y AVG que se permite utilizar además de `aggregate Columns` .	La `function` se puede aplicar a una `aggregate Columns` que esté asociada a ella.

Controles de combinación

Se utiliza una cláusula `JOIN` para combinar filas de dos o más tablas en función de una columna relacionada entre ellas.

Puede utilizar los controles de combinación para controlar cómo se puede combinar la tabla a otras tablas de la `table_expression`. AWS Clean Rooms solo admite INNER JOIN. Las instrucciones INNER JOIN las declaraciones solo pueden usar columnas que se hayan categorizado explícitamente como `joinColumn` en la regla de análisis, con sujeción a los controles que usted defina.

INNER JOIN deben operar en una `joinColumn` de la tabla configurada y en una `joinColumn` de otra tabla configurada de la colaboración. Usted decide qué columnas de la tabla se pueden usar como `joinColumn`.

Cada condición de coincidencia de la cláusula ON debe utilizar la condición de comparación de igualdad (=) entre dos columnas.

Las condiciones de coincidencia múltiples dentro de una cláusula ON pueden ser:

- Combinación con el operador lógico `AND`
- Separación mediante el operador lógico `OR`

> **Note**
>
> Todas las condiciones de coincidencia JOIN deben coincidir con una fila de cada lado de JOIN. Todos los condicionales conectados por un operador lógico `OR` o `AND` también deben cumplir este requisito.

A continuación se muestra un ejemplo de consulta con un operador lógico `AND`.

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

A continuación se muestra un ejemplo de consulta con un operador lógico `OR`.

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

Control	Definición	Uso
`joinColumns`	Las columnas (si las hay) que se desea permitir que el miembro que puede realizar la consulta utilice en la instrucción INNER JOIN.	También se puede categorizar una `joinColumn` como `aggregateColumn` (consulte Controles de agregación). La misma columna no se puede usar como `joinColumn` y `dimensionColumns` a la vez (consulte más adelante). A menos que también se haya categorizado como `aggregateColumn`, una `joinColumn` no se puede usar en ninguna otra parte de la consulta que no sea INNER JOIN.
`joinRequired`	Controle si necesita una INNER JOIN con una tabla	Si habilita este parámetro, INNER JOIN es obligatorio.

Control	Definición	Uso
	configurada del miembro que puede realizar la consulta.	Si no habilita este parámetro, INNER JOIN es opcional. Presuponiendo que se habilite este parámetro, el miembro que puede realizar la consulta debe incluir una tabla de su propiedad en INNER JOIN. Debe combinar su tabla JOIN con la suya, ya sea de forma directa o transitiva (es decir, combinar su tabla con otra tabla que, a su vez, está combinada con la suya).

A continuación se muestra un ejemplo de transitividad.

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

> **Note**
>
> El miembro que puede realizar la consulta también puede usar el parámetro `joinRequired`. En ese caso, la consulta debe combinar su tabla con al menos otra tabla.

Controles de dimensión

Los controles de dimensión controlan la columna en la cual se pueden filtrar, agrupar o agregar las columnas de agregación.

Control	Definición	Uso
`dimensionColumns`	Las columnas (si las hay) que se permite que el miembro que puede realizar la consulta utilice en SELECT, WHERE, GROUP BY y ORDER BY.	Se puede usar una `dimensionColumn` en SELECT (`select_grouping_column_expression`), WHERE, GROUP BY y ORDER BY. Una misma columna no puede ser a la vez `dimensionColumn`, `joinColumn` y/o `aggregateColumn`.

Funciones escalares

Las funciones escalares controlan qué funciones escalares se pueden usar en las columnas de dimensión.

Control	Definición	Uso
`scalarFunctions`	Las funciones escalares que se pueden utilizar en `dimensionColumns` en la consulta.	Especifica las funciones escalares (si las hay) que se permite (por ejemplo, CAST) aplicar a `dimensionColumns`. Las funciones escalares no se pueden usar además de otras funciones ni dentro de otras funciones. Los argumentos de las funciones escalares pueden ser columnas, literales de cadena o literales numéricos.

Se admiten las siguientes funciones escalares:

- Funciones matemáticas: ABS, CEILING, FLOOR, LOG, LN, ROUND, SQRT
- Funciones de formato de tipo de datos: CAST, CONVERT, TO_CHAR, TO_DATE, TO_NUMBER, TO_TIMESTAMP
- Funciones de cadena: LOWER, UPPER, TRIM, RTRIM, SUBSTRING
  - En el caso de RTRIM, no se permiten conjuntos de caracteres personalizados para recortar.
- Expresiones condicionales: COALESCE
- Funciones de fecha: EXTRACT, GETDATE, CURRENT_DATE, DATEADD
- Otras funciones: TRUNC

Para obtener más información, consulte Referencia de SQL de AWS Clean Rooms.

Regla de análisis de agregación: controles de resultados de consulta

Los controles de resultados de consulta de agregación le permiten controlar qué resultados se devuelven especificando una o más condiciones que debe cumplir cada fila de salida. AWS Clean Rooms admite restricciones de agregación en forma de `COUNT (DISTINCT column) >= X`. Este formato requiere que cada fila agregue al menos X valores diferenciados de una selección de la tabla configurada (por ejemplo, un número mínimo de valores `user_id` diferenciados). Este umbral mínimo se aplica automáticamente, incluso si la consulta enviada en sí misma no utiliza la columna especificada. Se aplican de manera conjunta en cada tabla configurada de la consulta desde las tablas configuradas de cada miembro de la colaboración.

Cada tabla configurada debe tener al menos una restricción de agregación en su regla de análisis. Los propietarios de las tablas configuradas pueden añadir varios `columnName` y su `minimum` asociado y estos se aplicarán conjuntamente.

Restricciones de agregación

Las restricciones de agregación controlan qué filas de los resultados de la consulta se devuelven. Para incluirse en los resultados devueltos, una fila debe cumplir con el número mínimo especificado de valores diferenciados en cada columna especificada en la restricción de agregación. Este requisito se aplica incluso si la columna no se menciona explícitamente en la consulta o en otras partes de la regla de análisis.

Control	Definición	Uso
`columnName`	La `aggregateColumn` que se usa en la condición que debe cumplir cada fila de salida.	Puede tratarse de cualquier columna de la tabla configura da.
`minimum`	El número mínimo de valores diferenciados de la `aggregateColumn` asociada que debe tener la fila de salida (por ejemplo, COUNT DISTINCT) para que se devuelva en los resultados de la consulta.	El `minimum` debe tener al menos un valor de 2.

Estructura de la regla de análisis de agregación

El siguiente ejemplo muestra una estructura predefinida para una regla de análisis de agregación.

En el siguiente ejemplo, *`MyTable`* hace referencia a nuestra tabla de datos. Puede reemplazar cada *`marcador de posición de entrada del usuario`* con información propia.

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

Regla de análisis de agregación: ejemplo

El siguiente ejemplo demuestra cómo dos empresas pueden colaborar en AWS Clean Rooms utilizando el análisis de agregación.

La empresa A tiene datos de clientes y de ventas. La empresa A está interesada en conocer la actividad de devolución de productos. La empresa B es uno de los minoristas de la empresa A y dispone de datos sobre devoluciones. La empresa B también tiene atributos de segmento sobre los clientes que son útiles para la empresa A (por ejemplo, compra de productos relacionados o uso del servicio de atención al cliente del minorista). La empresa B no quiere proporcionar información sobre atributos ni datos sobre devoluciones de los clientes por fila. La empresa B solo quiere habilitar un conjunto de consultas para que la empresa A obtenga estadísticas agregadas sobre los clientes que se superponen dentro de un umbral de agregación mínimo.

La empresa A y la empresa B deciden colaborar para que la empresa A pueda entender la actividad de devolución de productos y ofrecer mejores productos en la empresa B y en otros canales.

Para crear la colaboración y realizar un análisis de agregación, las empresas hacen lo siguiente:

1. La empresa A crea una colaboración y crea una pertenencia. La colaboración tiene a la empresa B como otro miembro de la colaboración. La empresa A habilita el registro de consultas en la colaboración y habilita el registro de consultas en su cuenta.
2. La empresa B crea una pertenencia en la colaboración. Habilita el registro de consultas en su cuenta.
3. La empresa A crea una tabla configurada de ventas.
4. La empresa A añade la siguiente regla de análisis de agregación a la tabla configurada de ventas.

```
{
  "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`: la empresa A quiere contar el número de clientes únicos que se superponen entre los datos de ventas y los datos de devoluciones. La empresa A también quiere sumar el número de `purchases` fabricados para compararlo con el número de `returns`.

`joinColumns`: la empresa A desea usar `identifier` para cotejar los clientes de los datos de ventas con los clientes de los datos de devoluciones. Esto ayudará a la empresa A a relacionar las devoluciones con las compras correctas. También ayudará a la empresa A a segmentar los clientes superpuestos.

`dimensionColumns`: la empresa A usa `dimensionColumns` para filtrar por un producto específico, comparar las compras y las devoluciones correspondientes a un periodo de tiempo

determinado, asegurarse de que la fecha de devolución sea posterior a la fecha del producto y ayudar a segmentar los clientes superpuestos.

`scalarFunctions`: la empresa A selecciona la función escalar CAST para ayudar a actualizar los formatos de tipo de datos si es necesario, basándose en la tabla configurada que la empresa A ha asociado a la colaboración. También añade funciones escalares para ayudar a dar formato a las columnas si es necesario.

`outputConstraints`: la empresa A establece restricciones de salida mínimas. No necesita restringir los resultados, ya que el analista puede ver los datos de la tabla de ventas por fila.

> **Note**
>
> La empresa A no incluye `joinRequired` en la regla de análisis. Ofrece flexibilidad para que el analista consulte solo la tabla de ventas.

5. La empresa B crea una tabla configurada de devoluciones.
6. La empresa B añade la siguiente regla de análisis de agregación a la tabla configurada de devoluciones.

```
{
  "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`: la empresa B permite a la empresa A sumar las `returns` para compararlas con el número de compras. Tienen al menos una columna agregada porque han habilitado una consulta agregada.

`joinColumns`: la empresa B permite a la empresa A combinar por `identifier` para cotejar los clientes de los datos de devoluciones con los clientes de los datos de ventas. Los datos de `identifier` son especialmente sensibles, y tenerlos como `joinColumn` garantiza que los datos no se incluyan nunca en una consulta.

`joinRequired`: la empresa B impone como requisito que las consultas sobre los datos de devoluciones se superpongan con los datos de ventas. No quieren permitir que la empresa A consulte todas las personas de su conjunto de datos. También acordaron esa restricción en su contrato de colaboración.

`dimensionColumns`: la empresa B permite a la empresa A filtrar y agrupar por `state`, `popularpurchases` y `customerserviceuser`, que son atributos únicos que podrían ayudar a realizar el análisis para la empresa A. La empresa B permite a la empresa A usar `returndate` para filtrar la salida por `returndate` que sea posterior a `purchasedate`. Con este filtrado, la salida es más precisa a la hora de evaluar el impacto del cambio de producto.

`scalarFunctions`: la empresa B habilita lo siguiente:

- TRUNC para las fechas
- LOWER y UPPER en caso de que `producttype` se introduzca en un formato distinto en sus datos
- CAST si la empresa A necesita convertir los tipos de datos de las ventas para que sean iguales a los tipos de datos de las devoluciones.

La empresa A no habilita otras funciones escalares porque no cree que sean necesarias para las consultas.

`outputConstraints`: la empresa B establece restricciones de salida mínimas en `hashedemail` para reducir en mayor medida la posibilidad de volver a identificar a los clientes. También añade una restricción de salida mínima en `producttype` para reducir en mayor medida la posibilidad de volver a identificar los productos específicos devueltos. Determinados tipos de productos podrían ser más dominantes en función de las dimensiones de la salida (por ejemplo, `state`). Sus restricciones de salida se aplicarán siempre, independientemente de las restricciones de salida que añada la empresa A a sus datos.

7. La empresa A crea una asociación a la tabla de ventas en la colaboración.
8. La empresa B crea una asociación a la tabla de devoluciones en la colaboración.
9. La empresa A realiza consultas, como las del ejemplo siguiente, para entender mejor la cantidad de devoluciones de la empresa B en comparación con el total de compras por ubicación en 2022.

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

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

10. La empresa A y la empresa B revisan los registros de consultas. La empresa B comprueba que la consulta se ajusta a lo acordado en el contrato de colaboración.

Solución de problemas relacionados con reglas de análisis de agregación

Utilice la información que se incluye aquí para diagnosticar y solucionar problemas frecuentes cuando utilice reglas de análisis de agregación.

Problemas

- Mi consulta no ha devuelto ningún resultado

Mi consulta no ha devuelto ningún resultado

Esto puede ocurrir cuando no hay resultados coincidentes o cuando los resultados coincidentes no cumplen uno o más umbrales de agregación mínimos.

Para obtener más información sobre los umbrales de agregación mínimos, consulte Regla de análisis de agregación: ejemplo.

Regla de análisis de lista

En AWS Clean Rooms, una regla de análisis de lista genera listas de nivel de fila de la superposición entre la tabla configurada a la que se agrega y las tablas configuradas del miembro que puede realizar la consulta. El miembro que puede realizar consultas ejecuta consultas que incluyen una regla de análisis de lista.

El tipo de regla de análisis de listas admite casos de uso como el enriquecimiento y la creación de audiencia.

Para obtener más información sobre la estructura y la sintaxis de consulta predefinidas de esta regla de análisis, consulte Estructura predefinida de la regla de análisis de lista.

Los parámetros de la regla de análisis de lista, que se define en Regla de análisis de lista: controles de consulta, tienen controles de consulta. Estos controles de consulta incluyen la posibilidad de seleccionar las columnas que se pueden enumerar en la salida. La consulta debe tener al menos una combinación con una tabla configurada del miembro que puede realizar consultas, ya sea de forma directa o transitiva.

No hay controles de resultados de consulta como los que existen para la regla de análisis de agregación.

Las consultas de lista solo pueden utilizar operadores matemáticos. No pueden usar otras funciones (por ejemplo, de agregación o escalares).

Temas

- Estructura y sintaxis de las consultas de lista
- Regla de análisis de lista: controles de consulta
- Estructura predefinida de la regla de análisis de lista
- Regla de análisis de lista: ejemplo

Estructura y sintaxis de las consultas de lista

Las consultas de las tablas que tienen una regla de análisis de lista deben respetar la siguiente sintaxis.

```
--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]
```

En la siguiente tabla se explica cada una de las expresiones enumeradas en la sintaxis anterior.

Expression	Definición	Ejemplos
select_list_expression	Una lista separada por comas que contiene al menos un nombre de columna de tabla. Es obligatorio un parámetro DISTINCT. **Note** La select_list_expression pueden asignar un alias a las columnas con o sin el parámetro AS. También admite el parámetro TOP. Para obtener más información, consulte Referencia de SQL deAWS Clean Rooms.	SELECT DISTINCT segment
table_expression	Una tabla, o combinación de tablas, con join_condition para conectarla a join_condition . join_condition devuelve un valor booleano. La table_expression admite: • Un tipo JOIN específico (INNER JOIN)	FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2

Expression	Definición	Ejemplos
	• Las condiciones de comparación de igualdad dentro de una `join_condition (=)` • Operadores lógicos (`AND`, `OR`).	

`where_expression`	Una expresión condicional que devuelve un valor booleano. Puede constar de los siguientes elementos:
	• Nombres de columna de la tabla
	• Operadores matemáticos
	• Literales de cadena
	• Literales numéricos
	
	Las condiciones de comparación admitidas son (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Los operadores lógicos admitidos son (`AND, OR`).
	
	La `where_expression` es opcional.
		`WHERE state + '_' + city = 'NY_NYC'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

Expression	Definición	Ejemplos
limit_expression	Esta expresión debe tener adoptar un entero positivo. También se puede intercambiar con un parámetro TOP. La `limit_expression` es opcional.	`LIMIT 100`

En cuanto a la estructura y sintaxis de las consultas de lista, tenga en cuenta lo siguiente:

- No se admiten comandos SQL distintos de SELECT.
- No se admiten subconsultas ni expresiones de tabla comunes (por ejemplo, WITH).
- No se admiten las cláusulas HAVING, GROUP BY ni ORDER BY.
- No se admite el parámetro OFFSET.

Regla de análisis de lista: controles de consulta

Los controles de consulta de lista le permiten controlar cómo se utilizan las columnas de su tabla a la hora de consultar esta última. Por ejemplo, puede controlar qué columna se usa para combinar, o qué columna se puede usar en una instrucción SELECT y en una cláusula WHERE.

En las secciones siguientes se explica cada uno de los controles.

Temas

Controles de combinación

Los controles de combinación le permiten controlar cómo se puede combinar su tabla a otras tablas en la table_expression. AWS Clean Rooms solo admite INNER JOIN. En la regla de análisis de lista, se requiere al menos una INNER JOIN, y el miembro que puede realizar consultas debe incluir una tabla de su propiedad en la INNER JOIN. Esto significa que deben combinar su tabla con la suya, ya sea de forma directa o transitiva.

A continuación se muestra un ejemplo de transitividad.

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

Las instrucciones INNER JOIN solo pueden usar columnas que se hayan categorizado explícitamente como `joinColumn` en la regla de análisis.

La instrucción INNER JOIN debe operar en una `joinColumn` de su tabla configurada y en una `joinColumn` de otra tabla configurada de la colaboración. Usted decide qué columnas de la tabla se pueden usar como `joinColumn`.

Cada condición de coincidencia de la cláusula ON debe utilizar la condición de comparación de igualdad (=) entre dos columnas.

Las condiciones de coincidencia múltiples dentro de una cláusula ON pueden ser:

- Combinación con el operador lógico `AND`
- Separación mediante el operador lógico `OR`

> **Note**
>
> Todas las condiciones de coincidencia JOIN deben coincidir con una fila de cada lado de JOIN. Todos los condicionales conectados por un operador lógico `OR` o `AND` también deben cumplir este requisito.

A continuación se muestra un ejemplo de consulta con un operador lógico `AND`.

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

A continuación se muestra un ejemplo de consulta con un operador lógico `OR`.

```
SELECT some_col, other_col
```

```
FROM table1
    JOIN table2
    ON table1.id = table2.id OR table1.name = table2.name
```

Control	Definición	Uso
`joinColumns`	Las columnas que se desea permitir que el miembro que puede realizar consultas utilice en la instrucción INNER JOIN.	Una misma columna no se puede categorizar como `joinColumn` y `listColumn` a la vez (consulte Controles de lista). `joinColumn` no se puede usar en ninguna otra parte de la consulta que no sea INNER JOIN.

Controles de lista

Los controles de lista controlan las columnas que se pueden enumerar en el resultado de la consulta (es decir, se pueden usar en la instrucción SELECT) o se pueden usar para filtrar los resultados (es decir, se pueden usar en la WHERE declaración).

Control	Definición	Uso
`listColumns`	Las columnas que se permite que el miembro que puede realizar consultas utilice en SELECT y WHERE	Se puede usar una `listColumn` en SELECT y WHERE. Una misma columna no se puede usar como `listColumn` y `joinColumn` a la vez.

Estructura predefinida de la regla de análisis de lista

El siguiente ejemplo incluye una estructura predefinida que muestra cómo completar una regla de análisis de lista.

En el siguiente ejemplo, *MyTable* hace referencia a nuestra tabla de datos. Puede reemplazar cada *marcador de posición de entrada del usuario* con información propia.

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

Regla de análisis de lista: ejemplo

El siguiente ejemplo demuestra cómo dos empresas pueden colaborar en AWS Clean Rooms utilizando el análisis de lista.

La empresa A dispone de datos de administración de las relaciones con los clientes (CRM). La empresa A desea obtener datos de segmento adicionales sobre sus clientes para conocer mejor a estos últimos y, posiblemente, utilizar los atributos como entrada en otros análisis. La empresa B tiene datos de segmento compuestos por atributos de segmento únicos que creó basándose en sus datos de primera parte. La empresa B desea proporcionar los atributos de segmento únicos a la empresa A solo para aquellos clientes que se superponen entre sus datos y los datos de la empresa A.

Las empresas deciden colaborar para que la empresa A pueda enriquecer los datos superpuestos. La empresa A es el miembro que puede realizar consultas y la empresa B es el colaborador.

Para crear una colaboración y ejecutar en ella un análisis de lista, las empresas hacen lo siguiente:

1. La empresa A crea una colaboración y crea una pertenencia. La colaboración tiene a la empresa B como un miembro más de la colaboración. La empresa A habilita el registro de consultas en la colaboración y habilita el registro de consultas en su cuenta.
2. La empresa B crea una pertenencia en la colaboración. Habilita el registro de consultas en su cuenta.
3. La empresa A crea una tabla configurada de CRM.
4. La empresa A agrega la regla de análisis a la tabla configurada por el cliente, como se muestra en el siguiente ejemplo.

```
{
  "joinColumns": [
    "identifier1",
```

```
    "identifier2"
  ],
  "listColumns": [
    "internalid",
    "segment1",
    "segment2",
    "customercategory"
  ]
}
```

`joinColumns`: la empresa A quiere usar `hashedemail` y/o `thirdpartyid` (obtenidos de un proveedor de identidad) para cotejar los clientes de los datos de CRM con los clientes de los datos de segmento. Esto ayudará a garantizar que la empresa A relacione los datos enriquecidos con los clientes correctos. Tienen dos JoinColumns para mejorar potencialmente la tasa de coincidencia del análisis.

`listColumns`: la empresa A usa `listColumns` para obtener columnas enriquecidas junto con un `internalid` que utiliza en sus propios sistemas. Añade `segment1`, `segment2` y `customercategory` para, potencialmente, limitar el enriquecimiento a segmentos específicos mediante su uso en filtros.

5. La empresa B crea una tabla configurada de segmento.
6. La empresa B añade la regla de análisis a la tabla configurada por de segmento.

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

`joinColumns`: la empresa B permite a la empresa A combinarse con `identifier2` para relacionar a los clientes de los datos de segmento con los datos de CRM. La empresa A y la empresa B trabajaron con el proveedor de identidades para obtener un `identifier2` que se ajustara a la colaboración. No añadieron otras `joinColumns` porque creían que `identifier2` proporciona la tasa de coincidencia más alta y precisa y que no se precisaban otros identificadores para las consultas.

`listColumns`: la empresa B permite a la empresa A enriquecer sus datos con los atributos `segment3` y `segment4`, que son atributos únicos que han creado, recopilado y alineado en (con el cliente A) para formar parte del enriquecimiento de datos. Quieren que la empresa A obtenga estos segmentos para solaparlos a nivel de fila, ya que se trata de una colaboración de enriquecimiento de datos.

7. La empresa A crea una asociación a la tabla de CRM en la colaboración.
8. La empresa B crea una asociación a la tabla de segmento en la colaboración.
9. La empresa A ejecuta consultas, como la siguiente, para enriquecer los datos de clientes que se solapan.

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

10. La empresa A y la empresa B revisan los registros de consultas. La empresa B comprueba que la consulta se ajusta a lo acordado en el contrato de colaboración.

Regla de análisis personalizada en AWS Clean Rooms

En AWS Clean Rooms, una regla de análisis personalizada es un nuevo tipo de regla de análisis que permite ejecutar consultas personalizadas en la tabla configurada. Las consultas SQL personalizadas mantienen la restricción de tener solo el comando SELECT, pero pueden usar más constructos SQL que las consultas de agregación y las consultas de lista (por ejemplo, funciones de ventana, OUTER JOIN, CTE o subconsultas; consulte Referencia de SQL de AWS Clean Rooms para obtener una lista completa). Las consultas SQL personalizadas no tienen que seguir una estructura de consulta como las consultas de agregación y las consultas de lista.

La regla de análisis personalizada admite casos de uso más avanzados que los que admite una regla de análisis de agregación y de lista, como análisis de atribución personalizado, análisis comparativo, análisis de incrementalidad y detección de audiencias. Esto se suma a un superconjunto de casos de uso compatibles con la regla de análisis de agregación y de lista.

La regla de análisis personalizado también admite privacidad diferencial. La privacidad diferencial es un marco matemáticamente riguroso para la protección de la privacidad de los datos. Para obtener más información, consulte AWS Clean Rooms Privacidad diferencial. Al crear una plantilla

de análisis, AWS Clean Rooms Differential Privacy comprueba la plantilla para determinar si es compatible con la estructura de consultas de uso general de AWS Clean Rooms Differential Privacy. Esta validación garantiza que no se cree una plantilla de análisis que no esté permitida con una tabla con protección de privacidad diferencial.

Para configurar la regla de análisis personalizada, los propietarios de los datos pueden optar por permitir que determinadas consultas personalizadas, almacenadas en plantillas de análisis, se ejecuten en sus tablas configuradas. Los propietarios de los datos revisan las plantillas de análisis antes de añadirlas al control de análisis permitido en la regla de análisis personalizada. Las plantillas de análisis están disponibles y visibles solo en la colaboración en la que se crean (incluso si la tabla está asociada a otras colaboraciones) y solo las puede ejecutar el miembro que pueda realizar consultas en esa colaboración.

Como alternativa, los miembros pueden optar por permitir que otros miembros (proveedores de consultas) creen consultas sin revisión. Los miembros añaden las cuentas de proveedores de consultas que los proveedores de consultas permitidos pueden controlar en la regla de análisis personalizada. Si el proveedor de consultas es el miembro que puede realizar la consulta, este puede ejecutar cualquier consulta directamente en la tabla configurada. Los proveedores de consultas también pueden crear consultas mediante la creación de plantillas de análisis. Todas las consultas que hayan creado los proveedores de consultas pueden ejecutarse automáticamente en la tabla en todas las colaboraciones en las que Cuenta de AWS esté presente y la tabla esté asociada.

Los propietarios de los datos solo pueden permitir que las plantillas de análisis o las cuentas creen consultas, pero no ambas. Si el propietario de los datos lo deja en blanco, el miembro que puede realizar la consulta no puede ejecutar consultas en la tabla configurada.

Temas

Estructura predefinida de la regla de análisis personalizada

El siguiente ejemplo incluye una estructura predefinida que muestra cómo completar una regla de análisis personalizada con la privacidad diferencia activada. El valor `userIdentifier` es la columna que identifica de forma exclusiva a los usuarios, como user_id. Si tiene dos o más tablas con privacidad diferencial activada en una colaboración, es AWS Clean Rooms necesario configurar

la misma columna que la columna de identificación de usuario en ambas reglas de análisis para mantener una definición coherente de los usuarios en todas las tablas.

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

Puede:

- Añadir ARN de plantillas de análisis al control de análisis permitidos. En este caso, el control `allowedAnalysisProviders` no está incluido.

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

- Agregue los Cuenta de AWS ID de los miembros al `allowedAnalysisProviders` control. En este caso, se añade `ANY_QUERY` al control `allowedAnalyses`.

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

Ejemplo de regla de análisis personalizada

El siguiente ejemplo demuestra cómo dos empresas pueden colaborar en el AWS Clean Rooms uso de la regla de análisis personalizada.

La empresa A tiene datos de clientes y de ventas. La empresa A está interesada en conocer la incrementalidad de las ventas de una campaña publicitaria en el sitio de la empresa B. La empresa B

tiene datos de visualizaciones y atributos de segmento que son útiles para la empresa (por ejemplo, el dispositivo utilizado para ver la publicidad).

La empresa A tiene una consulta de incrementalidad específica que quiere ejecutar en la colaboración.

Para crear una colaboración y ejecutar en ella un análisis personalizado, las empresas hacen lo siguiente:

1. La empresa A crea una colaboración y crea una pertenencia. La colaboración tiene a la empresa B como un miembro más de la colaboración. La empresa A habilita el registro de consultas en la colaboración y habilita el registro de consultas en su cuenta.
2. La empresa B crea una pertenencia en la colaboración. Habilita el registro de consultas en su cuenta.
3. La empresa A crea una tabla configurada de CRM.
4. La empresa A añade una regla de análisis personalizada vacía a la tabla de ventas configurada.
5. La empresa A asocia la tabla configurada de ventas a la colaboración.
6. La empresa B crea una tabla configurada de visualizaciones.
7. La empresa B agrega una regla de análisis personalizada vacía a la tabla configurada de visualizaciones.
8. La empresa B asocia la tabla configurada de visualizaciones a la colaboración.
9. La empresa A visualiza la tabla de ventas y la tabla de visualizaciones asociada a la colaboración y crea una plantilla de análisis, añadiendo la consulta de incrementalidad y el parámetro para el mes de la campaña.

```
{
    "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. La empresa A añade su cuenta (por ejemplo, 444455556666) al control del proveedor de análisis permitido en la regla de análisis personalizada. Utilizan el control de proveedor de análisis permitido porque quieren permitir que las consultas que creen se ejecuten en su tabla configurada de ventas.

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

11. La empresa B ve la plantilla de análisis creada en la colaboración y revisa su contenido, incluidos la cadena de consulta y el parámetro.

12. La empresa B determina que la plantilla de análisis cumple con el caso de uso de incrementalidad y cumple con sus requisitos de privacidad en cuanto a la forma en que se puede consultar su tabla configurada de visualizaciones.

13. La empresa B agrega la plantilla de análisis ARN al control de análisis permitido en la regla de análisis personalizada de la tabla de visualizaciones. Utilizan el control de análisis permitido porque solo quieren permitir que la consulta de incrementalidad se ejecute en su tabla configurada de visualizaciones.

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

14La empresa A ejecuta la plantilla de análisis y utiliza el valor del parámetro `05-01-2023`.

Regla de análisis personalizada con privacidad diferencial

En AWS Clean Rooms, la regla de análisis personalizada admite la privacidad diferencial. La privacidad diferencial es un marco matemáticamente riguroso para la protección de la privacidad de los datos que le ayuda a proteger sus datos contra los intentos de reidentificación.

La privacidad diferencial permite el análisis agregado, como la planificación de campañas publicitarias, la post-ad-campaign medición, la evaluación comparativa en un consorcio de instituciones financieras y las pruebas A/B para la investigación sanitaria.

La estructura y sintaxis de consulta admitidas se definen en Estructura y sintaxis de las consultas.

Regla de análisis personalizada con privacidad diferencial

Analice el ejemplo de regla de análisis personalizado que se presenta en la sección anterior. En este ejemplo se demuestra cómo puede utilizar la privacidad diferencial para proteger sus datos frente a intentos de reidentificación y, al mismo tiempo, permitir que su socio obtenga información crítica para la empresa a partir de sus datos. Supongamos que la empresa B, que tiene los datos de audiencia, quiere proteger sus datos con una privacidad diferencial. Para completar la configuración de privacidad diferencial, la empresa B realiza los siguientes pasos:

1. La empresa B activa la privacidad diferencial mientras añade una regla de análisis personalizada a la tabla configurada de visualizaciones. La empresa B selecciona `viewershipdata.hashedemail` como columna de identificador de usuario.
2. La empresa B añade una política de privacidad diferencial a la colaboración para que su tabla de datos de audiencia esté disponible para su consulta. La empresa B selecciona la política predeterminada para completar rápidamente la configuración.

La empresa A, que desea comprender la incrementalidad de ventas de una campaña publicitaria en el sitio de la empresa B, utiliza la plantilla de análisis. Puesto que la consulta es compatible con la estructura de consulta de uso general de la privacidad diferencial de AWS Clean Rooms , la consulta se ejecuta correctamente.

Estructura y sintaxis de las consultas

Las consultas que contengan al menos una tabla y que tengan activada la privacidad diferencial deben seguir la siguiente sintaxis.

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

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

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

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

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

 window_functions_on_user_id:
```

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

> **Note**
>
> En cuanto a la estructura y sintaxis de las consultas de privacidad diferencial, tenga en cuenta lo siguiente:
>
> - No se admiten las subconsultas.
> - Las expresiones de tabla comunes (CTE) deberían emitir la columna de identificador de usuario si una tabla o CTE incluye datos protegidos por una privacidad diferencial. Los filtros, agrupaciones y agregaciones deben realizarse en el nivel de usuario.
> - Final_select permite las funciones de agregación COUNT DISTINCT, COUNT, SUM, AVG y STDDEV.

Para obtener más información sobre qué palabras clave de SQL se admiten para una privacidad diferencial, consulte Capacidades SQL de AWS Clean Rooms Differential Privacy.

AWS Clean Rooms Privacidad diferencial

AWS Clean Rooms La privacidad diferencial le ayuda a proteger la privacidad de sus usuarios con una técnica respaldada matemáticamente que se implementa con controles intuitivos en unos pocos clics. Al tratarse de una funcionalidad totalmente gestionada, no es necesario tener experiencia previa en materia de privacidad diferencial para evitar que los usuarios vuelvan a identificarse. AWS Clean Rooms añade automáticamente una cantidad de ruido cuidadosamente calibrada a los resultados de las consultas en tiempo de ejecución para ayudar a proteger sus datos a nivel individual.

AWS Clean Rooms Differential Privacy admite una amplia gama de consultas analíticas y es ideal para una amplia variedad de casos de uso, en los que un pequeño error en los resultados de la consulta no comprometa la utilidad del análisis. Con él, sus socios pueden generar información crítica para la empresa sobre campañas publicitarias, decisiones de inversión, investigaciones clínicas y mucho más, todo ello sin necesidad de ninguna configuración adicional por parte de sus socios.

AWS Clean Rooms Differential Privacy protege contra errores de conversión excesivos o inválidos que utilizan funciones escalares o símbolos de operadores matemáticos de forma malintencionada.

Para obtener más información sobre la privacidad AWS Clean Rooms diferencial, consulte los siguientes temas.

Temas

Privacidad diferencial

La privacidad diferencial solo permite obtener información agregada y oculta la contribución de los datos de cualquier persona a esa información. La privacidad diferencial protege los datos de

la colaboración para que el miembro pueda obtener resultados al aprender sobre una persona específica. Sin una privacidad diferencial, el miembro que puede recibir los resultados puede intentar deducir los datos de un usuario individual añadiendo o quitando registros sobre una persona y observando la diferencia en los resultados de las consultas.

Cuando se activa la privacidad diferencial, se añade una cantidad específica de ruido a los resultados de la consulta para ocultar la contribución de los usuarios individuales. Si el miembro que puede recibir los resultados intenta observar la diferencia en los resultados de la consulta después de eliminar los registros sobre una persona de su conjunto de datos, la variabilidad del resultado de la consulta ayuda a impedir la identificación de los datos de la persona. AWS Clean Rooms Differential Privacy utiliza el SampCertmuestreador, una implementación comprobada y correcta desarrollada por. AWS

Cómo funciona Differential Privacy in AWS Clean Rooms

El flujo de trabajo para activar la privacidad diferencial AWS Clean Rooms requiere los siguientes pasos adicionales al completar el flujo de trabajo para AWS Clean Rooms:

1. La privacidad diferencial se activa al añadir una regla de análisis personalizada.
2. Puede configurar la política de privacidad diferencial de la colaboración para que las tablas de datos protegidas con privacidad diferencial estén disponibles para su consulta.

Tras completar estos pasos, el miembro que pueda realizar la consulta podrá empezar a ejecutar consultas sobre datos protegidos por la privacidad diferencial. AWS Clean Rooms devuelve resultados que cumplen con la política de privacidad diferencial. AWS Clean Rooms Differential Privacy registra el número estimado de consultas pendientes que puede ejecutar, de forma similar al indicador de combustible de un automóvil que muestra el nivel de combustible actual del automóvil. El número de consultas que puede ejecutar el miembro que puede realizar la consulta está limitado por los parámetros Presupuesto de privacidad y el Ruido añadido por consulta establecidos en Política de privacidad diferencial.

Consideraciones

Cuando utilices la privacidad diferencial en AWS Clean Rooms, ten en cuenta lo siguiente:

- El miembro que puede recibir los resultados no puede utilizar la privacidad diferencial. Configurará una regla de análisis personalizada con la privacidad diferencial desactivada para las tablas configuradas.

- El miembro que puede realizar consultas no puede unir tablas de dos o más proveedores de datos cuando ambos tienen activada la privacidad diferencial.

Política de privacidad diferencial

La política de privacidad diferencial controla cuántas funciones de agregación puede ejecutar el miembro que puede realizar la consulta en una colaboración. El Presupuesto de privacidad define un recurso común y limitado que se aplica a todas las tablas durante una colaboración. El Ruido agregado por consulta determina la velocidad a la que se agota el presupuesto de privacidad.

Es necesaria una política de privacidad diferencial para que las tablas con protección de privacidad diferencial estén disponibles para su consulta. Se trata de un paso único en una colaboración e incluye dos entradas:

- Presupuesto de privacidad: cuantificado en términos de épsilon, el presupuesto de privacidad controla el nivel de protección de la privacidad. Se trata de un recurso común y limitado que se aplica a todas las tablas protegidas con privacidad diferencial durante la colaboración, ya que el objetivo es conservar la privacidad de los usuarios, cuya información puede estar presente en varias tablas.

  El presupuesto de privacidad se consume cada vez que se ejecuta una consulta en las tablas. Cuando el presupuesto de privacidad se agote por completo, el miembro de la colaboración que puede realizar consultas no podrá ejecutar consultas adicionales hasta que se aumente o actualice. Al establecer un presupuesto de privacidad mayor, el miembro que puede recibir los resultados puede reducir su incertidumbre acerca de las personas que contienen los datos. Elija un presupuesto de privacidad que equilibre sus requisitos de colaboración con sus necesidades de privacidad y tras consultar con los responsables de la toma de decisiones empresariales.

  Si tiene previsto incorporar nuevos datos a la colaboración de forma periódica, puede seleccionar Actualización mensual del presupuesto de privacidad para crear automáticamente un nuevo presupuesto de privacidad cada mes natural. Al elegir esta opción, se mostrarán cantidades arbitrarias de información sobre las filas de datos cuando se consulten repetidamente durante las actualizaciones. Evite elegir esta opción si se van a consultar repetidamente las mismas filas entre las actualizaciones del presupuesto de privacidad.
- El Ruido agregado por consulta se mide en función del número de usuarios cuyas contribuciones desea ocultar. Este valor determina el ritmo al que se agota el presupuesto de privacidad. Un valor de ruido mayor reduce el ritmo al que se agota el presupuesto de privacidad y, por lo tanto, permite

ejecutar más consultas sobre los datos. Sin embargo, esto debe equilibrarse con la publicación de información de datos menos precisa. Al establecer este valor, tenga en cuenta la precisión deseada para obtener información sobre la colaboración.

Puedes usar la política de privacidad diferencial predeterminada para completar rápidamente la configuración o personalizar tu política de privacidad diferencial según tu caso de uso. AWS Clean Rooms Differential Privacy proporciona controles intuitivos para configurar la política. AWS Clean Rooms Differential Privacy le permite obtener una vista previa de la utilidad en términos del número de agregaciones posibles en todas las consultas de sus datos y estimar el número de consultas que se pueden ejecutar en una colaboración de datos.

Puede utilizar los ejemplos interactivos para comprender cómo los distintos valores de Presupuesto de privacidad y Ruido añadido por consulta afectarían a los resultados de los distintos tipos de consultas SQL. En general, es necesario equilibrar sus necesidades de privacidad con el número de consultas que desea permitir y la precisión de esas consultas. Un menor Presupuesto de privacidad o un mayor Ruido añadido por consulta puede proteger mejor la privacidad de los usuarios, pero proporciona información menos significativa a sus socios de colaboración.

Si aumenta el Presupuesto de privacidad y mantiene igual el parámetro Ruido añadido por consulta, el miembro que pueda realizar la consulta podrá ejecutar más agregaciones en sus tablas durante la colaboración. Puede aumentar el Presupuesto de privacidad en cualquier momento durante la colaboración. Si reduce el Presupuesto de privacidad y mantiene igual el parámetro Ruido añadido por consulta, el miembro que pueda realizar la consulta podrá ejecutar menos agregaciones. No puede reducir el Presupuesto de privacidad una vez que el miembro que puede realizar la consulta haya empezado a analizar sus datos.

Si aumenta el Ruido añadido por consulta y mantiene igual la entrada de Presupuesto de privacidad, el miembro que pueda realizar la consulta podrá ejecutar más agregaciones en sus tablas durante la colaboración. Si reduce el Ruido añadido por consulta y mantiene igual la entrada en de Presupuesto de privacidad, el miembro que pueda realizar la consulta podrá ejecutar menos agregaciones. Puede aumentar o disminuir el Ruido agregado por consulta en cualquier momento durante la colaboración.

La política de privacidad diferencial se gestiona mediante las acciones de la API de la plantilla de presupuesto de privacidad.

Capacidades SQL de AWS Clean Rooms Differential Privacy

AWS Clean Rooms Differential Privacy utiliza una estructura de consultas de uso general para admitir consultas SQL complejas. Las plantillas de análisis personalizadas se validan con esta estructura para garantizar que se puedan ejecutar en tablas protegidas por una privacidad diferencial. En la siguiente tabla se indican las funciones compatibles. Para obtener más información, consulte Estructura y sintaxis de las consultas.

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Funciones de agregación	• Función ANY_VALUE • Función APPROXIMATE PERCENTILE_DISC • Función AVG • Funciones COUNT y COUNT DISTINCT • Función LISTAGG • Función MAX • Función MEDIAN • Función MIN • Función PERCENTILE_CONT • Funciones STDDEV_SAMP y STDDEV_POP • Funciones SUM y SUM DISTINCT	Se admiten con la condición de que los CTE que utilicen tablas con protección de privacidad diferencial deben generar datos con registros a nivel de usuario. Debe escribir la expresión SELECT en esos CTE utilizando el formato. `SELECT userIdentifierColumn...'	Agregaciones compatibles: AVG, COUNT, COUNT DISTINCT, STDDEV y SUM.

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
	• Funciones VAR_SAMP y VAR_POP		
CTE	cláusula WITH, subconsulta de cláusula WITH	Se admite con la condición de que los CTE que utilicen tablas con protección de privacidad diferencial deben generar datos con registros a nivel de usuario. Debe escribir la expresión SELECT en esos CTE utilizando el formato. `` `SELECT userIdentifierColumn...' ``	N/A
subconsultas	Subconsulta de lista SELECT, subconsulta de cláusula FROM, subconsulta de cláusula WHERE	No admitido. No se admiten las subconsultas de la consulta que hace referencia a una tabla con la privacidad diferencial activada. Reescribe las subconsultas como expresiones de tabla comunes (CTE).	

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Unir cláusulas	• INNER JOIN • LEFT JOIN • RIGHT JOIN • FULL JOIN • Operador [JOIN] OR • CROSS JOIN	Se admite con la condición de que solo se admitan las funciones JOIN que son equi-joins en las columnas del identificador de usuario y son obligatorias cuando se consultan dos o más tablas con la privacidad diferencial activada. Asegúrese de que las condiciones obligatorias de equi-join sean correctas. Confirme que el propietario de la tabla haya configurado la misma columna de identificador de usuario en todas las tablas para que la definición de usuario siga siendo coherente en todas las tablas. Las funciones CROSS JOIN no se admiten cuando se combinan dos o más relaciones con la privacidad diferencial activada.	
Operadores de establecimiento	UNION, UNION ALL, INTERSECT, EXCEPT | MINUS (son sinónimos)	Todos son compatibles	No compatible

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Funciones de ventana	Funciones de agregación • Función de ventana AVG • Función de ventana COUNT • Función de ventana CUME_DIST • Función de ventana DENSE_RANK • Función de ventana FIRST_VALUE • Función de ventana LAG • Función de ventana LAST_VALUE • Función de ventana LEAD • Funciones de ventana MAX • Funciones de ventana MEDIAN • Funciones de ventana MIN • Función de ventana DENSE_NTH • Función de ventana RATIO_TO_REPORT	Todos son compatibles con la condición de que la columna de identificación de usuario de la cláusula de partición de la función de ventana sea obligatoria cuando se consulte una relación con la privacidad diferencial activada.	No compatible

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
	• Las funciones de ventana STDDEV_SAMP y STDDEV_POP (STDDEV_SAMP y STDDEV son sinónimos) • Funciones de ventana SUM • Las funciones de ventana VAR_SAMP y VAR_POP (VAR_SAMP y VARIANCE son sinónimos) Funciones de clasificación • Función de ventana DENSE_RANK • Función de ventana NTILE • Función de ventana PERCENT_RANK • Función de ventana RANK • Función de ventana ROW_NUMBER		

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Expresiones condicionales	• Expresión condicional CASE • Expresión COALESCE • Funciones GREATEST y LEAST • Funciones NVL y COALESCE • Función NVL2 • Función NULLIF	Todos son compatibles	Todos son compatibles
Condiciones	• Condición de comparación • Condiciones lógicas • Condiciones de coincidencia de patrones • Condiciones de rango BETWEEN • Condición nula	`EXISTS`y `IN` no se pueden usar porque requieren subconsultas. Se admiten todas las demás.	Todos son compatibles

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Funciones de fecha y hora	• Funciones de fecha y hora en transacciones • Operador de concatenación • Funciones ADD_MONTHS • Función CONVERT_TIMEZONE • Función CURRENT_DATE • Función DATEADD • Función DATEDIFF • Funciones DATE_PART • Función DATE_TRUNC • Función EXTRACT • Función GETDATE • Funciones TIMEOFDAY • Función TO_TIMESTAMP • Partes de fecha para funciones de fecha o marca temporal	Todas son compatibles	Todos son compatibles

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Funciones de cadena	• || Operador (concatenación) • Función BTRIM • Función CHAR_LENGTH • Función CHARACTER _LENGTH • Función CHARINDEX • Función CONCAT • Funciones LEFT y RIGHT • Función LEN • Función LENGTH • Función LOWER • Funciones LPAD y RPAD • Función LTRIM • Funciones POSITION • Función REGEXP_COUNT • Función REGEXP_INSTR • Función REGEXP_RE PLACE • Función REGEXP_SUBSTR	Todos son compatibl es	Todos son compatibl es

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
	• Función REPEAT • Función REPLACE • Función REPLICATE • Función REVERSE • Función RTRIM • Función SOUNDEX • Función SPLIT_PART • Función STRPOS • Función SUBSTRING • Función TEXTLEN • Función TRANSLATE • Funciones TRIM • Función UPPER		
Funciones de formato de tipo de datos	• Función CAST • TO_CHAR • Función TO_DATE • TO_NUMBER • Cadenas de formatos de fecha y hora • Cadenas de formatos numéricos	Todos son compatibles	Todos son compatibles

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Funciones hash	• Función MD5 • Función SHA • Función SHA1 • Función SHA2 • MURMUR3_32_HASH	Todos son compatibles	Todos son compatibles
Símbolos de operadores matemáticos	+, -, *,/,% y @	Todos son compatibles	Todos son compatibles

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Funciones matemáticas	• Función ABS • Función ACOS • Función ASIN • Función ATAN • Función ATAN2 • Función CBRT • Función CEILING (o CEIL) • Función COS • Función COT • Función DEGREES • Función DEXP • Función LTRIM • Función DLOG1 • Función DLOG10 • Función EXP • Función FLOOR • Función LN • Función LOG • Función MOD • Función PI • Función POWER • Función RADIANS • Función RANDOM • Función ROUND • Función SIGN • Función SIN • Funciones SQRT	Todos son compatibles	Todos son compatibles

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
	• Función TRUNC		
Funciones de información acerca del tipo SUPER	• Función DECIMAL_PRECISION • Función DECIMAL_SCALE • Función IS_ARRAY • Función IS_BIGINT • Función IS_CHAR • Función IS_DECIMAL • Función IS_FLOAT • Función IS_INTEGER • Función IS_OBJECT • Función IS_SCALAR • Función IS_SMALLINT • Función IS_VARCHAR • Función JSON_TYPEOF	Todos son compatibles	Todos son compatibles

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Funciones VARBYTE	• Función FROM_HEX • Función FROM_VARBYTE • Función TO_HEX • Función TO_VARBYTE	Todos son compatibles	Todos son compatibles
JSON	• Función CAN_JSON_PARSE • Función JSON_EXTRACT_ARRAY_ELEMENT_TEXT • Función JSON_EXTRACT_PATH_TEXT • Función JSON_PARSE • Función JSON_SERIALIZE • Funciones JSON_SERALIZE_TO_VARBYTE	Todos son compatibles	Todos son compatibles

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Funciones de matriz	• Función array • función array_concat • Función array_flatten • Función get_array_length • Función split_to_array • función de submatriz	No admitido	No admitido
GRUPO AMPLIADO POR	AGRUPAR CONJUNTOS, ENROLLAR, CUBOS	No admitido	No admitido
Operación de clasificación	ORDER BY	Se admite con la condición de que la cláusula ORDER BY solo se admita en la cláusula de partición de una función de ventana cuando se consultan tablas con la privacidad diferencial activada.	Compatible
Límites de filas	LIMIT, OFFSET	No se admiten en los CTE que utilizan tablas con protección de privacidad diferencial	Todos son compatibles

Nombre corto	Constructos SQL	Expresiones de tabla comunes (CTE)	Una cláusula SELECT final
Alias de tablas y columnas		Soportado	Soportado
Funciones matemáticas en funciones agregadas		Soportado	Soportado
Funciones escalares dentro de funciones agregadas		Soportado	Soportado

Alternativas comunes para constructos SQL no admitidos

Categoría	Constructo SQL	Alternativa
Funciones de ventana	• LISTAGG • PERCENTILE_CONT • PERCENTILE_DISC	Puede utilizar la función de agregado equivalente con GROUP BY.
Símbolos de operadores matemáticos	• $column ||/ 2 • $column |/ 2 • $column ^ 2	• CBRT • SQRT • POWER($column, 2)
Funciones escalares	• SYSDATE • $column::integer • convert(type, $column)	• CURRENT_DATE • CAST $column AS integer • CAST $column AS type
Literales	INTERVALO «1 SEGUNDO»	INTERVALO «1» SEGUNDO
Límite de filas	TOP n	LÍMITE n

Categoría	Constructo SQL	Alternativa
Join	• USING • NATURAL	La cláusula ON debe contener explícitamente un criterio de unión.

Consejos y ejemplos de consultas sobre privacidad diferencial

AWS Clean Rooms Differential Privacy utiliza una estructura de consulta de uso general para admitir una amplia variedad de estructuras de SQL, como las expresiones de tabla comunes (CTE) para la preparación de datos y las funciones agregadas de uso común, como, o. `COUNT` `SUM` Para ocultar la contribución de cualquier posible usuario a los datos y hacer más ruido al agregado de los resultados de las consultas en tiempo de ejecución, AWS Clean Rooms Differential Privacy exige que, al final, las funciones de agregado se ejecuten en datos de nivel de usuario. `SELECT statement`

En el siguiente ejemplo se utilizan dos tablas denominadas `socialco_impressions` y `socialco_users` de un publicador de medios que quiere proteger los datos mediante una privacidad diferencial y, al mismo tiempo, colaborar con una marca deportiva que utiliza datos `athletic_brand_sales`. El publicador multimedia ha configurado la columna `user_id` como columna de identificador de usuario y, al mismo tiempo, ha habilitado una privacidad diferencial en AWS Clean Rooms. El anunciante no necesita una protección de privacidad diferencial y desea ejecutar una consulta mediante CTE sobre datos combinados. Puesto que su CTE utiliza tablas protegidas por la privacidad diferencial, el anunciante incluye la columna de identificador de usuario de esas tablas protegidas en la lista de columnas de CTE y une las tablas protegidas en la columna de identificador de usuario.

```
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
```

Del mismo modo, si desea ejecutar funciones de ventana en tablas de datos con protección de privacidad diferencial, debe incluir la columna de identificador de usuario en la cláusula `PARTITION BY`.

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

Limitaciones de la privacidad diferencial AWS Clean Rooms

AWS Clean Rooms La privacidad diferencial no aborda las siguientes situaciones:

1. AWS Clean Rooms Differential Privacy no aborda los ataques cronometrados. Por ejemplo, estos ataques son posibles en situaciones en las que un usuario individual contribuye con un gran número de filas y la adición o eliminación de este usuario cambia considerablemente el tiempo de cálculo de la consulta.
2. La privacidad diferencial de AWS Clean Rooms no garantiza la privacidad diferencial cuando una consulta SQL puede provocar desbordamientos o errores de conversión no válidos en tiempo de ejecución debido al uso de determinadas construcciones de SQL. En la siguiente tabla se enumeran algunas construcciones de SQL, pero no todas, que pueden producir errores en tiempo de ejecución y que deben verificarse en las plantillas de análisis. Le recomendamos que apruebe plantillas de análisis que minimicen las posibilidades de que se produzcan dichos errores en tiempo de ejecución y que revise periódicamente los registros de consultas para determinar si las consultas se ajustan al acuerdo de colaboración.

   Las siguientes estructuras de SQL son vulnerables a los errores de desbordamiento:

- Funciones de agregado: AVG, LISTAVG, PERCENTILE_COUNT, PERCENTILE_DISC, SUM/SUM_DISTINCT
- Funciones de formato de tipos de datos: TO_TIMESTAMP, TO_DATE
- Funciones de fecha y hora: ADD_MONTHS, DATEADD, DATEDIFF
- Funciones matemáticas: +, -, *,/, POWER
- Funciones de cadena: ||, CONCAT, REPEAT, REPLICATE
- Funciones de ventana: AVG, LISTAGG, PERCENTILE_COUNT, PERCENTILE_DISC, RATIO_TO_REPORT, SUM

La función de formateo de tipos de datos CAST es vulnerable a errores de conversión no válidos.

AWS Clean Rooms ML

AWS Clean Rooms ML

AWS Clean Rooms ML proporciona un método que preserva la privacidad para que dos partes identifiquen a usuarios similares en sus datos sin necesidad de compartir sus datos entre sí. La primera parte aporta los datos de entrenamiento para AWS Clean Rooms poder crear y configurar un modelo similar y asociarlo a una colaboración. Luego, la segunda parte trae sus datos iniciales AWS Clean Rooms y genera un segmento similar que se parece a los datos de entrenamiento.

Para obtener una explicación más detallada de cómo funciona esto, consulte Trabajos entre cuentas

- Proveedor de datos de entrenamiento: la parte que aporta los datos de entrenamiento, crea y configura un modelo similar y, a continuación, lo asocia a una colaboración.
- Proveedor de datos iniciales: la parte que aporta los datos iniciales, genera un segmento similar y exporta su segmento similar.
- Datos de entrenamiento: los datos del proveedor de datos de entrenamiento, que se utilizan para generar un modelo similar. Los datos de entrenamiento se utilizan para medir la similitud en los comportamientos de los usuarios.

  Los datos de entrenamiento deben contener un ID de usuario, un ID de elemento y una columna de marca de tiempo. De forma opcional, los datos de entrenamiento pueden contener otras interacciones, como características numéricas o categóricas. Algunos ejemplos de interacciones son una lista de los vídeos visualizados, los artículos comprados o los artículos leídos.
- Datos iniciales: los datos del proveedor de datos iniciales, que se utilizan para crear un segmento similar. El resultado del segmento similar es un conjunto de usuarios a partir de los datos de entrenamiento que se parece más a los usuarios iniciales.
- Modelo similar: un modelo de machine learning de los datos de entrenamiento que se utiliza para encontrar usuarios similares en otros conjuntos de datos.

  Cuando se utiliza la API, el término modelo de audiencia se utiliza de manera equivalente a modelo similar. Por ejemplo, utilizas la API de modelos para crear un CreateAudiencemodelo similar.
- Segmento similar: un subconjunto de los datos de entrenamiento que más se parece a los datos iniciales.

Al usar la API, se crea un segmento similar con la API. StartAudienceGenerationJob

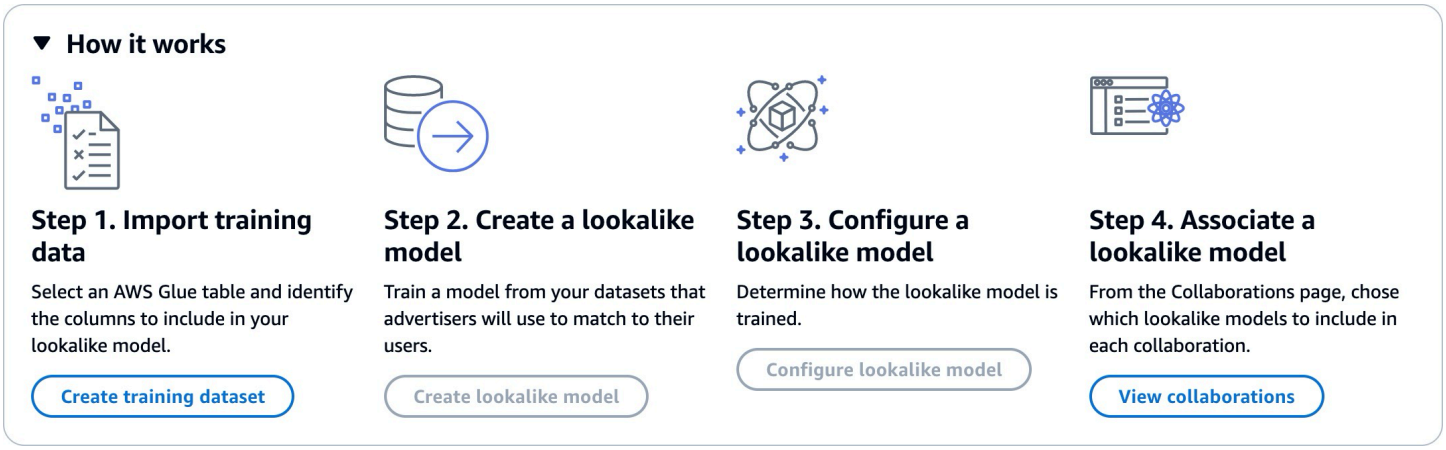
Los datos del proveedor de datos de entrenamiento nunca se comparten con el proveedor de datos iniciales, y viceversa. La salida del segmento similar se comparte con el proveedor de datos de entrenamiento, pero nunca con el proveedor de datos iniciales.

Para obtener más información acerca de los modelos similares, consulte los temas siguientes.

Temas

- Cómo funciona el AWS Clean Rooms aprendizaje automático

Cómo funciona el AWS Clean Rooms aprendizaje automático



Clean Rooms ML requiere que dos partes, un proveedor de datos de formación y un proveedor de datos iniciales, trabajen secuencialmente AWS Clean Rooms para integrar sus datos en una colaboración. Este es el flujo de trabajo que el proveedor de datos de entrenamiento debe completar primero:

1. Los datos del proveedor de datos de formación deben almacenarse en una tabla de catálogo de AWS Glue datos con las interacciones entre usuarios y elementos. Como mínimo, los datos de entrenamiento deben contener una columna de ID de usuario, una columna de ID de interacción y una columna de fecha y hora.
2. El proveedor de datos de entrenamiento registra los datos de entrenamiento con. AWS Clean Rooms
3. El proveedor de datos de entrenamiento crea un modelo similar que se puede compartir con varios proveedores de datos iniciales. El modelo similar es una red neuronal profunda que puede tardar

hasta 24 horas en entrenarse. No se reentrena automáticamente y le recomendamos que vuelva a entrenar el modelo una vez por semana.

4. El proveedor de datos de entrenamiento configura el modelo similar, que incluye si desea compartir las métricas de relevancia y la ubicación en Amazon S3 de los segmentos de salida. El proveedor de datos de entrenamiento puede crear varios modelos similares configurados a partir de un único modelo similar.
5. El proveedor de datos de entrenamiento asocia el modelo de audiencia configurado a una colaboración que se comparte con un proveedor de datos iniciales.

Este es el flujo de trabajo que el proveedor de datos iniciales debe completar a continuación:

1. Los datos del proveedor de datos iniciales deben estar almacenados en un bucket de Amazon S3.
2. El proveedor de datos iniciales comienza la colaboración que comparte con el proveedor de datos de entrenamiento.
3. El proveedor de datos iniciales crea un segmento similar en la pestaña Clean Rooms ML de la página de colaboración.
4. El proveedor de datos iniciales puede evaluar las métricas de relevancia, en caso de que se hayan compartido, y exportar el segmento similar para su uso fuera de AWS Clean Rooms.

Protecciones de privacidad de ML AWS Clean Rooms

Clean Rooms ML está diseñado para reducir el riesgo de ataques de inferencia de miembros, en los que el proveedor de datos de formación puede saber quién está en los datos iniciales y quién está en los datos de formación. Para prevenir este ataque, se toman varias medidas.

En primer lugar, los proveedores de datos iniciales no observan directamente los resultados de Clean Rooms ML y los proveedores de datos de formación nunca pueden observar los datos iniciales. Los proveedores de datos iniciales pueden optar por incluir los datos iniciales en el segmento de salida.

A continuación, se crea el modelo similar a partir de una muestra aleatoria de los datos de entrenamiento. Este ejemplo incluye un número significativo de usuarios que no coinciden con la audiencia inicial. Este proceso hace que sea más difícil determinar si un usuario no aparecía en los datos, lo cual es otra forma de deducir la membresía.

Además, se pueden utilizar varios clientes iniciales para cada parámetro del entrenamiento de modelos similares específicos del inicio. Esto limita cuánto puede sobreajustarse el modelo y, por

lo tanto, cuánto se puede deducir sobre un usuario. Como resultado, se recomienda que el tamaño mínimo de los datos iniciales sea de 500 usuarios.

Por último, nunca se proporcionan métricas en el nivel de usuario a los proveedores de datos de entrenamiento, lo que elimina otra posibilidad de que se produzca un ataque de inferencia de pertenencia.

AWS Clean Rooms Métricas de evaluación del modelo ML

Clean Rooms ML calcula la puntuación de recordación y relevancia para determinar el rendimiento de su modelo. Recall compara la similitud entre los datos similares y los datos de entrenamiento. La puntuación de relevancia se utiliza para decidir qué tan grande debe ser la audiencia, no para determinar si el modelo tiene un buen rendimiento.

El recuerdo es una medida imparcial de la similitud entre el segmento similar y los datos de entrenamiento. El recuerdo es el porcentaje de usuarios más similares (de forma predeterminada, el 20% más similar) de una muestra de los datos de entrenamiento que se incluyen en la audiencia inicial según el trabajo de generación de audiencia. Los valores oscilan entre 0 y 1, mientras que los valores más altos indican una mejor audiencia. Un valor de recuperación aproximadamente igual al porcentaje máximo de intervalo indica que el modelo de audiencia equivale a una selección aleatoria.

Consideramos que esta métrica de evaluación es mejor que la exactitud, la precisión y las puntuaciones de F1, ya que Clean Rooms ML no ha etiquetado con precisión a los usuarios que realmente son negativos al crear su modelo.

La puntuación de relevancia del segmento es una medida de similitud con valores que van desde -1 (menos similar) a 1 (más similar). Clean Rooms ML calcula un conjunto de puntuaciones de relevancia para varios tamaños de segmento a fin de ayudarle a determinar el mejor tamaño de segmento para sus datos. Las puntuaciones de relevancia disminuyen de forma monótona a medida que aumenta el tamaño del segmento, por lo que, a medida que aumenta el tamaño del segmento, pueden ser menos similares a los datos iniciales. Cuando la puntuación de relevancia del segmento llega a 0, el modelo predice que todos los usuarios del segmento similar provienen de la misma distribución que los datos iniciales. Al aumentar el tamaño de salida, es probable que se incluyan usuarios del segmento similar que no pertenezcan a la misma distribución que los datos iniciales.

Las puntuaciones de relevancia se normalizan en una sola campaña y no se deben utilizar para comparar campañas. Las puntuaciones de relevancia no deben utilizarse como prueba única de ningún resultado empresarial, ya que se ven afectadas por varios factores complejos además de la relevancia, como la calidad del inventario, el tipo de inventario, el tiempo de la publicidad, etc.

Las puntuaciones de relevancia no se deben utilizar para juzgar la calidad del inicio, sino para determinar si se puede aumentar o disminuir. Considere los siguientes ejemplos:

- Todas las puntuaciones son positivas: esto indica que hay más usuarios de salida que se consideran similares que los que se incluyen en el segmento similar. Esto es habitual en el caso de los datos iniciales que forman parte de un mercado grande, como el de todos los que han comprado pasta de dientes en el último mes. Le recomendamos que consulte los datos iniciales más pequeños, como los de todas las personas que han comprado pasta dental más de una vez en el último mes.
- Todas las puntuaciones son negativas o negativas para el tamaño de segmento similar deseado: esto indica que Clean Rooms ML predice que no hay suficientes usuarios similares en el tamaño de segmento similar deseado. Esto se puede deber a que los datos iniciales son demasiado específicos o a que el mercado es demasiado pequeño. Recomendamos aplicar menos filtros a los datos iniciales o ampliar el mercado. Por ejemplo, si los datos iniciales originales eran clientes que habían comprado un cochecito y una silla de coche, podría ampliar el mercado a clientes que hayan comprado varios productos para bebés.

Los proveedores de datos de entrenamiento determinan si se exponen las puntuaciones de relevancia y cuáles son los contenedores de bucket en los que se calculan las puntuaciones de relevancia.

¿Trabajando con ML AWS Clean Rooms

Un modelo similar es un modelo de los datos de un proveedor de datos de entrenamiento que permite a un proveedor de datos iniciales crear un segmento similar de los datos del proveedor de datos de entrenamiento que se parezca más a sus datos iniciales. Para crear un modelo similar que se pueda utilizar en una colaboración, debe importar los datos de entrenamiento, crear un modelo similar, configurar ese modelo similar y, después, asociarlo a una colaboración.

Una vez que el proveedor de datos de entrenamiento haya terminado de crear el modelo de ML, podrá crear y exportar el segmento inicial.

Temas

Trabajar con modelos similares (proveedor de datos de entrenamiento)

Importación de datos de entrenamiento

Antes de crear un modelo similar, debe especificar la AWS Glue tabla que contiene los datos de entrenamiento. Clean Rooms ML no almacena una copia de estos datos, solo los metadatos que le permiten acceder a los datos.

Para importar datos de entrenamiento en AWS Clean Rooms

1. Inicia sesión AWS Management Console y abre la AWS Clean Rooms consola con la tuya Cuenta de AWS (si aún no lo has hecho).
2. En el panel de navegación izquierdo, elija Modelos.
3. En la pestaña Conjuntos de datos de entrenamiento, seleccione Crear conjunto de datos de entrenamiento.
4. Escriba un Nombre y una Descripción opcional.
5. En Fuente de datos, elige tu AWS Glue tabla:

   a. Seleccione la Base de datos que desea configurar en la lista desplegable.

   b. Elija la fuente de datos de entrenamiento seleccionando la base de datos y la tabla que desee configurar en las listas desplegables.

   > **Note**
   >
   > Para comprobar que se trata de la tabla correcta, realice una de las siguientes acciones:
   >
   > - Seleccione Ver en AWS Glue.
   > - Active Ver esquema para ver el esquema.

6. Para ver los detalles de la formación, selecciona la columna de identificador de usuario, la columna de identificador de artículo y la columna de fecha y hora de tus datos. Los datos de entrenamiento deben contener estas tres columnas. También puede seleccionar cualquier otra columna que quiera incluir en los datos de entrenamiento.

   Los datos de la columna Timestamp deben estar en el formato Unix de época y tiempo en segundos.

7. En Acceso al servicio, debe especificar un rol de servicio que pueda acceder a sus datos y proporcionar una clave KMS si los datos están cifrados. Elija Crear y usar un nuevo rol de servicio y Clean Rooms ML creará automáticamente un rol de servicio y agregará la política de permisos necesaria. Elija Usar un rol de servicio existente e ingréselo en el campo Nombre del rol de servicio si tiene un rol de servicio específico que quiera usar.

   Si sus datos están cifrados, introduzca su clave de KMS en el AWS KMS keycampo o haga clic en Crear una AWS KMS key para generar una nueva clave de KMS.
8. Si desea habilitar la opción de Etiquetas para el conjunto de datos de entrenamiento, seleccione Añadir nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.
9. Elija Crear el conjunto de datos de entrenamiento.

Para ver la acción de API correspondiente, consulte CreateTrainingConjunto de datos.

Creación de un modelo similar

Una vez que haya creado un conjunto de datos de entrenamiento, estará listo para crear un modelo similar. Puede crear muchos modelos similares a partir de un único conjunto de datos de entrenamiento.

Debe crear una base de datos predeterminada en su función AWS Glue Data Catalog o incluir el `glue:createDatabase` permiso en la función proporcionada.

Para crear un modelo similar en AWS Clean Rooms

1. Inicia sesión en la consola AWS Management Console y abre la AWS Clean Rooms consola con tu Cuenta de AWS (si aún no lo has hecho).
2. En el panel de navegación izquierdo, elija Modelos.
3. En la pestaña Modelos similares, seleccione Crear un modelo similar.
4. En Crear un modelo similar, para Detalles del modelo similar:

   a. Escriba un Nombre y una Descripción opcional.
   b. Seleccione el Conjunto de datos de entrenamiento que desea modelar en la lista desplegable.
   c. Introduzca una ventana de entrenamiento opcional.
5. Si desea activar la configuración de cifrado personalizada para el modelo similar, elija Personalizar la configuración de cifrado y, a continuación, introduzca la clave de KMS.

6. Si desea habilitar la opción de Etiquetas para el modelo similar, seleccione Añadir nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.
7. Seleccione Crear un modelo similar.

Para ver la acción de API correspondiente, consulte CreateAudienceModelo.

Configuración de un modelo similar

Una vez que haya creado un modelo similar, estará listo para configurarlo para su uso en una colaboración. Puede crear varios modelos similares configurados a partir de un único modelo similar.

Para configurar un modelo similar en AWS Clean Rooms

1. Inicie sesión en la consola AWS Management Console y abra la AWS Clean Rooms consola con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Modelos.
3. En la pestaña Modelos similares configurados, elija Configurar un modelo similar.
4. En Configurar un modelo similar, para Detalles del modelo similar configurado:
    a. Escriba un Nombre y una Descripción opcional.
    b. Seleccione el Modelo similar que desea configurar en la lista desplegable.
    c. Elija el Tamaño mínimo de coincidencia de la lista inicial que desee. Es el número mínimo de usuarios de los datos del proveedor de datos iniciales que se superponen con los usuarios de los datos de entrenamiento. Este valor debe ser superior a 0.
5. En Métricas para compartir con otros miembros, elija si desea que el proveedor de datos iniciales de su colaboración reciba métricas del modelo, incluidas las puntuaciones de relevancia.
6. En Ubicación de destino del segmento similar, introduzca el bucket de Amazon S3 al que se exporta el segmento similar. Este depósito debe estar ubicado en la misma región que los demás recursos.
7. En Acceso a los servicios, elija el Nombre del rol de servicio existente que se utilizará para acceder a esta tabla.
8. Elija Configurar un modelo parecido.
9. Si desea habilitar la opción de Etiquetas para el recurso de tabla configurada, seleccione Añadir nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.

Para ver la acción de API correspondiente, consulte CreateConfiguredAudienceModel.

Asociación de un modelo similar configurado

Después de haber configurado un modelo similar, puede asociarlo a una colaboración.

Para asociar un modelo similar configurado en AWS Clean Rooms

1. Inicie sesión en AWS Management Console y abra la AWS Clean Rooms consola con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. En la pestaña Con pertenencia activa, elija una colaboración.
4. En la pestaña Generación de modelos de ML, elija Asociar un modelo similar.
5. En Asociar modelo similar configurado, para Asociar detalles de modelos similares:
   a. Introduzca un Nombre para el modelo de audiencia configurado asociado.
   b. Introduzca una Descripción de la tabla.

      La descripción ayuda a diferenciarlo de otros modelos de audiencia configurados asociados con nombres similares.
6. En Modelo similar configurado, elija un modelo similar configurado de la lista desplegable.
7. Elija Asociar.

Para ver la acción de API correspondiente, consulta CreateConfiguredAudienceModelAsociación.

Actualice un modelo similar configurado

Una vez que haya asociado un modelo similar configurado, puede actualizarlo para cambiar información como el nombre, las métricas que desea compartir o la ubicación de salida de Amazon S3.

Para actualizar un modelo similar configurado asociado en AWS Clean Rooms

1. Inicie sesión en AWS Management Console y abra la AWS Clean Rooms consola con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, selecciona el modelado de aprendizaje automático.
3. En la pestaña Modelos similares configurados, elija un modelo similar configurado y seleccione Editar.

4. En Configurar un modelo similar, para Detalles del modelo similar configurado:
    a. Elija el modelo similar que desee configurar en la lista desplegable.
    b. Elija el Tamaño mínimo de coincidencia de la lista inicial que desee. Es el número mínimo de usuarios de los datos del proveedor de datos iniciales que se superponen con los usuarios de los datos de entrenamiento. Este valor debe ser superior a 0.
5. En Métricas para compartir con otros miembros, elija si desea que el proveedor de datos iniciales de su colaboración reciba métricas del modelo, incluidas las puntuaciones de relevancia.
6. En Ubicación de destino del segmento similar, introduzca el bucket de Amazon S3 al que se exporta el segmento similar. Este depósito debe estar ubicado en la misma región que los demás recursos.
7. En Acceso a los servicios, elija el Nombre del rol de servicio existente que se utilizará para acceder a esta tabla.
8. Para la configuración avanzada del tamaño de los contenedores, elija cómo desea configurar los tamaños de los contenedores de audiencia.
9. Elija Guardar cambios.

Para ver la acción de API correspondiente, consulte UpdateConfiguredAudienceModel.

Trabajar con segmentos similares (proveedor de datos iniciales)

Creación de un segmento similar

Un segmento similar es un subconjunto de los datos de entrenamiento que se parece más a los datos iniciales.

Para crear un segmento similar en AWS Clean Rooms

1. Inicia sesión en la consola AWS Management Console y abre la AWS Clean Rooms consola con tu Cuenta de AWS (si aún no lo has hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. En la pestaña Con pertenencia activa, elija una colaboración.
4. En la pestaña Modelado de ML, seleccione Crear segmento similar.
5. En Crear segmento similar, para Detalles del segmento similar, introduzca un Nombre y una Descripción opcional.

6. En Perfiles iniciales, elija el Origen de entrada de Amazon S3 en el que se almacenan los datos iniciales.
7. En Acceso a los servicios, elija el Nombre del rol de servicio existente que se utilizará para acceder a esta tabla.
8. Si desea habilitar la opción de Etiquetas para el conjunto de datos de entrenamiento, seleccione Añadir nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.
9. Elija Crear segmento similar.

Para ver la acción de API correspondiente, consulte StartAudienceGenerationJob.

Exportación de un segmento similar

Después de crear un segmento similar, puede exportar esos datos a un bucket de Amazon S3.

Para exportar un segmento similar a AWS Clean Rooms

1. Inicia sesión en la consola AWS Management Console y abre la AWS Clean Rooms consola con tu Cuenta de AWS (si aún no lo has hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. En la pestaña Con pertenencia activa, elija una colaboración.
4. En la pestaña Modelado de ML, seleccione un segmento similar y elija Exportar.
5. En Exportar modelo similar, para Exportar detalles de modelo similar, introduzca un Nombre y una Descripción opcional.
6. En Tamaño del segmento, elija el tamaño que desee para el segmento exportado.
7. Seleccione Exportar.

Para ver la acción de API correspondiente, consulte StartAudienceExportJob.

Siguientes pasos

Ahora que ha creado un modelo similar y ha exportado un segmento inicial, está preparado para:

- Administración AWS Clean Rooms

Computación criptográfica para Clean Rooms

La computación criptográfica para Clean Rooms (C3R) es una capacidad AWS Clean Rooms que se puede utilizar además de las reglas de análisis. Con C3R, las organizaciones pueden recopilar datos confidenciales para obtener nuevos conocimientos a partir del análisis de datos al tiempo que limitan criptográficamente la información que puede conocer cualquiera de las partes que interviene en el proceso. C3R lo pueden utilizar dos o más partes que deseen colaborar con sus datos confidenciales, pero que estén obligadas a usar solo datos cifrados en la nube.

El cliente de cifrado C3R es una herramienta de cifrado del lado del cliente que puede utilizar para cifrar sus datos y utilizarlos con ellos. AWS Clean Rooms Cuando se usa el cliente de cifrado C3R, los datos permanecen protegidos criptográficamente mientras se utilizan en una colaboración de AWS Clean Rooms . Al igual que en una AWS Clean Rooms colaboración habitual, los datos de entrada son tablas de bases de datos relacionales y el cálculo se expresa como una consulta SQL. Sin embargo, C3R admite solo un subconjunto limitado de consultas SQL en datos cifrados.

En concreto, C3R admite las instrucciones SQL JOIN y SELECT en datos protegidos criptográficamente. Cada columna de la tabla de entrada se puede utilizar exactamente en uno de los siguientes tipos de instrucciones SQL:

- Las columnas que están protegidas criptográficamente para su uso en instrucciones JOIN se denominan columnas fingerprint.
- Las columnas que están protegidas criptográficamente para su uso en instrucciones SELECT se denominan columnas sealed.
- Las columnas que no están protegidas criptográficamente para su uso en instrucciones JOIN o SELECT se denominan columnas cleartext.

En algunos casos, se admiten instrucciones GROUP BY en columnas fingerprint. Para obtener más información, consulte Columnas Fingerprint. Actualmente, C3R no admite el uso de otros constructos SQL en datos cifrados, como cláusulas WHERE o funciones de agregación como SUM y AVERAGE, ni siquiera si están permitidas por las reglas de análisis pertinentes.

C3R está diseñado para proteger los datos de celdas específicas de una tabla. Con la configuración predeterminada de C3R, los datos subyacentes que un cliente pone a disposición de terceros a través de una colaboración permanecen cifrados mientras el contenido se utiliza en AWS Clean Rooms. C3R utiliza el cifrado AES-GCM estándar del sector para todas las columnas sealed, y una

función pseudoaleatoria estándar del sector, denominada "código de autenticación de mensajes basado en hash (HMAC)", para proteger las columnas fingerprint.

A pesar de que C3R cifra los datos de las tablas, es posible que aún se pueda inferir la siguiente información:

- Información sobre las propias tablas, incluido el número de columnas, los nombres de columna y el número de filas de la tabla.
- Como ocurre con la mayoría de las formas de cifrado estándar, C3R no intenta ocultar la longitud de los valores cifrados. C3R ofrece la posibilidad de rellenar los valores cifrados para ocultar la longitud exacta del texto sin cifrar. Sin embargo, aun así se podría revelar un límite superior de la longitud del texto sin cifrar de cada columna a un tercero.
- Información de registro, como cuándo se agregó una fila determinada a una tabla cifrada de C3R.

Para obtener más información acerca de CR3, consulte los siguientes temas.

Temas

Consideraciones al utilizar la computación criptográfica para Clean Rooms

La computación criptográfica para Clean Rooms (C3R) busca maximizar la protección de los datos. Sin embargo, algunos casos de uso pueden beneficiarse de niveles más bajos de protección de datos a cambio de funcionalidades adicionales. Puede hacer estas concesiones específicas modificando C3R a partir de su configuración más segura. Como cliente, debe conocer estas

ventajas y desventajas, y determinar si son apropiadas para su caso de uso. Entre las ventajas que debe considerar se incluyen las siguientes:

Temas

- Permitir cleartext mixto y datos cifrados en sus tablas
- Permitir valores repetidos en columnas fingerprint
- Disminuir las restricciones de nomenclatura de las columnas fingerprint
- Determinar cómo se representan los valores NULL

Para obtener más información sobre cómo establecer parámetros para estos escenarios, consulte Parámetros de computación criptográfica.

Permitir cleartext mixto y datos cifrados en sus tablas

Hacer que todos los datos se cifren en el cliente proporciona la máxima protección de datos. Sin embargo, esto limita ciertos tipos de consultas (por ejemplo, la función de agregación SUM). El riesgo de permitir datos de cleartext es que es factible que cualquier persona con acceso a las tablas cifradas pueda inferir cierta información sobre los valores cifrados. Esto podría hacerse realizando un análisis estadístico de los datos de cleartext y de los datos relacionados.

Por ejemplo, supongamos que tiene las columnas de `City` y `State`. La columna `City` es cleartext y la columna `State` está cifrada. Cuando ve el valor `Chicago` en la columna `City`, esto le ayuda a determinar con una alta probabilidad que el `State` es `Illinois`. Por el contrario, si una columna es `City` y la otra columna es `EmailAddress`, es poco probable que un cleartext `City` revele algo sobre una `EmailAddress` cifrada.

Para obtener más información acerca del parámetro para este escenario, consulte Parámetro Permitir columnas cleartext.

Permitir valores repetidos en columnas fingerprint

Para optar por un método más seguro, presuponemos que cualquier columna fingerprint contiene exactamente una instancia de una variable. En una columna fingerprint no se puede repetir ningún elemento. El cliente de cifrado de C3R asigna estos valores cleartext a valores únicos que son indistinguibles de los valores aleatorios. Por lo tanto, es imposible inferir información acerca del cleartext a partir de estos valores aleatorios.

El riesgo de los valores repetidos en una columna fingerprint es que estos valores repetidos resulten en valores repetidos que parezcan aleatorios. Por lo tanto, cualquier persona que tenga acceso a las tablas cifradas podría, en teoría, realizar un análisis estadístico de las columnas fingerprint que podría revelar información sobre los valores cleartext.

De nuevo, presupongamos que la columna fingerprint es `State`, y que cada fila de la tabla corresponde a un hogar estadounidense. Un análisis de frecuencia permitiría inferir qué estado es `California` y cuál es `Wyoming` con una alta probabilidad. Esta inferencia es posible porque `California` tiene muchos más residentes que `Wyoming`. Por el contrario, presupongamos que la columna fingerprint está en un identificador de hogar y que cada hogar aparece en la base de datos entre 1 y 4 veces en una base de datos de millones de entradas. Es poco probable que un análisis de frecuencia revele información útil.

Para obtener más información acerca del parámetro para este escenario, consulte Parámetro Permitir duplicados.

Disminuir las restricciones de nomenclatura de las columnas fingerprint

De forma predeterminada, presuponemos que, cuando se combinan dos tablas utilizando columnas fingerprint cifradas, dichas columnas tienen el mismo nombre en cada tabla. El motivo técnico de este resultado es que, de forma predeterminada, deducimos una clave criptográfica diferente para cifrar cada columna fingerprint. Esa clave se deriva de una combinación de la clave secreta compartida de la colaboración y el nombre de la columna. Si intentamos combinar dos columnas con nombres de columna diferentes, obtenemos claves diferentes y no podemos procesar una combinación válida.

Para solucionar este problema, puede desactivar la característica que deriva las claves a partir de cada nombre de columna. A continuación, el cliente de cifrado de C3R utiliza una única clave derivada para todas las columnas fingerprint. El riesgo reside en que se pueda realizar otro tipo de análisis de frecuencia que pueda revelar información.

Volvamos al ejemplo de `City` y `State`. Si derivamos los mismos valores aleatorios para cada columna fingerprint (al no incorporar el nombre de columna), `New  York` tiene el mismo valor aleatorio en las columnas `City` y `State`. Nueva York es una de las pocas ciudades de EE. UU. donde el nombre de `City` coincide con el nombre del `State` nombre. Por el contrario, si su conjunto de datos tiene valores completamente diferentes en cada columna, no se filtra información.

Para obtener más información acerca del parámetro para este escenario, consulte Parámetro Permitir JOIN de columnas con nombres diferentes.

Determinar cómo se representan los valores NULL

La opción que tiene a su disposición consiste en procesar criptográficamente los valores NULL (cifrado y HMAC) como cualquier otro valor. Si no procesa los valores NULL como cualquier otro valor, es posible que se revele información.

Por ejemplo, supongamos que NULL en la columna `Middle Name` de cleartext señala a las personas sin segundo nombre. Si no cifra esos valores, filtrará qué filas de la tabla cifrada se utilizan para personas sin segundo nombre. Esa información podría ser una señal de identificación para algunas personas de ciertas poblaciones. Sin embargo, si procesa los valores NULL criptográficamente, algunas consultas SQL actúan de forma diferente. Por ejemplo, las cláusulas GROUP BY no agruparán los valores fingerprint NULL en columnas fingerprint.

Para obtener más información acerca del parámetro para este escenario, consulte Parámetro Conservar valores NULL.

Tipos de archivo y de datos admitidos en computación criptográfica para Clean Rooms

El cliente de cifrado de C3R reconoce los siguientes tipos de archivo:

- Archivos CSV
- Archivos de Parquet

Puede utilizar el indicador `--fileFormat` del cliente de cifrado de C3R para especificar un formato de archivo de forma explícita. Cuando se especifica de forma explícita, el formato de archivo no viene determinado por la extensión del archivo.

Temas

- Archivos CSV
- Archivos de Parquet
- Cifrar valores que no son de cadena

Archivos CSV

Se presupone que un archivo con la extensión .csv tiene formato CSV y contiene texto codificado en UTF-8. El cliente de cifrado de C3R trata todos los valores como cadenas.

Propiedades admitidas en los archivos .csv

El cliente de cifrado de C3R requiere que los archivos .csv tengan las siguientes propiedades:

- Puede contener o no una fila de encabezado inicial que designe de manera exclusiva cada columna.
- Delimitado por comas. (actualmente no se admiten delimitadores personalizados).
- Texto codificado en UTF-8.

Recorte de espacios en blanco de las entradas .csv

Los espacios en blanco iniciales y finales se recortan de las entradas .csv.

Codificación NULL personalizada para un archivo .csv

Un archivo .csv puede utilizar una codificación personalizada NULL.

Con el cliente de cifrado de C3R, puede especificar codificaciones personalizadas para las entradas NULL de los datos de entrada utilizando el indicador `--csvInputNULLValue=<csv-input-null>`. El cliente de cifrado de C3R puede usar codificaciones personalizadas en el archivo de salida generado para las entradas NULL utilizando el indicador `--csvOutputNULLValue=<csv-output-null>`.

> **Note**
>
> Una entrada NULL se considera carente de contenido, especialmente en el contexto de un formato tabular más enriquecido, como una tabla SQL. Aunque el formato .csv no admite explícitamente esta caracterización por razones históricas, es una convención habitual considerar que una entrada vacía que contiene solo espacios en blanco es NULL. Por lo tanto, ese es el comportamiento predeterminado del cliente de cifrado de C3R, y se puede personalizar según sea necesario.

¿Cómo interpreta C3R las entradas .csv?

La siguiente tabla proporciona ejemplos de cómo se serializan las entradas .csv (de cleartext a cleartext, para mayor claridad) en función de los valores (si los hay) que se proporcionan para los indicadores `--csvInputNULLValue=<csv-input-null>` y `--csvOutputNULLValue=<csv-`

output-null>. Los espacios en blanco iniciales y finales fuera de las comillas se recortan antes de que C3R interprete el significado de cualquier valor.

<csv-input-null>	**<csv-output-null>**	Entrada de entrada	Entrada de salida
Ninguna	Ninguna	,AnyProduct,	,AnyProduct,
Ninguna	Ninguna	, AnyProduct ,	,AnyProduct,
Ninguna	Ninguna	,"AnyProduct",	,AnyProduct,
Ninguna	Ninguna	, "AnyProduct" ,	,AnyProduct,
Ninguna	Ninguna	,,	,,
Ninguna	Ninguna	, ,	,,
Ninguna	Ninguna	,"",	,,
Ninguna	Ninguna	," ",	," ",
Ninguna	Ninguna	, " " ,	," ",
"AnyProduct"	"NULL"	,AnyProduct,	,NULL,
"AnyProduct"	"NULL"	, AnyProduct ,	,NULL,
"AnyProduct"	"NULL"	,"AnyProduct",	,NULL,
"AnyProduct"	"NULL"	, "AnyProduct" ,	,NULL,
Ninguna	"NULL"	,,	,NULL,
Ninguna	"NULL"	, ,	,NULL,
Ninguna	"NULL"	,"",	,NULL,
Ninguna	"NULL"	," ",	," ",

<csv-input-null>	**<csv-output-null>**	Entrada de entrada	Entrada de salida
Ninguna	"NULL"	, " " ,	," ",
""	"NULL"	,,	,NULL,
""	"NULL"	, ,	,NULL,
""	"NULL"	,"",	,"",
""	"NULL"	," ",	," ",
""	"NULL"	, " " ,	," ",
"\"\""	"NULL"	,,	,,
"\"\""	"NULL"	, ,	,,
"\"\""	"NULL"	,"",	,NULL,
"\"\""	"NULL"	," ",	," ",
"\"\""	"NULL"	, " " ,	," ",

Archivo CSV sin encabezados

No es necesario que el archivo .csv de origen tenga encabezados en la primera fila que asignen un nombre exclusivo a cada columna. Sin embargo, un archivo .csv sin una fila de encabezados requiere un esquema de cifrado posicional. Se requiere el esquema de cifrado posicional en lugar del esquema mapeado típico que se usa tanto para los archivos .csv con una fila de encabezado como para los archivos de Parquet.

Un esquema de cifrado posicional especifica las columnas de salida por posición en lugar de por nombre. Un esquema de cifrado mapeado asigna los nombres de columnas de origen a nombres de columnas de destino. Para obtener más información, incluida una explicación detallada y ejemplos de ambos formatos de esquema, consulte Esquemas de tablas mapeados y posicionales.

Archivos de Parquet

Se presupone que un archivo con la extensión .parquet tiene formato de Apache Parquet.

Tipos de datos Parquet admitidos

El cliente de cifrado de C3R puede procesar cualquier dato no complejo (es decir, de tipo primitivo) de un archivo Parquet que corresponda a un tipo de datos admitido por AWS Clean Rooms.

Sin embargo, en las columnas sealed solo se pueden usar columnas de cadena.

Se admiten los siguientes tipos de datos de Parquet:

- Tipo primitivo `Binary` con las siguientes anotaciones lógicas:
  - Ninguno si `--parquetBinaryAsString` está definido (tipo de datos `STRING`)
  - `Decimal(scale, precision)` (tipo de datos `DECIMAL`)
  - `String` (tipo de datos `STRING`)
- Tipo de datos primitivo `Boolean` sin anotación lógica (tipo de datos `BOOLEAN`)
- Tipo de datos primitivo `Double` sin anotación lógica (tipo de datos `DOUBLE`)
- Tipo primitivo `Fixed_Len_Binary_Array` con anotación lógica `Decimal(scale, precision)` (tipo de datos `DECIMAL`)
- Tipo de datos primitivo `Float` sin anotación lógica (tipo de datos `FLOAT`)
- Tipo primitivo `Int32` con las siguientes anotaciones lógicas:
  - Ninguna (tipo de datos `INT`)
  - `Date` (tipo de datos `DATE`)
  - `Decimal(scale, precision)` (tipo de datos `DECIMAL`)
  - `Int(16, true)` (tipo de datos `SMALLINT`)
  - `Int(32, true)` (tipo de datos `INT`)
- Tipo de datos primitivo `Int64` con las siguientes anotaciones lógicas:
  - Ninguna (tipo de datos `BIGINT`)
  - `Decimal(scale, precision)` (tipo de datos `DECIMAL`)
  - `Int(64, true)` (tipo de datos `BIGINT`)
  - `Timestamp(isUTCAdjusted, TimeUnit.MILLIS)` (tipo de datos `TIMESTAMP`)
  - `Timestamp(isUTCAdjusted, TimeUnit.MICROS)` (tipo de datos `TIMESTAMP`)

- `Timestamp(isUTCAdjusted, TimeUnit.NANOS)` (tipo de datos `TIMESTAMP`)

Cifrar valores que no son de cadena

Actualmente, solo se admiten valores de cadena en las columnas sealed.

En el caso de los archivos .csv, el cliente de cifrado de C3R trata todos los valores como texto codificado en UTF-8 y no intenta interpretarlos de forma diferente antes del cifrado.

En el caso de las columnas de huella digital, los tipos se agrupan en clases de equivalencia. Una clase de equivalencia es un conjunto de tipos de datos que se pueden comparar de forma inequívoca para determinar su igualdad mediante un tipo de datos representativo.

Las clases de equivalencia permiten asignar huellas dactilares idénticas al mismo valor semántico independientemente de la representación original. Sin embargo, el mismo valor en dos clases de equivalencia no dará como resultado la misma columna de huella digital.

Por ejemplo, al valor `INTEGRAL 42` se le asignará la misma huella digital independientemente de si originalmente era `SMALLINT`, `INT` o `BIGINT`. Además, el valor `INTEGRAL 0` nunca coincidirá con el valor `BOOLEAN FALSE` (que se representa mediante el valor `0`).

Las columnas de huellas digitales admiten las siguientes clases de equivalencia y los tipos de AWS Clean Rooms datos correspondientes:

Clase de equivalencia	Tipo de datos AWS Clean Rooms admitido
`BOOLEAN`	`BOOLEAN`
`DATE`	`DATE`
`INTEGRAL`	`BIGINT`, `INT`, `SMALLINT`
`STRING`	`CHAR`, `STRING`, `VARCHAR`

Nombres de columnas en computación criptográfica para Clean Rooms

De forma predeterminada, los nombres de columnas son importantes en computación criptográfica para Clean Rooms.

Si el valor del parámetro Permitir JOIN de columnas con nombres diferentes es false, se utilizan los nombres de columna durante el cifrado de las columnas fingerprint. Por este motivo, de forma predeterminada, los colaboradores deben coordinarse con antelación y utilizar los mismos nombres de columna de destino para los datos que se utilizarán en las instrucciones JOIN en las consultas. De forma predeterminada, las columnas cifradas para JOIN con nombres diferentes no ejecutan correctamente la instrucción JOIN en ningún valor.

Si el valor del parámetro Permitir JOIN de columnas con nombres diferentes es true, las instrucciones JOIN en columnas cifradas como columnas fingerprint se ejecutan correctamente. Cifrar los datos con este parámetro puede permitir cierta inferencia de los valores cleartext. Por ejemplo, si una fila tiene el mismo valor de código de autenticación de mensajes basado en hash (HMAC) tanto en la columna `City` como en la columna `State`, el valor podría ser `New York`.

Normalización de los nombres de encabezado de columna

El cliente de cifrado de C3R normaliza los nombres de los encabezados de columna. Se eliminan todos los espacios en blanco iniciales y finales, y el nombre de la columna se cambia a minúsculas en el resultado transformado.

La normalización se aplica antes de cualquier otro cómputo, cálculo u otra operación que pueda verse afectada por los nombres de columna. El archivo de salida emitido contiene solo los nombres normalizados.

Tipos de columnas en computación criptográfica para Clean Rooms

En este tema se proporciona información sobre los tipos de columnas en computación criptográfica para Clean Rooms.

Temas

- Columnas selladas
- Columnas Cleartext

Columnas Fingerprint

Las columnas Fingerprint son columnas que están protegidas criptográficamente para su uso en instrucciones JOIN.

Los datos de las columnas fingerprint no se pueden descifrar. Solo se pueden descifrar los datos de las columnas selladas.

Las columnas Fingerprint solo deben usarse en las siguientes cláusulas y funciones SQL:

- JOIN (INNER, OUTER, LEFT, RIGHT, or FULL) frente a otras columnas fingerprint:
  - Si el valor del parámetro `allowJoinsOnColumnsWithDifferentNames` se establece en `false`, ambas columnas fingerprint de la JOIN deben tener también el mismo nombre.
- `SELECT COUNT()`
- `SELECT COUNT(DISTINCT )`
- `GROUP BY` (usar solo si la colaboración ha definido el valor del parámetro `preserveNulls` como `true`).

Las consultas que infrinjan estas restricciones pueden arrojar resultados incorrectos.

Columnas selladas

Las columnas selladas son columnas que están protegidas criptográficamente para su uso en instrucciones SELECT.

Las columnas selladas solo deben usarse en las siguientes cláusulas y funciones SQL:

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

> **Note**
>
> `SELECT COUNT(DISTINCT )` no se admite.

Las consultas que infrinjan estas restricciones pueden arrojar resultados incorrectos.

Rellenar datos de una columna sealed antes del cifrado

Cuando se especifica que una columna debe ser una columna sealed, C3R pregunta qué tipo de relleno se desea elegir. El relleno de datos antes del cifrado es opcional. Sin relleno (un relleno de tipo `none`), la longitud de los datos cifrados indica el tamaño del cleartext. En determinadas circunstancias, el tamaño del cleartext podría dejar revelar el texto sin formato. Con el relleno (relleno de tipo `fixed` o `max`), todos los valores se rellenan primero hasta alcanzar un tamaño común, y entonces se cifran. Con el relleno, la longitud de los datos cifrados no proporciona información sobre la longitud del cleartext original, salvo por indicar un límite superior de su tamaño.

Si desea rellenar una columna y conoce la longitud máxima en bytes de los datos de esa columna, utilice el relleno `fixed`. Utilice un valor `length` que sea al menos tan grande como la mayor longitud en bytes de esa columna.

> **Note**
>
> Si un valor supera la `length` proporcionada, se produce un error y el cifrado falla.

Si desea rellenar una columna y no conoce la longitud máxima en bytes de los datos de esa columna, utilice `max` el relleno. Este modo de relleno rellena todos los datos hasta la longitud del valor más largo, más los bytes de `length` adicionales.

> **Note**
>
> Es posible que desee cifrar los datos por lotes o actualizar sus tablas con nuevos datos de forma periódica. Tenga en cuenta que el relleno `max` rellenará las entradas hasta la longitud (más el byte de `length`) de la entrada de texto sin formato más larga de un lote determinado. Esto significa que la longitud del texto cifrado puede variar de un lote a otro. Por lo tanto, si conoce la longitud máxima en bytes de una columna, entonces debe utilizar el relleno `fixed` en lugar de `max`.

Columnas Cleartext

Cleartextlas columnas son columnas que no están protegidas criptográficamente para su uso en sentencias o sentencias. JOIN SELECT

Las columnas Cleartext se pueden usar en cualquier parte de la consulta SQL.

Parámetros de computación criptográfica

Hay parámetros de computación criptográfica disponibles para las colaboraciones que utilizan la computación criptográfica para Clean Rooms (C3R) al crear una colaboración. Puede crear una colaboración mediante la AWS Clean Rooms consola o la operación de la `CreateCollaboration` API. En la consola, puede establecer valores para los parámetros en Parámetros de computación criptográfica después de activar la opción Admitir computación criptográfica. Para obtener más información, consulte los siguientes temas.

Temas

- Parámetro Permitir columnas cleartext
- Parámetro Permitir duplicados
- Parámetro Permitir JOIN de columnas con nombres diferentes
- Parámetro Conservar valores NULL

Parámetro Permitir columnas cleartext

En la consola, puede configurar el parámetro Permitir columnas cleartext al crear una colaboración para especificar si se permiten los datos cleartext en una tabla con datos cifrados.

En la siguiente tabla se describen los valores del parámetro Permitir columnas cleartext.

Valor del parámetro	Descripción
No	No se permiten columnas Cleartext en la tabla cifrada. Todos los datos están protegidos criptográficamente.
Sí	Se permiten columnas Cleartext en la tabla cifrada. Las columnas Cleartext no están protegidas criptográficamente y se incluyen como cleartext. Debe tomar nota de lo que los datos cleartext de las filas pueden revelar sobre el resto de datos de la tabla.

Valor del parámetro	Descripción
	Para ejecutar SUM o AVG en columnas específicas, las columnas deben estar en cleartext.

Mediante la operación `CreateCollaboration` de la API, para el parámetro `dataEncryptionMetadata`, puede establecer el valor de `allowCleartext` en `true` o `false`. Para obtener más información sobre las operaciones de la API, consulte Referencia de la API de AWS Clean Rooms.

Las columnas Cleartext corresponden a columnas que se clasifican como cleartext en el esquema específico de la tabla. Los datos de estas columnas no están cifrados y se pueden utilizar de cualquier forma. Las columnas Cleartext pueden resultar útiles si los datos no son confidenciales o si se precisa mayor flexibilidad de la que permite una columna sealed o una columna fingerprint.

Parámetro Permitir duplicados

En la consola, puede configurar el parámetro Permitir duplicados al crear una colaboración para especificar si las columnas cifradas para consultas JOIN pueden contener valores no NULL duplicados.

> **Important**
>
> Los parámetros Permitir duplicados, Permitir JOIN de columnas con nombres diferentes y Conservar los valores NULL tienen efectos distintos pero relacionados.

En la siguiente tabla se describen los valores del parámetro Permitir duplicados.

Valor del parámetro	Descripción
No	No se permiten valores repetidos en una columna fingerprint. Todos los valores de una misma columna fingerprint deben ser únicos.
Sí	Se permiten valores repetidos en una columna fingerprint. Si necesita combinar columnas con valores repetidos, defina este valor en Sí. Si se establece en Sí, los patrones de frecuenci

Valor del parámetro	Descripción
	a que aparecen en las columnas fingerprint de la tabla de C3R o en los resultados pueden implicar información adicional sobre la estructura de los datos cleartext.

Mediante la operación `CreateCollaboration` de la API, en el parámetro `dataEncryptionMetadata`, puede establecer el valor de `allowDuplicates` en `true` o `false`. Para obtener más información sobre las operaciones de la API, consulte Referencia de la API de AWS Clean Rooms.

De forma predeterminada, si se deben usar datos cifrados en consultas JOIN, el cliente de cifrado de C3R requiere que esas columnas no tengan valores duplicados. Con este requisito se pretende aumentar la protección de los datos. Este comportamiento puede contribuir a garantizar que los patrones repetidos en los datos no sean observables. Sin embargo, si desea trabajar con datos cifrados en consultas JOIN y no le preocupan los valores duplicados, el parámetro Permitir duplicados puede desactivar esta comprobación conservadora.

Parámetro Permitir JOIN de columnas con nombres diferentes

En la consola, puede configurar el parámetro Permitir JOIN de columnas con nombres diferentes al crear una colaboración para especificar si se admiten las instrucciones JOIN entre columnas con nombres diferentes.

Para obtener más información, consulte Normalización de los nombres de encabezado de columna

En la siguiente tabla se describen los valores del parámetro Permitir JOIN de columnas con nombres diferentes.

Valor del parámetro	Descripción
No	No se admiten las combinaciones de columnas fingerprint con nombres diferentes. Las instrucciones JOIN solo proporcio nan resultados precisos en las columnas que tienen el mismo nombre.

Valor del parámetro	Descripción
	Important El valor No proporciona una mayor seguridad de la información, pero requiere que los participantes en la colaboración acuerden previamente los nombres de las columnas. Si dos columnas tienen nombres diferentes cuando se cifran como columnas fingerprint y la opción Permitir JOIN de columnas con nombres diferentes está establecida en No, las instrucciones JOIN en esas columnas no producen ningún resultado. Esto se debe a que, después del cifrado, no se comparten valores entre ellas.
Sí	Se admiten las combinaciones de columnas fingerprint con nombres diferentes. Para mayor flexibilidad, los usuarios pueden establecer este valor en Sí, lo que permite las instrucciones JOIN en las columnas independientemente del nombre de la columna. Si se establece en Sí, el cliente de cifrado de C3R no tiene en cuenta el nombre de la columna al proteger las columnas fingerprint. Como resultado, en la tabla de C3R se pueden observar valores comunes en distintas columnas fingerprint. Por ejemplo, si una fila tiene el mismo valor JOIN cifrado tanto en una columna `City` como en una columna `State`, sería razonable inferir que ese valor es `New York`.

Mediante la operación `CreateCollaboration` de la API, para el parámetro `dataEncryptionMetadata`, puede establecer el valor de `allowJoinsOnColumnsWithDifferentNames` en `true` o `false`. Para obtener más información sobre las operaciones de la API, consulte Referencia de la API de AWS Clean Rooms.

De forma predeterminada, el cifrado de las columnas fingerprint se ve afectado por el `targetHeader` de esa columna, establecido en Paso 4: generar un esquema de cifrado para un

archivo tabular . Por lo tanto, el mismo valor cleartext tiene diferentes representaciones cifradas en cada columna fingerprint diferente en la que se cifra.

En algunos casos, este parámetro puede resultar útil para evitar la inferencia de los valores cleartext. Por ejemplo, observar el mismo valor cifrado en las columnas fingerprint `City` y `State` podría llevar a inferir de forma razonable que el valor es `New York`. Sin embargo, el uso de este parámetro requiere una coordinación adicional por adelantado, de modo que todas las columnas que se van a combinar en consultas tengan nombres compartidos.

Puede utilizar el parámetro Permitir JOIN de columnas con nombres diferentes para reducir esta restricción. Si el valor del parámetro se establece en `Yes`, permite que todas las columnas cifradas para JOIN se utilicen juntas independientemente del nombre.

Parámetro Conservar valores NULL

En la consola, puede configurar el parámetro Conservar valores NULL al crear una colaboración para indicar que no hay ningún valor presente en esa columna.

En la siguiente tabla se describen los valores del parámetro Conservar valores NULL.

Valor del parámetro	Descripción
No	Los valores NULL no se conservan. Los valores NULL no aparecen como NULL en una tabla cifrada. Los valores NULL aparecen como valores aleatorios únicos en una tabla de C3R.
Sí	Los valores NULL se conservan. Los valores NULL aparecen como NULL en una tabla cifrada. Si se requiere la semántica SQL de los NULL, puede establecer este valor en Sí. Como resultado, las entradas NULL aparecen como NULL en la tabla de C3R, independientemente de si la columna está cifrada o de la configuración del parámetro Permitir duplicados.

Mediante la operación `CreateCollaboration` de la API, para el parámetro `dataEncryptionMetadata`, puede establecer el valor de `preserveNulls` en `true` o `false`. Para obtener más información sobre las operaciones de la API, consulte Referencia de la API de AWS Clean Rooms.

Si el parámetro Conservar valores NULL está establecido en No para la colaboración:

1. Las entradas NULL de las columnas `cleartext` permanecen inalteradas.
2. Las entradas NULL de las columnas `fingerprint` cifradas se cifran como valores aleatorios para ocultar su contenido. Combinar una columna cifrada con entradas NULL de la columna cleartext no produce ninguna coincidencia para ninguna de las entradas NULL. No se realizan coincidencias porque cada una recibe su propio contenido aleatorio único.
3. Las entradas NULL de las columnas `sealed` cifradas se cifran.

Cuando el valor del parámetro Conservar valores NULL se establece en Sí para la colaboración, las entradas NULL de todas las columnas se mantienen como NULL, independientemente de si la columna está cifrada o no.

El parámetro Conservar valores NULL resulta útil en escenarios tales como el enriquecimiento de datos, donde se desea compartir una falta de información expresada como NULL. El parámetro Conservar valores NULL también es útil en formato fingerprint o HMAC cuando se tienen valores NULL en la columna que se desea ejecutar JOIN o GROUP BY.

Si el valor de los parámetros Permitir duplicados y Conservar valores NULL se establece en No, tener más de una entrada NULL en una columna fingerprint produce un error y detiene el cifrado. Si el valor de cualquiera de los parámetros se establece en Sí, no se produce tal error.

Indicadores opcionales en computación criptográfica para Clean Rooms

En las siguientes secciones se describen los indicadores opcionales que puede configurar al cifrar datos utilizando el cliente de cifrado de C3R para personalizar y probar archivos tabulares.

Temas

- Indicador --csvInputNULLValue
- Indicador --csvOutputNULLValue
- Indicador --enableStackTraces
- Indicador --dryRun
- Indicador --tempDir

Indicador `--csvInputNULLValue`

Puede usar el indicador `--csvInputNULLValue` para especificar codificaciones personalizadas para las entradas NULL de los datos de entrada al cifrar datos utilizando el cliente de cifrado de C3R.

En la siguiente tabla se resumen el uso y los parámetros de este indicador.

Uso	Parámetros
Opcional. Los usuarios pueden especific ar codificaciones personalizadas para las entradas NULL de los datos de entrada.	Codificación especificada por el usuario de valores NULL en el archivo CSV de entrada

Una entrada NULL es una entrada que se considera carente de contenido, específicamente en el contexto de un formato tabular más enriquecido, como una tabla SQL. Aunque el formato .CSV no admite explícitamente esta caracterización por razones históricas, es una convención habitual considerar que una entrada vacía que contiene solo espacios en blanco es NULL. Por lo tanto, ese es el comportamiento predeterminado del cliente de cifrado de C3R, y se puede personalizar según sea necesario.

Indicador `--csvOutputNULLValue`

Puede usar el indicador `--csvOutputNULLValue` para especificar codificaciones personalizadas para las entradas NULL en los datos de salida al cifrar datos con el cliente de cifrado de C3R.

En la siguiente tabla se resumen el uso y los parámetros de este indicador.

Uso	Parámetros
Opcional. Los usuarios pueden especificar codificaciones personalizadas en el archivo de salida generado para las entradas NULL.	Codificación especificada por el usuario de valores NULL en el archivo CSV de salida

Una entrada NULL es una entrada que se considera carente de contenido, específicamente en el contexto de un formato tabular más enriquecido, como una tabla SQL. Aunque el formato .CSV no admite explícitamente esta caracterización por razones históricas, es una convención habitual considerar que una entrada vacía que contiene solo espacios en blanco es NULL. Por lo tanto, ese

es el comportamiento predeterminado del cliente de cifrado de C3R, y se puede personalizar según sea necesario.

Indicador `--enableStackTraces`

Al cifrar datos utilizando el cliente de cifrado de C3R, utilice el indicador `--enableStackTraces` para proporcionar información contextual adicional para notificar errores cuando C3R detecte un error.

AWS no recopila errores. Si encuentras un error, utiliza el seguimiento de pila para solucionar el error tú mismo o envía el seguimiento de pila a AWS Support para obtener ayuda.

En la siguiente tabla se resumen el uso y los parámetros de este indicador.

Uso	Parámetros
Opcional. Se utiliza para proporcionar información contextual adicional para notificar errores cuando el cliente de cifrado de C3R detecta un error.	Ninguna

Indicador `--dryRun`

Los comandos encrypt y decrypt del cliente de cifrado de C3R incluyen un indicador `--dryRun` opcional. El indicador toma todos los argumentos proporcionados por el usuario y comprueba su validez y coherencia.

Puede usar el indicador `--dryRun` para comprobar si su archivo de esquema es válido y coherente con el archivo de entrada correspondiente.

En la siguiente tabla se resumen el uso y los parámetros de este indicador.

Uso	Parámetros
Opcional. Hace que el cliente de cifrado de C3R analice los parámetros y compruebe los archivos, pero no realiza ningún cifrado ni descifrado.	Ninguna

Indicador `--tempDir`

Es posible que desee utilizar un directorio temporal, ya que los archivos cifrados a veces pueden superar en tamaño a los no cifrados, dependiendo de la configuración. Los conjuntos de datos también deben cifrarse por colaboración para funcionar correctamente.

Al cifrar los datos utilizando C3R, utilice el indicador `--tempDir` para especificar la ubicación en la que se pueden crear los archivos temporales mientras se procesa la entrada.

En la siguiente tabla se resumen el uso y los parámetros de este indicador.

Uso	Parámetros
Los usuarios pueden especificar la ubicación en la que se pueden crear los archivos temporales mientras se procesa la entrada.	El valor predeterminado es el directorio temporal del sistema.

Consultas con computación criptográfica para Clean Rooms

En este tema se proporciona información sobre cómo escribir consultas que utilicen tablas de datos cifradas mediante computación criptográfica para Clean Rooms.

Temas

- Consultas que se ramifican en NULL
- Asignar una columna de origen a varias columnas de destino
- Usar los mismos datos para las consultas JOIN y SELECT

Consultas que se ramifican en NULL

Tener una ramificación de consulta en una instrucción NULL significa usar una sintaxis similar a `IF x IS NULL THEN 0 ELSE 1`.

Las consultas siempre se pueden ramificar en instrucciones NULL en columnas de cleartext.

Las consultas se pueden ramificar en instrucciones NULL en columnas sealed y en columnas fingerprint solo cuando el valor del parámetro Conservar valores NULL (`preserveNulls`) está establecido en `true`.

Las consultas que infrinjan estas restricciones pueden arrojar resultados incorrectos.

Asignar una columna de origen a varias columnas de destino

Una columna de origen puede asignarse a varias columnas de destino. Por ejemplo, puede que desee utilizar tanto JOIN como SELECT en una columna.

Para obtener más información, consulte Usar los mismos datos para las consultas JOIN y SELECT.

Usar los mismos datos para las consultas JOIN y SELECT

Si los datos de una columna no son confidenciales, pueden aparecer en una columna de destino de cleartext, lo que permite utilizarlos para cualquier fin.

Si los datos de una columna son confidenciales y deben usarse tanto para las consultas JOIN como para las consultas SELECT, asigne dicha columna de origen a dos columnas de destino del archivo de salida. Una columna se cifra con el `type` como columna fingerprint y la otra columna se cifra con el `type` como columna sellada. La generación de esquemas interactivos del cliente de cifrado C3R sugiere sufijos de encabezado de `_fingerprint` y `_sealed`. Estos sufijos de encabezado pueden ser una convención útil para diferenciar dichas columnas rápidamente.

Directrices para el cliente de cifrado de C3R

El cliente de cifrado de C3R es una herramienta que permite a las organizaciones recopilar datos confidenciales para obtener nueva información procesable a partir del análisis de datos. La herramienta limita criptográficamente lo que puede aprender cualquiera de las partes y durante el proceso. AWS Si bien esto es de vital importancia, el proceso de protección criptográfica de los datos puede suponer una sobrecarga considerable, tanto en términos de recursos de computación como de almacenamiento. Por lo tanto, es importante entender las ventajas y desventajas de usar cada ajuste y saber cómo optimizar la configuración sin dejar de mantener las garantías criptográficas deseadas. Este tema se centra en las implicaciones para el rendimiento de las diferentes configuraciones del cliente de cifrado de C3R y los esquemas.

Todas las configuraciones de cifrado del cliente de cifrado de C3R ofrecen diferentes garantías criptográficas. De forma predeterminada, los ajustes más seguros son aquellos en el nivel de la colaboración. Al habilitar funciones adicionales al crear una colaboración, se debilitan las garantías de privacidad, ya que se permite realizar actividades como análisis de frecuencia en el texto cifrado. Para obtener más información sobre cómo se utilizan estas configuraciones y cuáles son sus implicaciones, consulte Computación criptográfica.

Temas

Implicaciones en el rendimiento de los tipos de columnas

C3R utiliza tres tipos de columnas: cleartext, fingerprint y sealed. Cada uno de estos tipos de columnas proporciona diferentes garantías criptográficas y tiene distintos usos previstos. En las siguientes secciones se analizan las implicaciones de rendimiento del tipo de columna y el impacto de cada ajuste en el rendimiento.

Temas

Columnas Cleartext

Las columnas Cleartext no se modifican con respecto a su formato original ni se procesan criptográficamente en modo alguno. Este tipo de columna no se puede configurar y no afecta al rendimiento en términos de almacenamiento o de computación.

Columnas Fingerprint

Las columnas Fingerprint están previstas para utilizarse para combinar datos de varias tablas. Para ello, el tamaño del texto cifrado resultante debe ser siempre el mismo. Sin embargo, estas columnas se ven afectadas por los ajustes en el nivel de la colaboración. Las columnas Fingerprint pueden incidir en distinto grado en el tamaño del archivo de salida en función del cleartext contenido en la entrada.

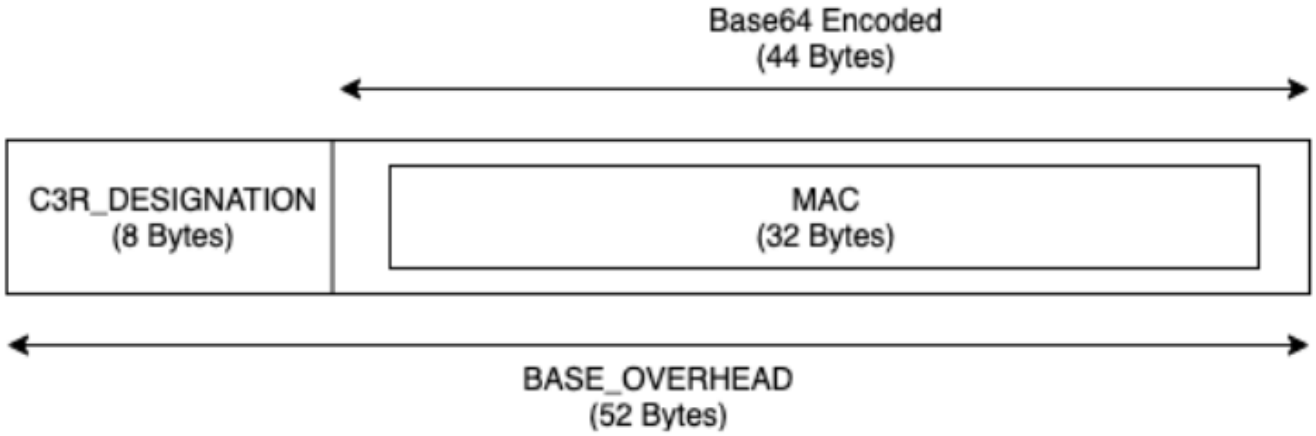
Temas

Sobrecarga de base para las columnas fingerprint

Existe una sobrecarga de base para las columnas fingerprint. Esta sobrecarga es constante y sustituye al tamaño de los bytes de cleartext.

Los datos de las columnas fingerprint se procesan criptográficamente mediante una función de código de autenticación de mensajes basado en hash (HMAC), que convierte los datos en un código de autenticación de mensajes (MAC) de 32 bytes. A continuación, estos datos se procesan a través de un codificador base64, lo que aumenta el tamaño del byte aproximadamente un 33 por ciento. Va precedido de una designación C3R de 8 bytes para designar el tipo de columna a la que pertenecen los datos y la versión de cliente que los generó. El resultado final es de 52 bytes. Este resultado se multiplica entonces por el número de filas para obtener la sobrecarga de base total (utilice el número total de valores distintos de `null` si `preserveNulls` se establece en true).

En la siguiente imagen se muestra cómo *`BASE_OVERHEAD = C3R_DESIGNATION + (MAC * 1.33)`*



El texto cifrado de salida de las columnas fingerprint siempre será de 52 bytes. Esto puede suponer una disminución significativa del almacenamiento si el promedio de los datos de cleartext de entrada es superior a 52 bytes (por ejemplo, las direcciones postales completas). Esto puede suponer un aumento significativo del almacenamiento si el promedio de los datos de cleartext de entrada es inferior a 52 bytes (por ejemplo, las edades de los clientes).

Ajustes de colaboración para las columnas fingerprint

Ajuste **`preserveNulls`**

Cuando el ajuste de nivel de la colaboración `preserveNulls` es `false` (predeterminado), cada valor `null` se sustituye por 32 bytes únicos y aleatorios y se procesa como si no fuera

`null`. El resultado es que cada valor `null` tiene ahora 52 bytes. Esto puede añadir requisitos de almacenamiento importantes para las tablas que contienen datos muy dispersos en comparación con cuando este ajuste es `true` y los valores `null` se transfieren como `null`.

Si no necesita las garantías de privacidad de este ajuste y prefiere retener los valores `null` de sus conjuntos de datos, habilite el ajuste `preserveNulls` en el momento de crear la colaboración. El ajuste `preserveNulls` no se puede cambiar una vez creada la colaboración.

Datos de ejemplo para una columna fingerprint

El siguiente es un ejemplo de conjunto de datos de entrada y salida para una columna fingerprint con los ajustes de configuración que se deben reproducir. Otros ajustes a nivel de la colaboración, como `allowCleartext` y `allowDuplicates`, no afectan a los resultados y se pueden configurar como `true` o `false` si se intenta reproducirlos localmente.

Secreto compartido de ejemplo: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

ID de colaboración de ejemplo: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

allowJoinsOnColumnsWithDifferentNames: `True` Este ajuste no afecta al rendimiento ni a los requisitos de almacenamiento. Sin embargo, este ajuste hace que la elección del nombre de la columna sea irrelevante al reproducir los valores que se muestran en las siguientes tablas.

Ejemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Salida	`null`
Determinista	`Yes`
Bytes de entrada	0
Bytes de salida	0

Ejemplo 2

Entrada	`null`

`preserveNulls`	`FALSE`
Salida	`01:hmac:3lkFjthvV3IUu6mMvFc1a +XAHwgw/ElmOq4p3Yg25kk=`
Determinista	No
Bytes de entrada	0
Bytes de salida	52

Ejemplo 3

Entrada	`empty string`
`preserveNulls`	-
Salida	`01:hmac:oKTgi3Gba+eUb3JteSz 2EMgXUkF1WgM77UP0Ydw5kPQ=`
Determinista	`Yes`
Bytes de entrada	0
Bytes de salida	52

Ejemplo 4

Entrada	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Salida	`01:hmac:kU/IqwG7FMmzzshr0B9 scomE0UJUEE7j9keTctplGww=`
Determinista	`Yes`
Bytes de entrada	26

Bytes de salida	52

Ejemplo 5

Entrada	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Salida	`01:hmac:ks3htnQbw2vdhCRFF6J NzW5LMndJaHG57uvE26mBtSs=`
Determinista	`Yes`
Bytes de entrada	62
Bytes de salida	52

Solución de problemas con columnas fingerprint

¿Por qué el texto cifrado de mis columnas fingerprint es varias veces mayor que el tamaño del cleartext que figuraba en ellas?

El texto cifrado de una columna de fingerprint tiene siempre una longitud de 52 bytes. Si los datos de entrada eran pequeños (por ejemplo, las edades de los clientes), mostrarán un aumento considerable de tamaño. Esto también puede ocurrir si el ajuste `preserveNulls` se define como `false`.

¿Por qué el texto cifrado de mis columnas de fingerprint es varias veces más pequeño que el cleartext que contiene?

El texto cifrado de una columna de fingerprint tiene siempre una longitud de 52 bytes. Si los datos de entrada eran grandes (por ejemplo, las direcciones completas de los clientes), su tamaño se reducirá considerablemente.

¿Cómo sé si necesito las garantías criptográficas que ofrece **`preserveNulls`**?

Lamentablemente, la respuesta es que depende. Como mínimo, se deben revisar los the section called “Parámetros” en cuanto a la forma en que el ajuste `preserveNulls` protege sus datos. No obstante, le recomendamos que consulte los requisitos de manejo de datos de su organización y cualquier contrato aplicable a la colaboración correspondiente.

¿Por qué tengo que incurrir en la sobrecarga de base64?

Para permitir la compatibilidad con los formatos de archivo tabulares como CSV, es necesaria la codificación base64. Si bien algunos formatos de archivo como Parquet podrían admitir representaciones binarias de datos, es importante que todos los participantes en una colaboración representen los datos de la misma manera para garantizar que los resultados de las consultas sean correctos.

Columnas Sealed

Las columnas Sealed están diseñadas para utilizarse para transferir datos entre los miembros de una colaboración. El texto cifrado de estas columnas no es determinista y tiene un impacto significativo tanto en el rendimiento como en el almacenamiento en función de cómo se configuren las columnas. Estas columnas se pueden configurar de forma individual y, a menudo, son las que más influyen en el rendimiento del cliente de cifrado de C3R y en el tamaño del archivo de salida resultante.

Temas

- Sobrecarga de base para las columnas sealed
- Ajustes de colaboración para las columnas sealed
- Columnas sealed de configuración de esquema: tipos de relleno
- Datos de ejemplo para una columna sealed
- Solución de problemas con columnas sealed

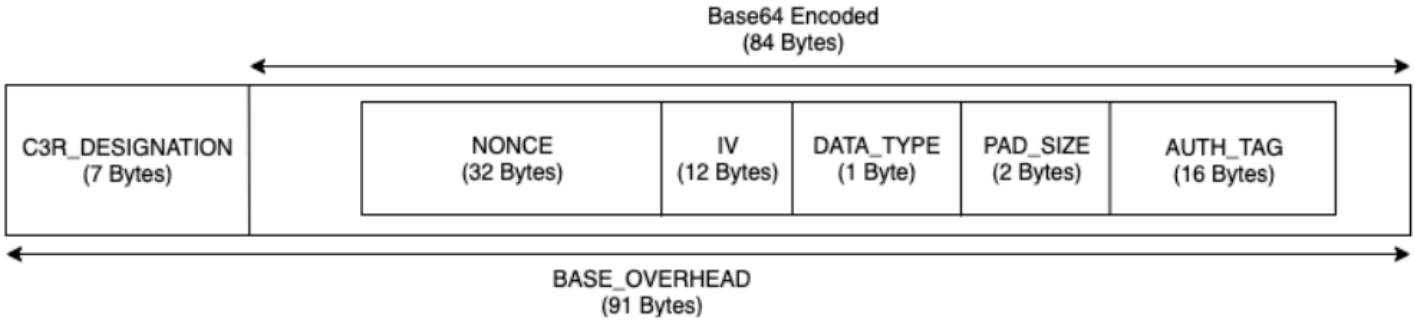
Sobrecarga de base para las columnas sealed

Existe una sobrecarga de base para las columnas sealed. Esta sobrecarga es constante y se suma al tamaño de los bytes de cleartext y de relleno (si los hubiera).

Antes de cualquier cifrado, a los datos de las columnas sealed se les añade como prefijo un carácter de 1 byte que designa el tipo de datos que contienen. Si se selecciona el relleno, los datos se rellenan y se añaden 2 bytes que indican el tamaño del relleno. Tras añadir estos bytes, los datos se procesan criptográficamente mediante AES-GCM y se almacenan con IV (12 bytes), nonce

(32 bytes) y Auth Tag (16 bytes). A continuación, estos datos se procesan a través de un codificador base64, lo que aumenta el tamaño del byte aproximadamente un 33 por ciento. Los datos van precedidos de una designación C3R de 7 bytes para indicar el tipo de columna a la que pertenecen los datos y la versión de cliente utilizada para generarlos. El resultado es una sobrecarga de base final de 91 bytes. A continuación, este resultado se puede multiplicar por el número de filas para obtener la sobrecarga de base total (utilice el número total de valores no nulos si `preserveNulls` está definido como true).

En la siguiente imagen se muestra cómo *`BASE_OVERHEAD = C3R_DESIGNATION + ((NONCE + IV + DATA_TYPE + PAD_SIZE + AUTH_TAG) * 1.33)`*



Ajustes de colaboración para las columnas sealed

Ajuste **`preserveNulls`**

Cuando el ajuste en el nivel de la colaboración `preserveNulls` es `false` (predeterminado), cada valor `null` es único, aleatorio de 32 bytes, y se procesa como si no fuera `null`. El resultado es que cada valor `null` tiene ahora 91 bytes (más si se rellena). Esto puede añadir requisitos de almacenamiento importantes para las tablas que contienen datos muy dispersos en comparación con cuando este ajuste es `true` y los valores `null` se transfieren como `null`.

Si no necesita las garantías de privacidad de este ajuste y prefiere retener los valores `null` de sus conjuntos de datos, habilite el ajuste `preserveNulls` en el momento de crear la colaboración. El ajuste `preserveNulls` no se puede cambiar una vez creada la colaboración.

Columnas sealed de configuración de esquema: tipos de relleno

Temas

- Tipo de relleno none
- Tipo de relleno fixed
- Tipo de relleno max

Tipo de relleno **none**

Seleccionar el tipo de relleno `none` no añade ningún relleno al cleartext ni añade ninguna sobrecarga adicional a la sobrecarga de base descrita anteriormente. La ausencia de relleno se traduce en el tamaño de salida más eficiente en términos de espacio. Sin embargo, no proporciona las mismas garantías de privacidad que los tipos de relleno `fixed` y `max`. Esto se debe a que el tamaño del cleartext subyacente es discernible a partir del tamaño del texto cifrado.

Tipo de relleno **fixed**

Seleccionar un tipo de relleno `fixed` es una medida que salvaguarda la privacidad para ocultar la longitud de los datos contenidos en una columna. Esto se hace rellenando todo el cleartext hasta la `pad_length` antes del cifrado. Cualquier dato que supere ese tamaño provoca un fallo del cliente de cifrado de C3R.

Dado que el relleno se añade al cleartext antes de cifrarlo, AES-GCM utiliza un mapeo 1 a 1 de cleartext a texto cifrado en bytes. La codificación base64 añadirá un 33 por ciento. La sobrecarga de almacenamiento adicional del relleno se puede calcular restando la longitud media del cleartext del valor de `pad_length` y multiplicándola por 1,33. El resultado es la sobrecarga promedio de relleno por registro. Este resultado puede entonces multiplicarse por el número de filas para obtener la sobrecarga de relleno total (utilice el número total de valores no `null` si `preserveNulls` está definido como `true`).

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

Se recomienda seleccionar la `pad_length` mínima que abarque el mayor valor de columna. Por ejemplo, si el mayor valor es de 50 bytes, basta con una `pad_length` de 50. Un valor superior a ese solo añadirá sobrecarga de almacenamiento adicional.

El relleno fijo no añade ninguna sobrecarga de computación significativa.

Tipo de relleno **max**

Seleccionar un tipo de relleno `max` es una medida que salvaguarda la privacidad para ocultar la longitud de los datos contenidos en una columna. Esto se hace rellenando todos los cleartext hasta el valor más alto de la columna, más la `pad_length` adicional, antes de cifrarla. Por lo general, el relleno `max` proporciona las mismas garantías que el relleno `fixed` para un único conjunto de datos, al tiempo que permite no conocer el valor de cleartext más alto de la columna. Sin embargo, es posible que el relleno `max` no ofrezca las mismas garantías de privacidad que el relleno `fixed` en todas las actualizaciones, ya que el valor más alto de cada conjuntos de datos podría variar.

Se recomienda seleccionar una `pad_length` adicional de 0 al usar el relleno `max`. Esta longitud rellena todos los valores para que tengan el mismo tamaño que el mayor valor de la columna. Un valor superior a ese solo añadirá sobrecarga de almacenamiento adicional.

Si conoce el valor de cleartext más alto de una columna determinada, le recomendamos que utilice el tipo de relleno `fixed` en su lugar. El uso del relleno `fixed` crea coherencia entre los conjuntos de datos actualizados. El uso del relleno `max` hace que cada subconjunto de datos se rellene hasta el mayor valor presente en el subconjunto.

Datos de ejemplo para una columna sealed

El siguiente es un ejemplo de conjunto de datos de entrada y salida para una columna sealed con los ajustes de configuración que se deben reproducir. Otros ajustes en el nivel de la colaboración, `allowCleartext`, `allowJoinsOnColumnsWithDifferentNames` y `allowDuplicates`, no afectan a los resultados y se pueden definir como `true` o `false` si se intentan reproducir localmente. Aunque estos son los ajustes básicos que se deben reproducir, la columna sealed no es determinista y los valores cambiarán de una vez a otra. El objetivo es mostrar los bytes de entrada en comparación con los bytes de salida. Los valores `pad_length` de ejemplo se han elegido de forma intencionada. Muestran que el relleno `fixed` da como resultado los mismos valores que el relleno `max` con los ajustes de `pad_length` mínima recomendada o cuando se desea un relleno adicional.

Secreto compartido de ejemplo: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

ID de colaboración de ejemplo: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

Temas

- Tipo de relleno none
- Tipo de relleno fixed (ejemplo 1)
- Tipo de relleno fixed (ejemplo 2)
- Tipo de relleno max (ejemplo 1)
- Tipo de relleno max (ejemplo 2)

Tipo de relleno **none**

Ejemplo 1

Entrada	`null`

`preserveNulls`	`TRUE`
Salida	`null`
Determinista	`Yes`
Bytes de entrada	0
Bytes de salida	0

Ejemplo 2

Entrada	`null`
`preserveNulls`	`FALSE`
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSPbNIJfG3iXmu6cbCUrizuV`
Determinista	No
Bytes de entrada	0
Bytes de salida	91

Ejemplo 3

Entrada	`empty string`
`preserveNulls`	-
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSPEM6qR8DWC2PB2GMlX41YK`
Determinista	No

Bytes de entrada	0
Bytes de salida	91

Ejemplo 4

Entrada	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9sGL5VLDQeHzh6DmPpyWNuI=`
Determinista	No
Bytes de entrada	26
Bytes de salida	127

Ejemplo 5

Entrada	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`

Determinista	No
Bytes de entrada	62
Bytes de salida	175

Tipo de relleno **`fixed`** (ejemplo 1)

En este ejemplo, `pad_length` es 62 y la mayor entrada es de 62 bytes.

Ejemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Salida	`null`
Determinista	`Yes`
Bytes de entrada	0
Bytes de salida	0

Ejemplo 2

Entrada	`null`
`preserveNulls`	`FALSE`
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/ hCz7oaIneVsrcoNpATs0GzbnLkor4L+/ aSuA=`
Determinista	No

Bytes de entrada	0
Bytes de salida	175

Ejemplo 3

Entrada	`empty string`
`preserveNulls`	-
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=`
Determinista	No
Bytes de entrada	0
Bytes de salida	175

Ejemplo 4

Entrada	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`

Determinista	No
Bytes de entrada	26
Bytes de salida	175

Ejemplo 5

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

Tipo de relleno **`fixed`** (ejemplo 2)

En este ejemplo, `pad_length` es 162 y la mayor entrada es de 62 bytes.

Ejemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Salida	`null`

Determinista	Yes
Bytes de entrada	0
Bytes de salida	0

Ejemplo 2

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

Ejemplo 3

Entrada	empty string
preserveNulls	-
Salida	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY

	`Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT`
Determinista	No
Bytes de entrada	0
Bytes de salida	307

Ejemplo 4

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

Bytes de salida	307

Ejemplo 5

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

Tipo de relleno **`max`** (ejemplo 1)

En este ejemplo, `pad_length` es 0 y la mayor entrada es de 62 bytes.

Ejemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`

Salida	`null`
Determinista	`Yes`
Bytes de entrada	0
Bytes de salida	0

Ejemplo 2

Entrada	`null`
`preserveNulls`	`FALSE`
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/ hCz7oaIneVsrcoNpATs0GzbnLkor4L+/ aSuA=`
Determinista	No
Bytes de entrada	0
Bytes de salida	175

Ejemplo 3

Entrada	`empty string`
`preserveNulls`	-
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48`

	`Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcoLB53l07VZp A6OwkuXu29CA=`
Determinista	No
Bytes de entrada	0
Bytes de salida	175

Ejemplo 4

Entrada	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcutBAcO+Mb9t uU2KIHH31AWg=`
Determinista	No
Bytes de entrada	26
Bytes de salida	175

Ejemplo 5

Entrada	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-

Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Determinista	No
Bytes de entrada	62
Bytes de salida	175

Tipo de relleno **`max`** (ejemplo 2)

En este ejemplo, `pad_length` es 100 y la mayor entrada es de 62 bytes.

Ejemplo 1

Entrada	`null`
`preserveNulls`	`TRUE`
Salida	`null`
Determinista	`Yes`
Bytes de entrada	0
Bytes de salida	0

Ejemplo 2

Entrada	`null`
`preserveNulls`	`FALSE`

Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb`
Determinista	No
Bytes de entrada	0
Bytes de salida	307

Ejemplo 3

Entrada	`empty string`
`preserveNulls`	-
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT`
Determinista	No

Bytes de entrada	0
Bytes de salida	307

Ejemplo 4

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

Ejemplo 5

Entrada	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Salida	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY`

	`Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/QOQ3cXb/pbvPcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i``
Determinista	No
Bytes de entrada	62
Bytes de salida	307

Solución de problemas con columnas sealed

¿Por qué el texto cifrado de mis columnas sealed es varias veces mayor que el tamaño del cleartext que figuraba en ellas?

Esto depende de varios factores. Por un lado, el texto cifrado de una columna Cleartext siempre tiene una longitud mínima de 91 bytes. Si los datos de entrada eran pequeños (por ejemplo, las edades de los clientes), mostrarán un aumento considerable de tamaño. En segundo lugar, si `preserveNulls` se hubiera definido como `false` y los datos de entrada contuvieran un gran número de valores `null`, cada uno de esos valores `null` se habrá convertido en 91 bytes de texto cifrado. Por último, si se utiliza el relleno, por definición, se añaden bytes a los datos de cleartext antes de cifrarlos.

La mayoría de los datos de una columna sealed son muy pequeños y necesito utilizar relleno. ¿Puedo simplemente eliminar los valores grandes y procesarlos por separado para ahorrar espacio?

No le recomendamos que elimine los valores grandes y los procese por separado. Al hacerlo, se modifican las garantías de privacidad que ofrece el cliente de cifrado de C3R. Como modelo de amenaza, presuponga que un observador puede ver ambos conjuntos de datos cifrados. Si el observador ve que un subconjunto de datos tiene una columna considerablemente más o menos rellena que otro subconjunto, puede hacer inferencias sobre el tamaño de los datos de cada subconjunto. Por ejemplo, imaginemos que una columna `fullName` se rellena hasta un total de

40 bytes en un archivo y se rellena hasta 800 bytes en otro archivo. Un observador podría deducir que un conjunto de datos contiene el nombre más largo del mundo (747 bytes).

¿Debo proporcionar un relleno adicional al usar el tipo de relleno **`max`**?

No. Al utilizar el relleno `max`, se recomienda establecer en 0 la `pad_length` (también conocida como relleno adicional complementario al mayor valor de la columna).

¿Puedo elegir una **`pad_length`** grande al usar el relleno **`fixed`** para evitar tener que preocuparme de que quepa el valor más grande?

Sí, pero la gran longitud de relleno es ineficiente y utiliza más almacenamiento del necesario. Le recomendamos que compruebe el tamaño del mayor valor y que defina la `pad_length` con ese valor.

¿Cómo sé si necesito las garantías criptográficas que ofrece **`preserveNulls`**?

Lamentablemente, la respuesta es que depende. Como mínimo, se deben revisar los Computación criptográfica para Clean Rooms en cuanto a la forma en que el ajuste `preserveNulls` protege sus datos. No obstante, le recomendamos que consulte los requisitos de manejo de datos de su organización y cualquier contrato aplicable a la colaboración correspondiente.

¿Por qué tengo que incurrir en la sobrecarga de base64?

Para permitir la compatibilidad con los formatos de archivo tabulares, como CSV, es necesaria la codificación base64. Si bien algunos formatos de archivo como Parquet podrían admitir representaciones binarias de datos, es importante que todos los participantes en una colaboración representen los datos de la misma manera para garantizar que los resultados de las consultas sean correctos.

Solución de problemas relacionados con el aumento imprevisto de tamaño del texto cifrado

Supongamos que ha cifrado los datos y que el tamaño de los datos resultantes es sorprendentemente grande. Los siguientes pasos pueden ayudarle a identificar dónde se produjo el aumento de tamaño y qué medidas puede adoptar, si las hubiera.

Identificar dónde se produjo el aumento de tamaño

Antes de poder averiguar por qué los datos cifrados son significativamente más grandes que los datos de cleartext, primero debe identificar dónde reside el aumento de tamaño. Las columnas

de Cleartext se pueden ignorar con total seguridad porque permanecen inalteradas. Observe las columnas fingerprint y sealed restantes, y elija una que parezca significativa.

Identificar el motivo por el que se produjo el aumento de tamaño

Una columna de fingerprint o una columna sealed pueden contribuir al aumento de tamaño.

Temas

¿Procede el aumento de tamaño de una columna fingerprint?

Si la columna que más contribuye al aumento del almacenamiento es una columna fingerprint, es probable que se deba a que los datos de cleartext son pequeños (por ejemplo, la edad de los clientes). Cada texto cifrado de fingerprint resultante tiene una longitud de 52 bytes. Lamentablemente, no se puede hacer nada al respecto sobre una column-by-column base sólida. Para obtener más información, consulte Sobrecarga de base para las columnas fingerprint para conocer los detalles de esta columna, incluida su incidencia en los requisitos de almacenamiento.

La otra causa posible del aumento de tamaño de una columna fingerprint es el ajuste de la colaboración `preserveNulls`. Si el ajuste de la colaboración para `preserveNulls` está deshabilitado (ajuste predeterminado), todos los valores `null` de las columnas fingerprint se convertirán en 52 bytes de texto cifrado. No hay nada que se pueda hacer al respecto en la colaboración actual. El ajuste `preserveNulls` se define en el momento en que se crea la colaboración, y todos los colaboradores deben usar el mismo ajuste para garantizar que los resultados de la consulta sean correctos. Para obtener más información sobre el ajuste `preserveNulls` y sobre cómo su habilitación afecta a las garantías de privacidad de los datos, consulte Computación criptográfica.

¿Procede el aumento de tamaño de una columna sealed?

Si la columna que más contribuye al aumento del almacenamiento es una columna sealed, hay algunos detalles que podrían contribuir al aumento de tamaño.

Si los datos de cleartext son pequeños (por ejemplo, las edades de los clientes), cada texto cifrado sealed resultante tiene una longitud mínima de 91 bytes. Lamentablemente, no se puede hacer nada al respecto. Para obtener más información, consulte Sobrecarga de base para las columnas

sealed para conocer los detalles de esta columna, incluida su incidencia en los requisitos de almacenamiento.

La segunda causa principal del aumento del almacenamiento en columnas sealed es el relleno. El relleno añade bytes adicionales al cleartext antes del cifrado para ocultar el tamaño de los valores individuales de un conjunto de datos. Se recomienda establecer el relleno en el valor mínimo posible para el conjunto de datos. Como mínimo, se debe definir `pad_length` para el relleno `fixed` de manera que abarque el mayor valor posible de la columna. Todo ajuste superior a ese no aportará garantías de privacidad adicionales. Por ejemplo, si sabe que el mayor valor posible de una columna puede ser de 50 bytes, le recomendamos que defina la `pad_length` en 50 bytes. Sin embargo, si la columna sealed utiliza el relleno `max`, le recomendamos que lo defina la `pad_length` en 0 bytes. Esto se debe a que el relleno `max` se refiere al relleno adicional que se suma al mayor valor de la columna.

La última causa posible del aumento de tamaño de una columna sealed es el ajuste de la colaboración `preserveNulls`. Si el ajuste de la colaboración para `preserveNulls` está deshabilitado (ajuste predeterminado), todos los valores `null` de las columnas sealed se convertirán en 91 bytes de texto cifrado. No hay nada que se pueda hacer al respecto en la colaboración actual. El ajuste `preserveNulls` se define en el momento en que se crea la colaboración, y todos los colaboradores deben usar el mismo ajuste para garantizar que los resultados de la consulta sean correctos. Para obtener más información sobre los efectos de esta configuración y sobre cómo su activación afecta a las garantías de privacidad de sus datos, consulte Computación criptográfica.

Inicio de sesión de consultas AWS Clean Rooms

El registro de consultas es una función de AWS Clean Rooms. Al crear una colaboración y activar el registro de consultas, los miembros pueden almacenar los registros de consultas relevantes para ellos en Amazon CloudWatch Logs.

Los registros de consultas permiten a los miembros determinar si las consultas cumplen las reglas de análisis y se ajustan al acuerdo de colaboración. Además, los registros de consultas respaldan las auditorías.

Cuando la opción de registro de consultas está activada en la AWS Clean Rooms consola, los registros de consultas incluyen lo siguiente:

- `analysisRule`: la regla de análisis de la tabla configurada.
- `analysisTemplateArn`: la plantilla de análisis que se ejecutó (aparece en función de la regla de análisis).
- `collaborationId`: el identificador único de la colaboración en la que se ejecutó la consulta.
- `configuredTableID`: el identificador único de la tabla configurada a la que hace referencia la consulta.
- `directQueryAnalysisRulePolicy.custom.allowedAnalysis`: la plantilla de análisis que se puede ejecutar en una tabla configurada (aparece según la regla de análisis).
- `directQueryAnalysisRulePolicy.v1.custom.allowedAnalysisProviders`: los proveedores de consultas que tienen permitido crear consultas (aparece según la regla de análisis).
- `eventID`: el identificador único de ejecución de la consulta. Desde el 31 de agosto de 2023, el identificador único coincidirá con el `protectedQueryID`.
- `eventTimestamp`: el momento de ejecución de la consulta.
- `parameters.parametervalue`: los valores de los parámetros (aparecen en función del texto de la consulta).
- `queryText`: la definición SQL de la ejecución de la consulta. Si hay parámetros, se etiquetan como `:parametervalue`.
- `queryValidationErrors`: los errores de consulta durante la validación de la consulta.
- `schemaName`: el nombre de la asociación de tablas configuradas a la que se hace referencia en la consulta.

Recibir registros de consultas

No es necesario realizar ninguna acción aparte de AWS Clean Rooms configurar los registros de consultas. AWS Clean Rooms crea grupos de registro para las colaboraciones después de que cada miembro de la colaboración cree una membresía.

Los miembros que pueden realizar consultas, los miembros que pueden recibir los resultados y los miembros a cuyas tablas de configuración se haga referencia en la consulta recibirán un registro de consultas.

El miembro que puede realizar consultas y el miembro que puede recibir los resultados recibirán registros de consultas para cada tabla configurada a la que se haga referencia en la consulta. Si no son el propietario de la tabla configurada, no podrán ver el ID de la tabla configurada (`configuredTableID`).

Si un miembro tiene varias asociaciones de tablas configuradas a las que se hace referencia en la consulta, recibirá un registro de consultas por cada tabla configurada.

Se crean registros para las consultas que contienen SQL admitido y no admitido en AWS Clean Rooms. Para obtener más información, consulte la Referencia de SQL de AWS Clean Rooms.

También se crean registros cuando las consultas hacen referencia a tablas configuradas que no están asociadas a la colaboración.

No se crean registros si el código SQL no es correcto. AWS Clean Rooms

Los registros de consultas no indican si la consulta se ha realizado correctamente o si se ha entregado el resultado de la consulta. Simplemente confirman que un miembro que puede realizar consultas envió una consulta. Los registros de consultas también confirman que la consulta contiene SQL compatible AWS Clean Rooms y hace referencia a las tablas configuradas asociadas a la colaboración.

Example

Por ejemplo, no se genera un registro si la consulta se canceló después de AWS Clean Rooms validar su conformidad con las reglas de análisis y durante el procesamiento de la consulta.

Si elimina el grupo de registros, debe volver a crearlo manualmente con el mismo nombre de grupo de registros (ID de colaboración de la colaboración). O bien, puede activar y desactivar el registro en su pertenencia.

Para obtener más información acerca de cómo activar el registro de consultas, consulte Crear una colaboración en AWS Clean Rooms.

Para obtener más información sobre Amazon CloudWatch Logs, consulta la Guía del usuario de Amazon CloudWatch Logs.

Usar los registros de consultas

Es aconsejable que los miembros tomen las siguientes medidas de forma periódica:

- Revisar las consultas ejecutadas en la colaboración para comprobar que coinciden con los casos de uso o con las consultas acordadas para la colaboración.

  Para obtener más información sobre cómo ver consultas recientes, consulte Visualización de consultas recientes.
- Revisar las columnas de la tabla configurada que se utilizan en las reglas de análisis de los miembros de la colaboración y en las consultas para asegurarse de que las columnas de la tabla configurada se ajustan a lo acordado para la colaboración.

  Para obtener más información sobre cómo ver las columnas configuradas, consulte Ver tablas y reglas de análisis.

Con AWS Clean Rooms figuración

En los temas siguientes se explica cómo configurarlos AWS Clean Rooms.

Temas

Inscríbase en AWS

Antes de poder usar cualquiera Servicio de AWS AWS Clean Rooms, incluso, debe registrarse en AWS.

Si no tienes uno Cuenta de AWS, sigue los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.
3. Cuando te registras en un Cuenta de AWS, se crea un usuario Cuenta de AWS root. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para realizar tareas que requieran acceso de usuario raíz.

Configure las funciones de servicio para AWS Clean Rooms

Temas

- Cree un rol de servicio para recibir los resultados

Creación de un usuario administrador

Para AWS Clean Rooms utilizarlos, debe crear un usuario administrador para usted y añadir el usuario administrador a un grupo de administradores.

Para crear un usuario administrador, elija una de las siguientes opciones.

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
En IAM Identity Center (recomendado)	Usar credenciales a corto plazo para acceder a AWS. Esto se ajusta a las prácticas recomendadas de seguridad. Para obtener información sobre las prácticas recomendadas, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.	Siga las instrucciones en Introducción en la Guía del usuario de AWS IAM Identity Center .	Configure el acceso mediante programación configurando el AWS CLI que se utilizará AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario.
En IAM	Usar credenciales a largo plazo para acceder a AWS.	Siga las instrucciones en Creación del primer grupo de usuarios y usuario de	Configurar el acceso programático mediante Administración de las claves

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
(no recomendado)		administrador de IAM en la Guía del usuario de IAM.	de acceso de los usuarios de IAM en la Guía del usuario de IAM.

Creación de un rol de IAM para un miembro de la colaboración

Un miembro es un AWS cliente que participa en una colaboración.

Para crear un rol de IAM para un miembro de la colaboración

1. Siga el procedimiento de creación de un rol para delegar permisos a un usuario de IAM de la Guía del AWS Identity and Access Management usuario.
2. Para el paso Crear política, seleccione la pestaña JSON en el editor de políticas y, a continuación, añada políticas en función de las capacidades otorgadas al miembro de la colaboración.

   AWS Clean Rooms ofrece las siguientes políticas gestionadas basadas en casos de uso comunes:

Si desea…	Entonces use...
Ver los recursos y metadatos	AWS política gestionada: `AWSCleanRoomsReadOnlyAccess`
Consultar	AWS política gestionada: `AWSCleanRoomsFullAccess`
Consultar y recibir resultados	AWS política gestionada: `AWSCleanRoomsFullAccess`

Si desea…	Entonces use...
Administre los recursos de colaboración, pero no realice consultas	AWS política gestionada: `AWSCleanRoomsFullAccessNoQuerying`

Para obtener información sobre las diferentes políticas gestionadas que ofrece AWS Clean Rooms, consulte AWS políticas gestionadas para AWS Clean Rooms

Creación de rol de servicio para leer datos

AWS Clean Rooms utiliza un rol de servicio para leer los datos.

Hay dos formas de crear este rol de servicio:

Si...	Entonces
Dispone de los permisos de IAM necesarios para crear un rol de servicio	Utilice la AWS Clean Rooms consola para crear un rol de servicio.
No tienes `iam:CreateRole` `iam:AttachRolePolicy` permisos `iam:CreatePolicy` ni permisos o Desea crear las funciones de IAM manualmente	Realice una de las siguientes acciones siguientes: • Utilice el siguiente procedimiento para crear un rol de servicio. • Pida al administrador que cree el rol de servicio mediante el siguiente procedimiento.

Para crear un rol de servicio para leer datos

> **Note**
>
> Usted o su administrador de IAM solo deben seguir este procedimiento si no tienen los permisos necesarios para crear un rol de servicio mediante la AWS Clean Rooms consola.

1. Siga el procedimiento de creación de un rol mediante políticas de confianza personalizadas (consola) de la Guía del AWS Identity and Access Management usuario.
2. Utilice la siguiente política de confianza personalizada según el procedimiento de creación de un rol mediante políticas de confianza personalizadas (consola).

> **Note**
>
> Si desea asegurarse de que el rol solo se pueda utilizar en el contexto de una determinada pertenencia a la colaboración, puede delimitar aún más la política de confianza. Para obtener más información, consulte Prevención de la sustitución confusa entre servicios.

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

3. Utilice la siguiente política de permisos según el procedimiento de creación de un rol mediante políticas de confianza personalizadas (consola).

> **Note**
>
> La siguiente política de ejemplo admite los permisos necesarios para leer los metadatos de AWS Glue y los datos de Amazon S3 correspondientes. No obstante, quizás tenga que modificar esta política en función de cómo haya configurado los datos de S3. Por ejemplo, si ha configurado una clave KMS personalizada para sus datos de S3, es posible que deba modificar esta política con AWS KMS permisos adicionales.

Sus AWS Glue recursos y los recursos subyacentes de Amazon S3 deben estar en la Región de AWS misma posición que los de la AWS Clean Rooms colaboración.

```
{
    "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. Sustituya cada *marcador de posición* por su propia información.
5. Siga el procedimiento de creación de un rol mediante políticas de confianza personalizadas (consola) para crear el rol.

Cree un rol de servicio para recibir los resultados

> **Note**
>
> Si usted es el miembro que solo puede recibir resultados (en la consola, las habilidades de su miembro son Solo recibir resultados), siga este procedimiento.

Si es un miembro que puede consultar y recibir resultados (en la consola, las habilidades de su miembro son consultar y recibir resultados), puede omitir este procedimiento.

Para los miembros de la colaboración que solo pueden recibir resultados, AWS Clean Rooms utiliza un rol de servicio para escribir los resultados de los datos consultados en la colaboración en el bucket de Amazon S3 especificado.

Hay dos formas de crear este rol de servicio:

Si...	Entonces
Dispone de los permisos de IAM necesarios para crear un rol de servicio	Utilice la AWS Clean Rooms consola para crear un rol de servicio.
No tienes `iam:CreateRole` `iam:AttachRolePolicy` permisos `iam:CreatePolicy` ni permisos o Desea crear las funciones de IAM manualmente	Realice una de las siguientes acciones siguientes: • Utilice el siguiente procedimiento para crear un rol de servicio. • Pida al administrador que cree el rol de servicio mediante el siguiente procedimiento.

Para crear un rol de servicio para recibir los resultados

> **Note**
>
> Usted o su administrador de IAM solo deben seguir este procedimiento si no tienen los permisos necesarios para crear un rol de servicio mediante la AWS Clean Rooms consola.

1. Siga el procedimiento de creación de un rol mediante políticas de confianza personalizadas (consola) de la Guía del AWS Identity and Access Management usuario.
2. Utilice la siguiente política de confianza personalizada según el procedimiento de creación de un rol mediante políticas de confianza personalizadas (consola).

```
{
    "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. Utilice la siguiente política de permisos según el procedimiento de creación de un rol mediante políticas de confianza personalizadas (consola).

> **Note**
>
> La siguiente política de ejemplo admite los permisos necesarios para leer los metadatos de AWS Glue y los datos de Amazon S3 correspondientes. No obstante, quizás tenga que modificar esta política en función de cómo haya configurado los datos de S3.
> Sus AWS Glue recursos y los recursos subyacentes de Amazon S3 deben estar en la Región de AWS misma posición que los de la AWS Clean Rooms colaboración.

```
{
    "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. Sustituya cada *marcador de posición* por su propia información:

   - *región*: el nombre de la Región de AWS. Por ejemplo, **us-east-1**.
   - *a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa*: el ID de pertenencia del miembro que puede realizar consultas. Puede encontrar el ID de pertenencia en la pestaña Detalles de la colaboración. Esto garantiza AWS Clean Rooms que solo asuma el rol cuando este miembro ejecute el análisis en esta colaboración.
   - *arn:aws:cleanrooms:us-east- 1:555555555555:membership/A1B2C3D4-5678-90AB-cdef-exampleAAAAA: el ARN de membresía* único del miembro que puede realizar la consulta. Puede encontrar el ARN de la pertenencia en la pestaña Detalles de la colaboración. Esto garantiza que solo AWS Clean Rooms asuma el rol cuando este miembro ejecute el análisis en esta colaboración.
   - *nombre_bucket*: el Nombre de recurso de Amazon (ARN) del bucket de S3. Puede encontrar el Nombre de recurso de Amazon (ARN) en la pestaña Propiedades del bucket en Amazon S3.
   - *AccountID*: Cuenta de AWS el ID en el que se encuentra el bucket de S3.

     nombre_bucket/prefijo_clave_opcional: el Nombre de recurso de Amazon (ARN) del destino de los resultados en S3. Puede encontrar el Nombre de recurso de Amazon (ARN) en la pestaña Propiedades del bucket en Amazon S3.

5. Siga el procedimiento de creación de un rol mediante políticas de confianza personalizadas (consola) para crear el rol.

Configure las funciones de servicio para AWS Clean Rooms ML

Temas

- Creación de rol de servicio para leer datos de entrenamiento
- Creación de un rol de servicio para escribir un segmento similar
- Creación de rol de servicio para leer datos iniciales

Creación de rol de servicio para leer datos de entrenamiento

AWS Clean Rooms usa un rol de servicio para leer los datos de entrenamiento. Puede crear este rol mediante la consola si dispone de los permisos de IAM necesarios. Si no tiene `CreateRole` permisos, pida al administrador que cree el rol de servicio.

Para crear un rol de servicio para entrenar un conjunto de datos

1. Inicie sesión en la consola de IAM (https://console.aws.amazon.com/iam/) con su cuenta de administrador.
2. En Access management (Administración de acceso), seleccione Policies (Políticas).
3. Elija Create Policy.
4. En el Editor de políticas, seleccione la pestaña JSON y, a continuación, copie y pegue la siguiente política.

> **Note**
>
> La siguiente política de ejemplo admite los permisos necesarios para leer los metadatos de AWS Glue y los datos de Amazon S3 correspondientes. No obstante, quizás tenga que modificar esta política en función de cómo haya configurado los datos de S3. Esta política no incluye una clave KMS para descifrar los datos.
> Sus AWS Glue recursos y los recursos subyacentes de Amazon S3 deben estar en la Región de AWS misma posición que los de la AWS Clean Rooms colaboración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetPartitions",
                "glue:GetPartition",
                "glue:BatchGetPartition",
                "glue:GetUserDefinedFunctions"
```

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

```
                    "s3:ResourceAccount":[
                        "accountId"
                    ]
                }
            }
        }
    ]
}
```

Si necesita usar una clave KMS para descifrar los datos, añada esta AWS KMS declaración a la plantilla 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. Elija Siguiente.
6. En Revisar y crear, introduzca un Nombre de política y una Descripción y revise el Resumen.
7. Elija Crear política.

   Ha creado una política para AWS Clean Rooms.
8. En Administración de accesos, elija Roles.

   Con Roles, puede crear credenciales a corto plazo, que son las recomendadas aumentar la seguridad. También puede elegir Usuarios para crear credenciales a largo plazo.
9. Elija Crear rol.

10. En el asistente Crear rol, en Tipo de entidad de confianza, elija Política de confianza personalizada.
11. Copie y pegue la siguiente política de confianza personalizada en el 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/*"
                }
            }
        }
    ]
}
```

    Siempre `SourceAccount` es tu AWS cuenta. El `SourceArn` puede limitarse a un conjunto de datos de entrenamiento específico, pero solo después de crear ese conjunto de datos. Puesto que no puede conocer previamente el ARN del conjunto de datos de entrenamiento, el comodín se especifica aquí.

12. Elija Siguiente y, en Agregar permisos, introduzca el nombre de la política que acaba de crear. (es posible que tenga que volver a cargar la página).
13. Seleccione la casilla de verificación situada junto al nombre de la política que creó y, a continuación, elija Siguiente.
14. En Nombre, revisar y crear, introduzca el Nombre del rol y la Descripción.

> **Note**
>
> El Nombre del rol debe coincidir con el patrón de los permisos de `passRole` concedidos al miembro que puede realizar consultas y recibir resultados y a roles de miembros.

a. Revise la sección Seleccionar entidades de confianza y edítela si es necesario.
b. Revise los permisos en Agregar permisos y edítelos si es necesario.
c. Revise las Etiquetas y añada etiquetas si es necesario.
d. Elija Crear rol.

15. Se AWS Clean Rooms ha creado el rol de servicio para.

Creación de un rol de servicio para escribir un segmento similar

AWS Clean Rooms usa un rol de servicio para escribir segmentos similares en un bucket. Puede crear este rol mediante la consola si dispone de los permisos de IAM necesarios. Si no tienes `CreateRole` permisos, pídele a tu administrador que cree el rol de servicio.

Creación de un rol de servicio para escribir un segmento similar

1. Inicie sesión en la consola de IAM (https://console.aws.amazon.com/iam/) con su cuenta de administrador.
2. En Access management (Administración de acceso), seleccione Policies (Políticas).
3. Elija Create Policy.
4. En el Editor de políticas, seleccione la pestaña JSON y, a continuación, copie y pegue la siguiente política.

> **Note**
>
> La siguiente política de ejemplo admite los permisos necesarios para leer los metadatos de AWS Glue y los datos de Amazon S3 correspondientes. No obstante, quizás tenga que modificar esta política en función de cómo haya configurado los datos de S3. Esta política no incluye una clave KMS para descifrar los datos.
> Sus AWS Glue recursos y los recursos subyacentes de Amazon S3 deben estar en la Región de AWS misma posición que los de la AWS Clean Rooms colaboración.

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

Si necesita usar una clave KMS para cifrar datos, añada esta AWS KMS declaración a la plantilla:

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

Si necesita usar una clave KMS para descifrar los datos, añada esta AWS KMS declaración a la plantilla:

```
{
            "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. Elija Siguiente.
6. En Revisar y crear, introduzca un Nombre de política y una Descripción y revise el Resumen.
7. Elija Crear política.

   Ha creado una política para AWS Clean Rooms.
8. En Administración de accesos, elija Roles.

   Con Roles, puede crear credenciales a corto plazo, que son las recomendadas aumentar la seguridad. También puede elegir Usuarios para crear credenciales a largo plazo.
9. Elija Crear rol.
10. En el asistente Crear rol, en Tipo de entidad de confianza, elija Política de confianza personalizada.
11. Copie y pegue la siguiente política de confianza personalizada en el 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/*"
                }
            }
        }
    ]
}
```

   Siempre `SourceAccount` es tu AWS cuenta. El `SourceArn` puede limitarse a un conjunto de datos de entrenamiento específico, pero solo después de crear ese conjunto de datos. Puesto

que no puede conocer previamente el ARN del conjunto de datos de entrenamiento, el comodín se especifica aquí.

12. Elija Siguiente.
13. Seleccione la casilla de verificación situada junto al nombre de la política que creó y, a continuación, elija Siguiente.
14. En Nombre, revisar y crear, introduzca el Nombre del rol y la Descripción.

> **Note**
>
> El Nombre del rol debe coincidir con el patrón de los permisos de `passRole` concedidos al miembro que puede realizar consultas y recibir resultados y a roles de miembros.

    a. Revise la sección Seleccionar entidades de confianza y edítela si es necesario.
    b. Revise los permisos en Agregar permisos y edítelos si es necesario.
    c. Revise las Etiquetas y añada etiquetas si es necesario.
    d. Elija Crear rol.
15. Se AWS Clean Rooms ha creado el rol de servicio para.

Creación de rol de servicio para leer datos iniciales

AWS Clean Rooms utiliza un rol de servicio para leer los datos iniciales. Puede crear este rol mediante la consola si dispone de los permisos de IAM necesarios. Si no tiene `CreateRole` permisos, pida al administrador que cree el rol de servicio.

Para crear un rol de servicio para leer datos iniciales

1. Inicie sesión en la consola de IAM (https://console.aws.amazon.com/iam/) con su cuenta de administrador.
2. En Access management (Administración de acceso), seleccione Policies (Políticas).
3. Elija Create Policy.
4. En el Editor de políticas, seleccione la pestaña JSON y, a continuación, copie y pegue la siguiente política.

> **Note**
>
> La siguiente política de ejemplo admite los permisos necesarios para leer los metadatos de AWS Glue y los datos de Amazon S3 correspondientes. No obstante, quizás tenga que modificar esta política en función de cómo haya configurado los datos de S3. Esta política no incluye una clave KMS para descifrar los datos.
> Sus AWS Glue recursos y los recursos subyacentes de Amazon S3 deben estar en la Región de AWS misma posición que los de la AWS Clean Rooms colaboración.

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

```
                    ]
                }
            }
        }
    ]
}
```

Si necesita usar una clave KMS para descifrar los datos, añada esta AWS KMS declaración a la plantilla:

```
{
            "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. Elija Siguiente.
6. En Revisar y crear, introduzca un Nombre de política y una Descripción y revise el Resumen.
7. Elija Crear política.

   Ha creado una política para AWS Clean Rooms.
8. En Administración de accesos, elija Roles.

   Con Roles, puede crear credenciales a corto plazo, que son las recomendadas aumentar la seguridad. También puede elegir Usuarios para crear credenciales a largo plazo.
9. Elija Crear rol.

10. En el asistente Crear rol, en Tipo de entidad de confianza, elija Política de confianza personalizada.
11. Copie y pegue la siguiente política de confianza personalizada en el 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/*"
                }
            }
        }
    ]
}
```

Siempre `SourceAccount` es tu AWS cuenta. El `SourceArn` puede limitarse a un conjunto de datos de entrenamiento específico, pero solo después de crear ese conjunto de datos. Puesto que no puede conocer previamente el ARN del conjunto de datos de entrenamiento, el comodín se especifica aquí.

12. Elija Siguiente.
13. Seleccione la casilla de verificación situada junto al nombre de la política que creó y, a continuación, elija Siguiente.
14. En Nombre, revisar y crear, introduzca el Nombre del rol y la Descripción.

> **Note**
>
> El Nombre del rol debe coincidir con el patrón de los permisos de `passRole` concedidos al miembro que puede realizar consultas y recibir resultados y a roles de miembros.

a. Revise la sección Seleccionar entidades de confianza y edítela si es necesario.
b. Revise los permisos en Agregar permisos y edítelos si es necesario.
c. Revise las Etiquetas y añada etiquetas si es necesario.
d. Elija Crear rol.

15. Se AWS Clean Rooms ha creado el rol de servicio para.

Crear una colaboración en AWS Clean Rooms

Una colaboración es un límite lógico seguro en AWS Clean Rooms en el que los miembros pueden realizar consultas SQL en tablas configuradas.

Cualquier miembro de AWS Clean Rooms puede crear una colaboración.

El creador de la colaboración puede designar a un único miembro para que realice consultas y reciba resultados. No obstante, es posible que el creador de la colaboración desee impedir que el miembro que puede realizar consultas tenga acceso a los resultados de las consultas. En ese caso, el creador de la colaboración puede designar a un miembro que realice las consultas y a otro miembro que reciba los resultados.

En la mayoría de los casos, el miembro que puede realizar consultas es también el que paga los costos de computación de consultas. No obstante, el creador de la colaboración puede configurar a otro miembro para que se encargue de pagar los costos de computación de consultas.

Para obtener información sobre cómo crear una colaboración con los SDK de AWS, consulte Referencia de API de AWS Clean Rooms.

Temas

Creación de una colaboración

Antes de comenzar, asegúrese de que cumple los siguientes requisitos previos:

- Dispone del nombre y el ID de Cuenta de AWS de cada miembro al que desea invitar a la colaboración.
- Tiene permiso para compartir el nombre y el ID de Cuenta de AWS de cada miembro con todos los miembros de la colaboración.

> **Note**
>
> No puede añadir más miembros una vez creada la colaboración.

Para crear una colaboración mediante la consola de AWS Clean Rooms.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con la Cuenta de AWS que actúe como creador de la colaboración.
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. En la esquina superior derecha, elija Crear colaboración.
4. En Paso 1: Definir la colaboración, haga lo siguiente:

    a. En Detalles, introduzca el Nombre y la Descripción de la colaboración.

    Esta información estará visible para los miembros de la colaboración que estén invitados a participar en la colaboración. La información de Nombre y Descripción les ayudará a entender a qué se refiere la colaboración.

    b. En Miembros:

        i. En Miembro 1: usted, introduzca su Nombre de miembro para mostrar tal y como desee que aparezca en la colaboración.

        > **Note**
        >
        > Su ID de Cuenta de AWS se incluye automáticamente en ID de Cuenta de AWS del miembro.

        ii. En Miembro 2, introduzca el Nombre del miembro para mostrar y el ID de Cuenta de AWS del miembro correspondientes al miembro a quien desea invitar a la colaboración.

        El Nombre del miembro para mostrar y el ID de Cuenta de AWS del miembro estarán visibles para todos los invitados a participar en la colaboración. Una vez introducidos y guardados, los valores de estos campos no se podrán editar.

        > **Note**
        >
        > Debe informar al miembro de la colaboración de que la información de los campos ID de Cuenta de AWS del miembro y Nombre del miembro para mostrar estará visible para todos los colaboradores activos de la colaboración.

iii. Si desea añadir otro miembro, elija Añadir otro miembro. A continuación, rellene los campos Nombre del miembro para mostrar e ID de Cuenta de AWS del miembro para cada miembro que pueda contribuir con datos y a quien desee invitar a la colaboración.

c. En Capacidades como miembro, elija una de las siguientes opciones:

Si desea…	Entonces...
Consultar los datos de la colaboración y recibir los resultados	1. Elíjase a usted mismo como miembro que puede Ejecutar las consultas. 2. Deje la configuración predeterm inada del miembro que puede Recibir los resultados como El mismo que ejecuta las consultas.
Consultar los datos de la colaboración y designar a un miembro distinto para recibir los resultados	1. Elíjase a usted mismo como miembro que puede Ejecutar las consultas. 2. Seleccione el miembro que puede Recibir los resultados en la lista desplegable.
Recibir los resultados de la consulta en la colaboración y designar a un miembro distinto para consultar los datos	1. Seleccione el miembro que puede Ejecutar las consultas en la lista desplegable. 2. Elíjase a usted mismo como miembro que puede Recibir los resultados en la lista desplegable.
Crear y administrar la colaborac ión, designar a un miembro distinto para consultar los datos y designar a un miembro distinto para recibir los resultados	1. Seleccione el miembro que puede Ejecutar las consultas en la lista desplegable. 2. Seleccione el miembro que puede Recibir los resultados en la lista desplegable.

d. En Configuración de pago, elija una de las opciones siguientes:

Si desea…	Entonces...
Designar al miembro que puede Ejecutar las consultas como miembro que paga los costos de computación de las consultas	Deje la configuración predeterm inada del miembro que va a Pagar las consultas como El mismo que ejecuta las consultas.
Designar a otro miembro que pague los costos de computación de las consultas	Seleccione el miembro que va a Pagar las consultas en la lista desplegable.

e. Si desea habilitar el Registro de consultas, seleccione la casilla de verificación Permitir el registro de consultas en esta colaboración.

f. Si desea habilitar la capacidad de computación criptográfica, seleccione la casilla de verificación Permitir computación criptográfica en esta colaboración y elija los siguientes parámetros de computación criptográfica:

- Permitir columnas cleartext

  Elija No si no desea permitir las columnas cleartext en la tabla cifrada.

  Elija Sí si desea permitir las columnas cleartext en la tabla cifrada.

  Para ejecutar SUM o AVG en columnas específicas, las columnas deben estar en cleartext.

- Permitir duplicados

  Elija No si no desea permitir las entradas duplicadas en una columna fingerprint.

  Elija Sí si desea permitir las entradas duplicadas en una columna fingerprint.

- Permitir JOIN de columnas con nombres diferentes

  Seleccione No si no desea combinar las columnas fingerprint con nombres diferentes.

  Elija Sí si desea combinar las columnas fingerprint con nombres diferentes.

- Conservar valores NULL

Elija No si no desea conservar los valores NULL. Los valores NULL no aparecerán como NULL en una tabla cifrada.

Elija Sí si desea conservar los valores NULL. Los valores NULL aparecerán como NULL en una tabla cifrada.

Para obtener más información acerca de los parámetros de computación criptográfica, consulte Parámetros de computación criptográfica.

Para obtener más información sobre cómo cifrar los datos para su uso en AWS Clean Rooms, consulte Preparar tablas de datos cifrados con computación criptográfica para Clean Rooms.

> **Note**
>
> Compruebe estas configuraciones detenidamente antes de completar el siguiente paso. Una vez que haya creado la colaboración, solo podrá editar el nombre y la descripción de la colaboración, y si los registros de consultas se almacenan en Registros de Amazon CloudWatch.

g. Si desea habilitar la opción de Etiquetas para el recurso de colaboración, seleccione Añadir nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.

h. Elija Siguiente.

5. En Paso 2: Configurar pertenencia, haga lo siguiente:

a. Seleccione una opción:

Si selecciona...	Entonces...
Sí, unirme y crear pertenencia ahora	Se crean tanto la colaboración como su pertenencia a ella. Su estado en la colaboración es activo.
No, crearé una pertenencia más tarde	Se crea solo la colaboración. Su estado en la colaboración es inactivo.

b. Si usted es el miembro que puede Recibir los resultados, en la sección Configuración predeterminada de los resultados de consulta, elija una opción:

Si...	Entonces...
Mantiene seleccionada la casilla de verificación Establecer configuración predeterminada ahora (está seleccionada de manera predeterminada)	1. En Destino de los resultados en Amazon S3, introduzca el destino de Amazon S3. 2. Como Formato de los resultados de la consulta, elija CSV o PARQUET.
Desactiva la casilla de verificación Establecer configuración predeterminada ahora	Se crea solo la colaboración. Su estado en la colaboración es inactivo.

c. Si opta por habilitar el Registro de consultas en el paso 4.e, elija una de las opciones siguientes para Almacenamiento de registros en Registros de Amazon CloudWatch:

Si selecciona...	Entonces...
Activar	Los registros de consultas relevantes para usted se almacenan en Registros de Amazon CloudWatch. Cada miembro solo puede recibir los registros de las consultas que haya iniciado o que contengan sus datos. El miembro que puede recibir los resultado s también recibe los registros de todas las consultas que se ejecutan en una colaboración, incluso si no se accede a sus datos en la consulta.
Desactivar	Los registros de consultas relevantes para usted no se almacenan en su cuenta de Registros de Amazon CloudWatch.

> **Note**
>
> Tras activar el Registro de consultas, el almacenamiento de registros puede tardar unos minutos en configurarse y empezar a recibir registros en Registros de Amazon CloudWatch. Durante este breve período, el miembro que puede realizar consultas puede ejecutar consultas que, en realidad, no enviarán registros.

d. Si desea habilitar la opción de Etiquetas para el recurso de pertenencia, seleccione Añadir nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.

e. Si usted es el miembro designado para Pagar las consultas, indique su aceptación marcando la casilla de verificación Acepto pagar los costos de computación de las consultas de esta colaboración.

> **Note**
>
> Debe seleccionar esta casilla de verificación para continuar.
> Para obtener más información sobre cómo se calculan los precios, consulte Precios para AWS Clean Rooms.

Si usted es el miembro que paga los costes de cómputo de consultas, pero no el miembro que puede realizar consultas, es recomendable que use AWS Budgets para configurar un presupuesto de AWS Clean Rooms y para recibir notificaciones una vez que se alcance el presupuesto máximo. Para obtener más información sobre cómo configurar un presupuesto, consulte Administración de costos con AWS Budgets en la Guía del usuario de AWS Cost Management. Para obtener más información sobre cómo configurar notificaciones, consulte Creación de un tema de Amazon SNS para las notificaciones de presupuesto en la Guía del usuario de AWS Cost Management. Si se ha alcanzado el presupuesto máximo, puede ponerse en contacto con el miembro que puede realizar consultas o abandonar la colaboración. Si abandona la colaboración, no se podrán ejecutar más consultas y, por lo tanto, ya no se le facturarán costos de cómputo de consultas.

f. Elija Siguiente.

6. En Revisar y crear, realice una de las siguientes acciones:

a. Revise las selecciones que realizó en los pasos anteriores y edítelas si es necesario.

b. Elija una de las siguientes opciones:

Si ha optado por...	Entonces elija...
Crear una pertenencia en la colaboración (Sí, unirme y crear pertenencia ahora)	Crear colaboración y pertenencia
Crear la colaboración y no crear una pertenencia en este momento (No, crearé una pertenencia más tarde)	Crear colaboración

Una vez que la colaboración se haya creado correctamente, podrá ver la página de detalles de la colaboración en Colaboraciones.

Pasos siguientes

Ya puede hacer lo siguiente:

- Preparar su tabla de datos para que se consulte en AWS Clean Rooms (opcional si desea consultar sus propios datos).
- Asociar la tabla configurada a su colaboración (opcional si desea consultar sus propios datos).
- Configurar una regla de análisis para la tabla configurada (opcional si desea consultar sus propios datos).
- Crear una pertenencia y unirse a una colaboración.
- Administrar la colaboración.

Crear una pertenencia y unirse a una colaboración

Una pertenencia es un recurso que se crea cuando un miembro se une a una colaboración en AWS Clean Rooms.

Puede unirse a una colaboración como miembro que puede realizar consultas de datos, como miembro que puede recibir resultados de una consulta, o ambos. También puede unirse a una colaboración como miembro que paga los costos de computación de las consultas. Todos los miembros pueden contribuir con datos.

Para obtener información sobre cómo crear una pertenencia y unirse a una colaboración utilizando los SDK de AWS , consulte la Referencia de la API de AWS Clean Rooms.

Temas

Creación de una pertenencia y unión a una colaboración

Para crear una pertenencia y unirse a una colaboración

1. Inicia sesión en la AWS Clean Rooms consola AWS Management Console y ábrela con tu miembro Cuenta de AWS.
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. En la pestaña Disponibles para combinar, en Colaboraciones disponibles para combinar, elija el Nombre de la colaboración.
4. En la página de detalles de la colaboración, consulte los detalles de la colaboración, incluidos sus detalles de miembro y una lista de los demás miembros.

   Compruebe que los Cuenta de AWS ID de cada miembro de la colaboración son aquellos con los que piensa iniciar la colaboración.
5. Elija Crear pertenencia.
6. En la página de creación de miembros, en la sección Descripción general, consulte el nombre de la colaboración, la descripción de la colaboración, el Cuenta de AWS ID del creador de la colaboración, las capacidades de sus miembros y el Cuenta de AWS ID del miembro que pagará las consultas.

7. Si el creador de la colaboración ha decidido habilitar el registro de consultas, elija una de las siguientes opciones para el almacenamiento de CloudWatch registros en Amazon Logs:

Si selecciona...	Entonces...
Activar	Los registros de consultas relevantes para usted se almacenan en Amazon CloudWatch Logs. Cada miembro solo puede recibir los registros de las consultas que haya iniciado o que contengan sus datos. El miembro que puede recibir los resultado s también recibe los registros de todas las consultas que se realicen en una colaborac ión, incluso si no se accede a sus datos en una consulta.
Desactivar	Los registros de consultas relevantes para ti no se almacenan en tu cuenta de Amazon CloudWatch Logs.

> **Note**
>
> Tras activar el registro de consultas, el almacenamiento de registros puede tardar unos minutos en configurarse y empezar a recibir registros en Amazon CloudWatch Logs. Durante este breve período, el miembro que puede realizar consultas puede ejecutar consultas que, en realidad, no enviarán registros.

8. Si Sus capacidades como miembro incluyen Recibir resultados:

   a. En Configuración de los resultados de consulta,

      i. Especifique el Destino de los resultados en Amazon S3 introduciendo el destino de S3, o elija Examinar S3 para seleccionarlo de una lista de buckets de S3 disponibles.

Example

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

ii. Elija el Formato de resultados (CSV o PARQUET).

b. En Acceso al servicio, seleccione Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

> **Note**
>
> Debe seleccionar un rol de servicio existente o tener permisos para crear uno nuevo. Para obtener más información, consulte Cree un rol de servicio para recibir los resultados.

9. Si desea habilitar la opción de Etiquetas para el recurso de pertenencia, seleccione Añadir nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.
10. Si el creador de la colaboración le ha designado responsable de Pagar las consultas, indique su aceptación marcando la casilla de verificación Acepto pagar los costes de cómputo de las consultas de esta colaboración.

> **Note**
>
> Debe seleccionar esta casilla de verificación para continuar.
> Para obtener más información sobre cómo se calculan los precios, consulte Precios para AWS Clean Rooms.

Si es el miembro que paga los costes de cálculo de la consulta, pero no el miembro que puede realizar la consulta AWS Budgets , se recomienda configurar un presupuesto AWS Clean Rooms y recibir notificaciones cuando se alcance el presupuesto máximo. Para obtener más información sobre cómo configurar un presupuesto, consulte Administración de costos con AWS Budgets en la Guía del usuario de AWS Cost Management . Para obtener más información sobre cómo configurar notificaciones, consulte Creación de un tema de Amazon SNS para las notificaciones de presupuesto en la Guía del usuario de AWS Cost Management . Si se ha alcanzado el presupuesto máximo, puede ponerse en contacto con el miembro que puede realizar consultas o abandonar la colaboración. Si abandona la colaboración, no se podrán ejecutar más consultas y, por lo tanto, ya no se le facturarán costos de cómputo de consultas.

11. Si tiene la certeza de que desea crear una pertenencia y unirse a la colaboración, consulte Crear pertenencia.

Se le concede acceso de lectura a los metadatos de la colaboración. Esto incluye información como el nombre para mostrar y la descripción de la colaboración, además de todos los nombres e ID de Cuenta de AWS de otros miembros.

Para obtener información sobre cómo abandonar una colaboración, consulte Abandonar una colaboración.

Siguientes pasos

Ya puede hacer lo siguiente:

- Prepare la tabla de datos para consultarla. AWS Clean Rooms(opcional si desea consultar sus propios datos).
- Asociar la tabla configurada a su colaboración
- Configurar una regla de análisis para la tabla configurada.

Preparación de tablas de datos para consultas en AWS Clean Rooms

> **Note**
>
> Puede preparar las tablas de datos antes o después de unirse a una colaboración. Una vez preparada una tabla, puedes reutilizarla en varias colaboraciones siempre que tus necesidades de privacidad para esa tabla sean las mismas.

Como miembro de la colaboración, debe preparar las tablas de datos antes de que el miembro de la colaboración que pueda consultarlas pueda consultarlas. AWS Clean Rooms

Si su caso de uso no requiere que traiga sus propios datos, puede omitir este procedimiento.

Si las tablas de datos ya están catalogadas AWS Glue, vaya aCrear una tabla configurada en AWS Clean Rooms.

La preparación de las tablas de datos consta de los siguientes pasos:

- Paso 1: completar los requisitos previos
- Paso 2: (opcional) preparar sus datos para la computación criptográfica
- Paso 3: cargar la tabla de datos en Amazon S3
- Paso 4: Crear una AWS Glue tabla
- Siguientes pasos

Para obtener más información sobre los formatos de datos que puede usar para las consultas, consulte Formatos de datos para AWS Clean Rooms.

Paso 1: completar los requisitos previos

Para preparar las tablas de datos para usarlas con AWS Clean Rooms ellas, debe cumplir los siguientes requisitos previos:

- Los conjuntos de datos deben guardarse en uno de los formatos de datos admitidos para AWS Clean Rooms.

- Las tablas de datos deben estar catalogadas AWS Glue y utilizar los tipos de datos compatibles. AWS Clean Rooms
- Todas las tablas de datos deben almacenarse en Amazon Simple Storage Service (Amazon S3), en el Región de AWS mismo lugar en el que se creó la colaboración.
- AWS Glue Data Catalog Debe estar en la misma región en la que se creó la colaboración.
- AWS Glue Data Catalog Debe estar en la misma posición Cuenta de AWS que la membresía.
- No se puede registrar el bucket de Amazon S3 AWS Lake Formation.
- El creador de la colaboración ha configurado una colaboración en AWS Clean Rooms. Para obtener más información, consulte Crear una colaboración en AWS Clean Rooms.
- El creador de la colaboración le ha enviado el ID de la colaboración como participante en la colaboración.

Paso 2: (opcional) preparar sus datos para la computación criptográfica

(Opcional) Si utiliza la computación criptográfica y su tabla de datos contiene información confidencial que desea cifrar, debe cifrar la tabla de datos mediante el cliente de cifrado de C3R.

Para preparar los datos para la computación criptográfica, siga los procedimientos descritos en Preparar tablas de datos cifrados con computación criptográfica para Clean Rooms.

Paso 3: cargar la tabla de datos en Amazon S3

> **Note**
>
> Si piensa utilizar tablas de datos cifrados en la colaboración, primero debe cifrar los datos para la computación criptográfica antes de cargar la tabla de datos en Amazon S3. Para obtener más información, consulte Preparar tablas de datos cifrados con computación criptográfica para Clean Rooms.

Para cargar la tabla de datos en Amazon S3

1. Inicie sesión en la consola de Amazon S3 AWS Management Console y ábrala en https://console.aws.amazon.com/s3/.

2. Elija Buckets y, a continuación, elija un bucket donde desee almacenar la tabla de datos.
3. Elija Cargar y siga las indicaciones de la pantalla.
4. Seleccione la pestaña Objetos para ver el prefijo donde se almacenan sus datos. Anote el nombre de la carpeta.

   Puede seleccionar la carpeta para ver los datos.

Paso 4: Crear una AWS Glue tabla

Si ya tiene una tabla AWS Glue de datos, puede omitir este paso.

En este paso, configuras un rastreador AWS Glue que rastrea todos los archivos del bucket de S3 y crea una AWS Glue tabla. Para obtener más información, consulte Definición de rastreadores AWS Glue en la Guía del AWS Glue usuario.

Para obtener más información sobre AWS Glue Data Catalog los tipos de datos compatibles, consulteTipos de datos compatibles.

> **Note**
>
> AWS Clean Rooms actualmente no admite los buckets S3 registrados en. AWS Lake Formation

El siguiente procedimiento describe cómo crear una AWS Glue tabla. Si desea utilizar un AWS Glue Data Catalog objeto cifrado con una clave AWS Key Management Service (AWS KMS), debe configurar la política de permisos de claves de KMS para permitir el acceso a esa tabla cifrada. Para obtener más información, consulte Configuración del cifrado en AWS Glue, en la Guía del desarrollador de AWS Glue .

Para crear una AWS Glue tabla

1. Siga el procedimiento de trabajo con rastreadores en la AWS Glue consola de la Guía del AWS Glue usuario.
2. Anote el nombre de la AWS Glue base de datos y el nombre de AWS Glue la tabla.

Siguientes pasos

Ahora que ha preparado las tablas de datos, está preparado para:

- Crear una tabla configurada
- Cree un modelo de aprendizaje automático

Formatos de datos para AWS Clean Rooms

Los conjuntos de datos que se utilizan para las consultas AWS Clean Rooms suelen ser los mismos tipos de conjuntos de datos que se utilizan para otras aplicaciones. Por ejemplo, los mismos tipos de conjuntos de datos se utilizan con Amazon Athena, Amazon EMR, Amazon Redshift Spectrum y Amazon. QuickSight Puede consultar los datos en su formato original directamente desde Amazon Simple Storage Service (Amazon S3).

Para consultar datos, los conjuntos de datos deben estar en un formato compatible. AWS Clean Rooms El bucket de Amazon S3 con los conjuntos de datos y el AWS Clean Rooms clúster deben estar en el mismo Región de AWS lugar.

Formatos de datos admitidos

AWS Clean Rooms admite los siguientes formatos estructurados:

- Tablas de Apache Iceberg
- Parquet
- RCFile
- TextFile
- SequenceFile
- RegexSerde
- OpenCSV
- AVRO
- JSON

> **Note**
>
> Un valor `timestamp` de un archivo de texto debe estar en formato `yyyy-MM-dd HH:mm:ss.SSSSSS`. Por ejemplo: `2017-05-01 11:30:59.000000`.

Recomendamos utilizar un formato de archivo de almacenamiento en columnas, como Apache Parquet. Un formato de archivo de almacenamiento en columnas le permite minimizar la transferencia de datos desde Amazon S3 seleccionando únicamente las columnas que necesite. Para obtener un rendimiento óptimo, los objetos grandes deben dividirse en objetos de 100 MB a 1 GB.

Tipos de datos compatibles

Para una experiencia óptima AWS Clean Rooms, todos sus datos deben estar catalogados en AWS Glue. Para obtener más información, consulte la sección titulada Introducción a AWS Glue Data Catalog en la Guía del desarrollador de AWS Glue .

AWS Clean Rooms admite los siguientes tipos AWS Glue Data Catalog de datos:

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

- varchar

AWS Clean Rooms no admite:

- binario
- intervalo

Tipos de compresión de archivos para AWS Clean Rooms

Para reducir el espacio de almacenamiento, mejorar el rendimiento y minimizar costos, es muy recomendable comprimir los archivos de datos.

AWS Clean Rooms reconoce los tipos de compresión de archivos en función de la extensión del archivo y admite los tipos y extensiones de compresión que se muestran en la tabla siguiente.

Algoritmo de compresión	Extensión de archivo
GZIP	.gz
Bzip2	.bz2
Snappy	.snappy

Puede aplicar compresión a distintos niveles. En la mayoría de los casos, se comprime un archivo completo o se comprimen bloques individuales dentro de un archivo. La compresión de formatos de columna por archivo no ofrece beneficios en términos de rendimiento.

Cifrado del lado del servidor para AWS Clean Rooms

> **Note**
>
> El cifrado en el servidor no reemplaza a la computación criptográfica en los casos de uso en los que esta última es obligatoria.

AWS Clean Rooms descifra de forma transparente los conjuntos de datos cifrados mediante las siguientes opciones de cifrado:

- SSE-S3: cifrado en el servidor mediante una clave de cifrado AES-256 administrada por Amazon S3
- SSE-KMS: cifrado del lado del servidor con claves administradas por AWS Key Management Service

Para usar SSE-S3, el rol de AWS Clean Rooms servicio utilizado para asociar la tabla configurada a la colaboración debe tener permisos de descifrado por KMS. Para usar SSE-KMS, la política de claves de KMS también debe permitir que la función de servicio descifre. AWS Clean Rooms

AWS Clean Rooms no admite el cifrado del lado del cliente de Amazon S3. Para obtener más información sobre el cifrado en el servidor, consulte Protección de datos con el cifrado del lado del servidor en la Guía del usuario de Amazon Simple Storage Service.

Uso de Apache Iceberg tablas en AWS Clean Rooms

Apache Icebergs un formato de tabla de código abierto para lagos de datos. AWS Clean Rooms puede utilizar las estadísticas almacenadas en Apache Iceberg los metadatos para optimizar los planes de consultas y reducir las digitalizaciones de archivos durante el procesamiento de consultas en salas limpias. Para obtener más información, consulte la documentación de Apache Iceberg.

Tenga en cuenta lo siguiente al utilizarlas AWS Clean Rooms con tablas Iceberg:

- AWS Glue Data Catalog Solo las tablas están dentro de Apache Iceberg las tablas: las tablas deben definirse en AWS Glue Data Catalog función de la implementación del catálogo Glue de código abierto.
- Formato de archivo Parquet: AWS Clean Rooms solo admite tablas Iceberg en el formato de archivo de datos Parquet.
- Compresión GZIP y Snappy: AWS Clean Rooms admite Parquet con GZIP y compresión. Snappy
- Versiones Iceberg: AWS Clean Rooms permite ejecutar consultas en tablas Iceberg de las versiones 1 y 2.
- Particiones: no es necesario añadir manualmente particiones para Apache Iceberg las tablas. AWS Glue AWS Clean Rooms detecta automáticamente Apache Iceberg las nuevas particiones en las tablas y no es necesaria ninguna operación manual para actualizar las particiones en la definición de la tabla. Las particiones de Iceberg aparecen como columnas normales en el esquema de tabla de AWS Clean Rooms , y no por separado como una clave de partición en el esquema de la tabla configurada.

- Limitaciones
  - Solo tablas de Iceberg nuevas

    No se admiten las tablas de Apache Iceberg convertidas a partir de tablas de Apache Parquet.
  - Consultas de viaje en el tiempo

    AWS Clean Rooms no admite consultas sobre viajes en el tiempo con Apache Iceberg tablas.
  - Versión 2 del motor Athena

    No se admiten las tablas de Iceberg creadas con la versión 2 del motor Athena.
  - Formatos de archivo

    No se admiten los formatos archivo Avro ni ORC (Optimized Row Columnar).
  - Compresión

    No se admite la compresión Zstandard (Zstd) para Parquet.

Tipos de datos admitidos para las tablas de Iceberg

AWS Clean Rooms puede consultar Iceberg tablas que contengan los siguientes tipos de datos:

- boolean
- date
- decimal
- double
- float
- int
- list
- long
- map
- string
- struct
- timestamp without time zone

Para obtener más información sobre los tipos de datos de Iceberg, consulte los esquemas para Iceberg en la documentación de Apache.

Preparar tablas de datos cifrados con computación criptográfica para Clean Rooms

La computación criptográfica para Clean Rooms (C3R) es una capacidad de. AWS Clean Rooms Puede utilizar el C3R para limitar criptográficamente lo que puede aprender cualquiera de las partes y en una colaboración. AWS AWS Clean Rooms

Puede cifrar la tabla de datos con el cliente de cifrado de C3R, una herramienta de cifrado del cliente, antes de cargar la tabla de datos en Amazon Simple Storage Service (Amazon S3).

Para obtener más información, consulte Computación criptográfica para Clean Rooms.

Para preparar tablas de datos cifrados con C3R, se deben seguir estos pasos:

Pasos

- Paso 1: completar los requisitos previos
- Paso 2: descargar el cliente de cifrado de C3R
- (Opcional) Paso 3: ver los comandos disponibles en el cliente de cifrado de C3R
- Paso 4: generar un esquema de cifrado para un archivo tabular
- Paso 5: crear una clave secreta compartida
- Paso 6: guardar la clave secreta compartida en la variable de entorno
- Paso 3: cifrar los datos
- Paso 8: verificar el cifrado de datos
- (Opcional) Crear un esquema (usuarios avanzados)

Paso 1: completar los requisitos previos

Para preparar las tablas de datos para su uso con C3R, debe cumplir con los siguientes requisitos previos:

- Puede acceder al repositorio de Cryptographic Computing for en: Clean Rooms GitHub

  https://github.com/aws/c3r
- Ha configurado AWS las credenciales para utilizar el cliente de cifrado C3R. El cliente de cifrado C3R utiliza estas credenciales para las llamadas a la API de solo lectura con el fin de recuperar

los metadatos de la colaboración. AWS Clean Rooms Para obtener más información, consulte Configurar la AWS CLI en la Guía del usuario de la versión 2 de AWS Command Line Interface .

- Tiene Java Runtime Environment (JRE) 11 o una versión posterior instalada en su equipo.
  - Puede descargar la versión recomendada de Java Runtime Environment, Amazon Corretto 11 o superior, desde https://aws.amazon.com/corretto.
  - El Java Development Kit (JDK) incluye una versión correspondiente de JRE de la misma versión. Sin embargo, las capacidades adicionales del JDK no son necesarias para ejecutar la computación criptográfica para el cliente de cifrado de Clean Rooms (C3R).
- Sus archivos de datos tabulares (.csv) o archivos Parquet (.parquet) se guardan localmente.
- Usted u otro miembro de la colaboración tienen la capacidad de crear una clave secreta compartida. Para obtener más información, consulte Paso 5: crear una clave secreta compartida.
- El creador de la colaboración ha creado una colaboración AWS Clean Rooms con la computación criptográfica habilitada para la colaboración. Para obtener más información, consulte Crear una colaboración en AWS Clean Rooms.
- El creador de la colaboración le ha enviado el ID de la colaboración como participante en la colaboración. El nombre de recurso de Amazon (ARN) de la colaboración se incluye en la invitación enviada, que contiene el ID de la colaboración.

Paso 2: descargar el cliente de cifrado de C3R

Para descargar el cliente de cifrado C3R desde GitHub

1. Diríjase al repositorio de Cryptographic Computing for Clean RoomsAWSGitHub: https://github.com/aws/c3r
2. Seleccione y descargue los archivos.

   El código fuente, las licencias y el material relacionado se pueden clonar o descargar como archivo .zip desde la página de inicio del repositorio de GitHub (vea el botón Código en la parte superior derecha de la lista de contenido del repositorio).

   El último cliente de cifrado de C3R con firma Java Executable File (es decir, la aplicación de interfaz de la línea de comandos) se encuentra en la página Versiones del repositorio de GitHub.

   El paquete del cliente de cifrado de C3R para Apache Spark (`c3r-cli-spark`) es una versión del c3r-cli que debe enviarse como trabajo a un servidor Apache Spark en ejecución. Para obtener más información, consulte Ejecutar C3R en Apache Spark.

(Opcional) Paso 3: ver los comandos disponibles en el cliente de cifrado de C3R

Utilice este procedimiento para familiarizarse con los comandos disponibles en el cliente de cifrado de C3R.

Para ver los comandos disponibles en el cliente de cifrado de C3R.

1. Desde una interfaz de la línea de comandos (CLI), vaya a la carpeta que contiene el archivo c3r-cli.jar descargado.
2. Ejecute el comando siguiente: `java -jar c3r-cli.jar`
3. Vea la lista de comandos y opciones disponibles.

Paso 4: generar un esquema de cifrado para un archivo tabular

Para cifrar datos, se requiere un esquema de cifrado que describa cómo se utilizarán los datos. En esta sección se describe cómo el cliente de cifrado de C3R ayuda a generar un esquema de cifrado para un archivo CSV con una fila de encabezado o un archivo Parquet.

Solo tiene que hacerlo una vez por archivo. Una vez creado el esquema, se puede volver a utilizar para cifrar el mismo archivo (o cualquier archivo con nombres de columna idénticos). Si los nombres de las columnas o el esquema de cifrado deseado cambian, debe actualizar el archivo de esquema. Para obtener más información, consulte (Opcional) Crear un esquema (usuarios avanzados).

> **Important**
>
> Es imprescindible que todas las partes colaboradoras utilicen la misma clave secreta compartida. Las partes colaboradoras también deben coordinar los nombres de las columnas para que coincidan si se va a ejecutar en ellas una operación JOIN o si se van a comparar de cualquier otro modo para garantizar la igualdad en las consultas. De lo contrario, las consultas SQL podrían producir resultados inesperados o incorrectos. No obstante, esto no será necesario si el creador de la colaboración habilitó la configuración de cifrado `allowJoinsOnColumnsWithDifferentNames` al crear la colaboración. Para obtener más información acerca de los ajustes relevantes para el cifrado, consulte Parámetros de computación criptográfica.

Cuando se ejecuta en modo de esquema, el cliente de cifrado de C3R revisa el archivo de entrada columna por columna y le pregunta si debe tratarse esa columna y de qué manera. Si el archivo contiene un gran número de columnas que no son necesarias para la salida cifrada, la generación del esquema interactivo podría resultar tediosa, ya que habría que saltarse todas las columnas no deseadas. Para evitarlo, puede escribir un esquema manualmente o crear una versión simplificada del archivo de entrada que incluya solo las columnas deseadas. Entonces, el generador de esquemas interactivo podrá ejecutarse en ese archivo reducido. El cliente de cifrado de C3R genera información sobre el archivo de esquema y le pregunta cómo se deben incluir o cifrar las columnas de origen (si es que se deben incluir) en el resultado de destino.

Para cada columna de origen del archivo de entrada, se le preguntará lo siguiente:

1. Cuántas columnas de destino se deben generar
2. Cómo se debe cifrar cada columna de destino (si procede)
3. El nombre de cada columna de destino
4. Cómo deben rellenarse los datos antes del cifrado si la columna se cifra como columna sealed

> **Note**
>
> Al cifrar datos de una columna que se ha cifrado como columna sealed, debe determinar qué datos precisan relleno. El cliente de cifrado de C3R sugiere un relleno predeterminado durante la generación del esquema, consistente en rellenar todas las entradas de una columna hasta que alcancen la misma longitud.
> Al determinar la longitud `fixed`, tenga en cuenta que el relleno está en bytes, no en bits.

A continuación se proporciona una tabla de decisión para crear el esquema.

Tabla de decisión del esquema

Decisión	¿Número de columnas de destino de la columna de origen <' '>? name-of-column	Tipo de columna de destino: [c] cleartext, [f] fingerprint o [s] sealed?	Nombre del encabezado de la columna de destino <default 'name-of-column'>	Añadir un sufijo <sufijo> al encabezado para indicar cómo se cifró, [y] sí o [n] no <predeterminado 'yes'>	<' name-of-column _sealed'> tipo de relleno: [n] uno, [f] fijo o [m] máximo <default 'max'>
Deje la columna sin cifrar.	1	c	No aplicable	No aplicable	No aplicable
Cifre la columna como columna fingerprint.	1	f	Elija el nombre predeterminado o introduzca un nombre de encabezado nuevo.	Introduzca y para elegir el valor predeterminado (`_fingerprint`) o introduzcan.	No aplicable
Cifre la columna como columna sealed.	1	s	Elija el nombre predeterminado o introduzca un nombre de encabezado nuevo.	Introduzca y para elegir el valor predeterminado (`_sealed`) o introduzcan.	Elija el tipo de relleno. Para obtener más información, consulte (Opcional) Crear un esquema (usuarios avanzados).

Decisión	¿Número de columnas de destino de la columna de origen <' '>? name-of-column	Tipo de columna de destino: [c] cleartext, [f] fingerprint o [s] sealed?	Nombre del encabezado de la columna de destino <default 'name-of-column'>	Añadir un sufijo <sufijo> al encabezado para indicar cómo se cifró, [y] sí o [n] no <predeterminado 'yes'>	<' name-of-column _sealed'> tipo de relleno: [n] uno, [f] fijo o [m] máximo <default 'max'>
Cifre la columna como fingerprint y sealed.	2	Introduzca la primera columna de destino: f. Introduzca la segunda columna de destino: s.	Elija los encabezados de destino para cada columna de destino.	Introduzca y para elegir el valor predeterminado o introduzca n. .	Elija el tipo de relleno (solo para columnas sealed). Para obtener más información, consulte (Opcional) Crear un esquema (usuarios avanzados).

A continuación se muestran dos ejemplos de cómo crear esquemas de cifrado. El contenido exacto de la interacción depende del archivo de entrada y de las respuestas que proporcione.

Ejemplos

- Ejemplo: Generar un esquema de cifrado para una columna fingerprint y una columna cleartext
- Ejemplo: Generar un esquema de cifrado con columnas sealed, fingerprint y columnas

Ejemplo: Generar un esquema de cifrado para una columna fingerprint y una columna cleartext

En este ejemplo, para `ads.csv`, solo hay dos columnas: `username` y `ad_variant`. Para estas columnas, queremos lo siguiente:

- Que la columna `username` se cifre como columna `fingerprint`
- Que la columna `ad_variant` sea una columna `cleartext`

Para generar un esquema de cifrado para una columna fingerprint y una columna cleartext

1. (Opcional) Para garantizar que el archivo c3r-cli.jar y el archivo que se va a cifrar estén presentes:

   a. Desplácese al directorio deseado y ejecute `ls` (si utiliza Mac o Unix/Linux) o `dir` si utiliza Windows).

   b. Vea la lista de archivos de datos tabulares (por ejemplo, .csv) y elija el archivo que desea cifrar.

   En este ejemplo, `ads.csv` es el archivo que queremos cifrar.

2. Desde la CLI, ejecute el siguiente comando para crear un esquema de forma interactiva.

```
java -jar c3r-cli.jar schema ads.csv --interactive --output=ads.json
```

> **Note**
>
> - Puede ejecutar `java --jar PATH/TO/c3r-cli.jar`. O bien, si ha añadido `PATH/TO/c3r-cli.jar` a su variable de entorno CLASSPATH, también puede ejecutar el nombre de la clase. El cliente de cifrado de C3R buscará en CLASSPATH para encontrarlo (por ejemplo, `java com.amazon.psion.cli.Main`).
> - El indicador `--interactive` selecciona el modo interactivo para desarrollar el esquema. Esto guía al usuario a través de un asistente para crear el esquema. Los usuarios con conocimientos avanzados pueden crear su propio esquema JSON sin necesidad de utilizar el asistente. Para obtener más información, consulte (Opcional) Crear un esquema (usuarios avanzados).

- El indicador `--output` establece un nombre de salida. Si no incluye el indicador `--output`, el cliente de cifrado de C3R intentará elegir un nombre de salida predeterminado (por ejemplo, `<input>.out.csv` o, para el esquema, `<input>.json`).

3. En `Number of target columns from source column ‘username’?`, escriba **1** y luego presione Intro.
4. En `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, escriba **f** y luego presione Intro.
5. En `Target column headername <default 'username'>`, presione Intro.

   Se utiliza el nombre predeterminado ‘`username`’.
6. En `Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, escriba **y** y luego presione Intro.

   > **Note**
   >
   > El modo interactivo sugiere añadir sufijos a los encabezados de las columna cifrados (`_fingerprint` para las columnas fingerprint y `_sealed` para las columnas sealed). Los sufijos pueden resultar útiles cuando realizas tareas como cargar datos o crear colaboraciones. Servicios de AWS AWS Clean Rooms Estos sufijos pueden ayudar a indicar qué se puede hacer con los datos cifrados de cada columna. Por ejemplo, la operación no funcionará si cifra una columna como columna sealed (`_sealed`) e intenta una operación JOIN en ella o a la inversa.

7. En `Number of target columns from source column ‘ad_variant’?`, escriba **1** y luego presione Intro.
8. En `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, escriba **c** y luego presione Intro.
9. En `Target column headername <default 'username'>`, presione Intro.

   Se utiliza el nombre predeterminado ‘`ad_variant`’.

   El esquema se escribe en un nuevo archivo llamado `ads.json`.

> **Note**
>
> Puede ver el esquema abriéndolo en cualquier editor de texto, por ejemplo, Notepad en Windows o TextEdit en macOS.

10. Ahora ya puede cifrar datos.

Ejemplo: Generar un esquema de cifrado con columnas sealed, fingerprint y columnas

En este ejemplo, para `sales.csv`, hay tres columnas: `username`, `purchased` y `product`. Para estas columnas, queremos lo siguiente:

- Que la `product` columna sea una columna `sealed`
- Que la columna `username` se cifre como columna `fingerprint`
- Que la `purchased` columna sea una columna `cleartext`

Para generar un esquema de cifrado con columnas sealed, fingerprint y cleartext

1. (Opcional) Para garantizar que el archivo c3r-cli.jar y el archivo que se va a cifrar estén presentes:

   a. Desplácese al directorio deseado y ejecute `ls` (si utiliza Mac o Unix/Linux) o `dir` si utiliza Windows).

   b. Vea la lista de archivos de datos tabulares (.csv) y elija el archivo que desea cifrar.

      En este ejemplo, `sales.csv` es el archivo que queremos cifrar.

2. Desde la CLI, ejecute el siguiente comando para crear un esquema de forma interactiva.

```
java -jar c3r-cli.jar schema sales.csv --interactive --
output=sales.json
```

> **Note**
>
> - El indicador `--interactive` selecciona el modo interactivo para desarrollar el esquema. Esto guía al usuario a través de un flujo de trabajo guiado para crear el esquema.
> - Si usted es un usuario avanzado, puede crear su propio esquema JSON sin utilizar el flujo de trabajo guiado. Para obtener más información, consulte (Opcional) Crear un esquema (usuarios avanzados).
> - Para los archivos .csv sin encabezados de columna, consulte el indicador `--noHeaders` del comando de esquema disponible en la CLI.
> - El indicador `--output` establece un nombre de salida. Si no incluye el indicador `--output`, el cliente de cifrado de C3R intentará elegir un nombre de salida predeterminado (por ejemplo, `<input>.out` o, para el esquema, `<input>.json`).

3. En `Number of target columns from source column 'username'?`, escriba **1** y luego presione Intro.
4. En `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, escriba **f** y luego presione Intro.
5. En `Target column headername <default 'username'>`, presione Intro.

   Se utiliza el nombre predeterminado '`username`'.
6. En `Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, escriba **y** y luego presione Intro.
7. En `Number of target columns from source column 'purchased'?`, escriba **1** y luego presione Intro.
8. En `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, escriba **c** y luego presione Intro.
9. En `Target column headername <default 'purchased'>`, presione Intro.

   Se utiliza el nombre predeterminado '`purchased`'.
10. En `Number of target columns from source column 'product'?`, escriba **1** y luego presione Intro.
11. En `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, escriba **s** y luego presione Intro.

12. En `Target column headername <default 'product'>`, presione Intro.

    Se utiliza el nombre predeterminado ‘`product`’.

13. En `‘product_sealed’ padding type: [n]one, [f]ixed, or [m]ax <default ’max’?>`, presione Intro para elegir el valor predeterminado.

14. Para `Byte-length beyond max length to pad cleartext to in ‘product_sealed’ <default ‘0’>?`, presione Intro para elegir el valor predeterminado.

    El esquema se escribe en un nuevo archivo llamado `sales.json`.

15. Ahora ya puede cifrar datos.

Paso 5: crear una clave secreta compartida

Para cifrar las tablas de datos, los participantes de la colaboración deben acordar una clave secreta compartida y compartirla de forma segura.

La clave secreta compartida debe tener al menos 256 bits (32 bytes). Puede especificar una clave de mayor tamaño, pero no le proporcionará ninguna garantía adicional.

> **Important**
>
> Recuerde que la clave y el ID de la colaboración utilizados para el cifrado y el descifrado deben ser idénticos para todos los participantes de la colaboración.

En las siguientes secciones se proporcionan ejemplos de comandos de consola para generar una clave secreta compartida guardada como `secret.key` en el directorio de trabajo actual del terminal correspondiente.

Temas

- Ejemplo: generación de claves con OpenSSL
- Ejemplo: generación de claves en Windows con PowerShell

Ejemplo: generación de claves con OpenSSL

Para una biblioteca de criptografía común de uso general, ejecute el comando siguiente para crear una clave secreta compartida.

```
openssl rand 32 > secret.key
```

Si la está utilizando Windows y no ha instalado OpenSSL, puede generar claves utilizando el ejemplo descrito en Ejemplo: generación de claves en Windows con PowerShell.

Ejemplo: generación de claves en Windows con PowerShell

En PowerShell, un terminal de aplicaciones disponible en Windows, ejecute el siguiente comando para crear una clave secreta compartida.

```
$bs = New-Object Byte[](32);
[Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($bs); Set-
Content 'secret.key' -Encoding Byte -Value $bs
```

Paso 6: guardar la clave secreta compartida en la variable de entorno

Una variable de entorno es una forma cómoda y ampliable para que los usuarios proporcionen una clave secreta de varios almacenes de claves, por ejemplo, AWS Secrets Manager y la pasen al cliente de cifrado C3R.

El cliente de cifrado C3R puede utilizar claves almacenadas en Servicios de AWS si se utiliza AWS CLI para almacenar esas claves en la variable de entorno correspondiente. Por ejemplo, el cliente de cifrado C3R puede usar una clave de. AWS Secrets Manager Para obtener más información, consulte Crear y administrar secretos con AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager .

> **Note**
>
> Sin embargo, antes de utilizar una Servicio de AWS como esta AWS Secrets Manager para guardar las claves C3R, compruebe que su caso de uso lo permite. Es posible que algunos casos de uso requieran que se oculte la clave. AWS Esto es para garantizar que los datos cifrados y la clave nunca estén en manos del mismo tercero.

Los únicos requisitos para una clave secreta compartida son que la clave secreta compartida esté codificada en base64 y almacenada en la variable de entorno `C3R_SHARED_SECRET`.

En las siguientes secciones se describen los comandos de la consola para convertir un archivo `secret.key` en base64 y almacenarlo como una variable de entorno. El archivo `secret.key` podría haberse generado a partir de cualquiera de los comandos enumerados en Paso 5: crear una clave secreta compartida, y este es solo un ejemplo de origen.

Almacenamiento de la clave en una variable de entorno en Windows con PowerShell

Para convertir a base64 y configurar la variable de entorno en Windows con PowerShell, ejecute el siguiente comando.

```
$Bytes=[IO.File]::ReadAllBytes((Get-Location).ToString()+'\secret.key');
 $env:C3R_SHARED_SECRET=[Convert]::ToBase64String($Bytes)
```

Almacenamiento de la clave en una variable de entorno en Linux o macOS

Para convertir a base64 y establecer la variable de entorno en Linux o macOS, ejecute el siguiente comando.

```
export C3R_SHARED_SECRET="$(cat secret.key | base64)"
```

Paso 3: cifrar los datos

Para realizar este paso, debe adquirir el ID de AWS Clean Rooms colaboración y la clave secreta compartida. Para obtener más información, consulte Requisitos previos.

En el siguiente ejemplo, ejecutamos el cifrado en `ads.csv` utilizando el esquema que hemos creado, denominado `ads.json`.

Para cifrar los datos

1. Almacene la clave secreta compartida de la colaboración en Paso 6: guardar la clave secreta compartida en la variable de entorno.
2. Desde la línea de comandos, ingrese el comando siguiente:

   ```
   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. En *<nombre de archivo .csv de entrada>*, introduzca el nombre del archivo .csv de entrada.
4. En `schema=`, introduzca el nombre del archivo de esquema de cifrado .json.
5. En `id=`, introduzca el ID de la colaboración.
6. En `output=`, introduzca el nombre del archivo de salida (por ejemplo, `ads-output.csv`).
7. Incluya cualquiera de los indicadores de línea de comandos descritos en Parámetros de computación criptográfica y Indicadores opcionales en computación criptográfica para Clean Rooms.
8. Ejecute el comando.

En el ejemplo de `ads.csv`, ejecutamos el siguiente comando.

java -jar c3r-cli.jar encrypt ***ads.csv*** --schema=***ads.json*** --id=***123e4567-e89b-42d3-a456-556642440000*** --output=***ads-output.csv***

En el ejemplo de sales.csv, ejecutamos el siguiente comando.

java -jar c3r-cli.jar encrypt ***sales.csv*** --schema=***sales.json*** --id=***123e4567-e89b-42d3-a456-556642440000***

> **Note**
>
> En este ejemplo, no especificamos un nombre de archivo de salida (`--output=`*`sales-output.csv`*). Como resultado, se generó el nombre de archivo de salida predeterminado `name-of-file.out.csv`.

Ahora ya puede verificar los datos cifrados.

Paso 8: verificar el cifrado de datos

Para verificar que los datos estaban cifrados

1. Vea el archivo de datos cifrados (por ejemplo, `sales-output.csv`).
2. Compruebe las siguientes columnas:
   a. Columna 1: cifrada (por ejemplo, `username_fingerprint`).

En las columnas fingerprint (HMAC), después de la versión y el prefijo de tipo (por ejemplo, `01:hmac:`), hay 44 caracteres de datos codificados en base64.

b. Columna 2: sin cifrar (por ejemplo, `purchased`).

c. Columna 3: cifrada (por ejemplo, `product_sealed`).

En el caso de las columnas cifradas (SELECT), la longitud del cleartext más cualquier relleno posterior a la versión y el prefijo de tipo (por ejemplo, `01:enc:`) es directamente proporcional a la longitud del cleartext columna cifrada. Es decir, la longitud es el tamaño de la entrada, más aproximadamente un 33 por ciento de sobrecarga debido a la codificación.

Ya puede hacer lo siguiente:

1. Cargar los datos cifrados a S3.
2. Crea una AWS Glue tabla.
3. Crear una tabla configurada en AWS Clean Rooms.

El cliente de cifrado de C3R creará archivos temporales que no contengan datos sin cifrar (a menos que esos datos tampoco estén cifrados en el resultado final). No obstante, es posible que algunos valores cifrados no se rellenen correctamente. Las columnas de huella digital pueden contener valores duplicados, incluso si el ajuste de colaboración `allowRepeatedFingerprintValue` es `false`. Este problema se debe a que el archivo temporal se escribe antes de comprobar las longitudes de relleno adecuadas y las propiedades de eliminación de duplicados.

Si el cliente de cifrado de C3R falla o se interrumpe durante el cifrado, es posible que se detenga después de escribir el archivo temporal, pero antes de comprobar estas propiedades y eliminar los archivos temporales. Por lo tanto, es posible que estos archivos temporales sigan en el disco. Si este es el caso, el contenido de estos archivos no protege los datos de texto sin formato en los mismos niveles que los de salida. En concreto, estos archivos temporales pueden revelar datos del texto sin formato para los análisis estadísticos, lo que no serviría de nada para el resultado final. El usuario debe eliminar estos archivos (especialmente la base de datos SQLite) para evitar que caigan en manos no autorizadas.

(Opcional) Crear un esquema (usuarios avanzados)

La creación manual de esquemas está reserva para los usuarios avanzados.

A continuación se describe el formato del archivo de esquema JSON para los archivos de entrada con o sin encabezados de columna. Los usuarios avanzados pueden escribir o modificar el esquema directamente si lo desean.

> **Note**
>
> El cliente de cifrado de C3R puede ayudarlo a crear un esquema mediante el proceso interactivo descrito en Ejemplo: Generar un esquema de cifrado con columnas sealed, fingerprint y columnas o mediante la creación de una plantilla stub.

Esquemas de tablas mapeados y posicionales

En la siguiente sección se describen dos tipos de esquemas de tabla:

- Esquema de tabla mapeado: este esquema se usa para cifrar archivos .csv con una fila de encabezado y archivos Apache Parquet.
- Esquema de tabla posicional: este esquema se usa para cifrar archivos .csv sin fila de encabezado.

El cliente de cifrado de C3R puede cifrar un archivo tabular para una colaboración. Para ello, debe tener un archivo de esquema correspondiente que especifique cómo se debe derivar la salida cifrada a partir de la entrada.

El cliente de cifrado de C3R puede ayudar a generar un esquema para un archivo `INPUT` ejecutando el comando de esquema del cliente de cifrado de C3R en la línea de comandos. Un ejemplo de comando es `java -jar c3r-cli.jar schema --interactive INPUT`.

El esquema especifica la siguiente información:

1. Qué columnas de origen se asignan a qué columnas transformadas en el archivo de salida mediante sus nombres de encabezado (esquemas mapeados) o su posición (esquemas posicionales)
2. Qué columnas de destino van a permanecer como cleartext
3. Qué columnas de destino se van a cifrar para las consultas SELECT
4. Qué columnas de destino se van a cifrar para las consultas JOIN

Esta información está codificada en un archivo de esquema JSON específico de tabla, que consta de un único objeto cuyo campo `headerRow` es un valor booleano. El valor debe ser `true` para los archivos Parquet y los archivos .csv con fila de encabezado, y `false` para el resto.

Esquema de la tabla mapeado

El esquema mapeado tiene la siguiente forma.

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": STRING,
      "targetHeader": STRING,
      "type": TYPE,
      "pad": PAD
    },
    ...
  ]
}
```

Si `headerRow` es `true`, es el siguiente campo del objeto es `columns`, que contiene una matriz de esquemas de columnas que asignan los encabezados de origen a los encabezados de destino (es decir, objetos JSON que describen lo que deben contener las columnas de salida).

- `sourceHeader`: el nombre del encabezado `STRING` de la columna de origen a partir de cual se derivan los datos.

  > **Note**
  >
  > Una misma columna de origen se puede utilizar para varias columnas de destino.
  > Una columna del archivo de entrada que no aparezca enumerada como `sourceHeader` en ninguna parte del esquema no aparecerá en el archivo de salida.

- `targetHeader`: el nombre del encabezado `STRING` de la columna correspondiente del archivo de salida.

> **Note**
>
> Este campo es opcional para los esquemas mapeados. Si se omite este campo, `sourceHeader` se reutiliza para el nombre del encabezado en el archivo de salida. Se anexa `_fingerprint` o `_sealed` si la columna de salida es una columna fingerprint o una columna sealed, respectivamente.

- `type`: el TYPE de la columna de destino del archivo de salida. Es decir, una de las columnas `cleartext`, `sealed` o `fingerprint` dependiendo de cómo se vaya a utilizar la columna en la colaboración.
- `pad`: un campo de un objeto de esquema de columnas que solo está presente cuando TYPE es `sealed`. Su valor correspondiente de PAD es un objeto que describe cómo deben rellenarse los datos antes del cifrado.

```
{
  "type": PAD_TYPE,
  "length": INT
}
```

  Para especificar el relleno previo al cifrado, se utiliza `type` y `length` de la siguiente manera:

  - PAD_TYPE como `none`: no se aplicará ningún relleno a los datos de la columna y el campo `length` no es aplicable (es decir, se omite).
  - PAD_TYPE como `fixed`: los datos de la columna se rellenan hasta el número de bytes especificado, `length`.
  - PAD_TYPE como `max`: los datos de la columna se rellenan hasta el tamaño de la longitud en bytes del valor más largo, más `length` bytes adicionales.

El siguiente es un ejemplo de esquema mapeado, con una columna 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
      }
    }
  ]
}
```

Un ejemplo más complejo sería el siguiente ejemplo de un archivo .csv con encabezados.

```
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
```

En el siguiente ejemplo de esquema mapeado, las columnas `FirstName` y `LastName` son columnas `cleartext`. La columna `State` está cifrada como columna `fingerprint` y como columna `sealed` con un relleno de `none`. Las columnas restantes se omiten.

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

El siguiente es el archivo .csv que resulta del 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 tabla posicional

El esquema posicional tiene la siguiente forma.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      },
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      }
    ],
    [],
    ...
  ]
}
```

Si `headerRow` es `false`, es el siguiente campo del objeto es `columns`, que contiene una matriz de entradas. Cada entrada es en sí misma una matriz de cero o más esquemas de columnas posicionales (sin campo `sourceHeader`), que son objetos JSON que describen lo que debe contener la salida.

- `sourceHeader`: el nombre del encabezado `STRING` de la columna de origen a partir de cual se derivan los datos.

> **Note**
>
> Este campo debe omitirse en los esquemas posicionales. En los esquemas posicionales, la columna de origen se deduce mediante el índice correspondiente de la columna en el archivo de esquema.

- `targetHeader`: el nombre del encabezado `STRING` de la columna correspondiente del archivo de salida.

> **Note**
>
> Este campo es obligatorio para los esquemas posicionales.

- `type`: el `TYPE` de la columna de destino del archivo de salida. Es decir, una de las columnas `cleartext`, `sealed` o `fingerprint` dependiendo de cómo se vaya a utilizar la columna en la colaboración.
- `pad`: un campo de un objeto de esquema de columnas que solo está presente cuando `TYPE` es `sealed`. Su valor correspondiente de `PAD` es un objeto que describe cómo deben rellenarse los datos antes del cifrado.

```
{
  "type": PAD_TYPE,
  "length": INT
}
```

Para especificar el relleno previo al cifrado, se utiliza `type` y `length` de la siguiente manera:

- `PAD_TYPE` como `none`: no se aplicará ningún relleno a los datos de la columna y el campo `length` no es aplicable (es decir, se omite).
- `PAD_TYPE` como `fixed`: los datos de la columna se rellenan hasta el número de bytes especificado, `length`.
- `PAD_TYPE` como `max`: los datos de la columna se rellenan hasta el tamaño de la longitud en bytes del valor más largo, más `length` bytes adicionales.

> **Note**
>
> `fixed` es útil si sabe con antelación cuál es el límite superior del tamaño en bytes de los datos de la columna. Se produce un error si algún dato de esa columna supera la `length` especificada.
> `max` resulta práctico cuando se desconoce el tamaño exacto de los datos de entrada, ya que funciona independientemente del tamaño de los datos. Sin embargo, `max` requiere un tiempo de procesamiento adicional porque cifra los datos dos veces. `max` cifra los datos una vez cuando se leen en el archivo temporal y una vez que se conoce la entrada de datos más larga de la columna.
> Además, la longitud del valor más largo no se guarda entre las invocaciones del cliente. Si tiene previsto cifrar los datos por lotes o cifrar datos nuevos periódicamente, tenga en cuenta que la longitud del texto cifrado resultante puede variar de un lote a otro.

A continuación se muestra un ejemplo de 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 ejemplo complejo, el siguiente es un ejemplo de un archivo .csv sin la primera fila con los encabezados.

```
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
```

El esquema posicional tiene la siguiente forma.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": "GivenName",
        "type": "cleartext"
      }
    ],
    [
      {
        "targetHeader": "Surname",
        "type": "cleartext"
      }
    ],
    [],
```

```
    [],
    [
      {
        "targetHeader": "State_Join",
        "type": "fingerprint"
      },
      {
        "targetHeader": "State",
        "type": "sealed",
        "pad": {
          "type": "none"
        }
      }
    ],
    [],
    [],
    [],
    []
  ]
}
```

El esquema anterior produce el siguiente archivo de salida con una fila de encabezados que contiene los encabezados 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=
```

Crear una tabla configurada en AWS Clean Rooms

Una tabla configurada es una referencia a una tabla existente en la AWS Glue Data Catalog. Contiene una regla de análisis que determina cómo se pueden consultar los datos en AWS Clean Rooms. Las tablas configuradas se pueden asociar a una o más colaboraciones. Para obtener más información AWS Glue, consulte la Guía para desarrolladores de AWS Glue.

Utilice la generación de estadísticas proporcionada por AWS Glue para calcular las estadísticas a nivel de columna para las tablas. AWS Glue Data Catalog Una vez que AWS Glue genera las estadísticas para las tablas del catálogo de datos, Amazon Redshift Spectrum las utiliza automáticamente para optimizar el plan de consultas. Para obtener más información sobre cómo calcular las estadísticas a nivel de columna mediante el uso de estadísticas de columnas AWS Glue, consulte la Guía para trabajar con estadísticas de columnas.

Creación de una tabla configurada

En este paso, creará una tabla configurada para AWS Clean Rooms utilizarla en la colaboración.

Para crear una tabla configurada en AWS Clean Rooms

1. Inicie sesión en la AWS Clean Rooms consola AWS Management Console y ábrala con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Tablas configuradas.
3. En la esquina superior derecha, elija Configurar nueva tabla.
4. En Configurar nueva tabla, seleccione Elegir tabla de AWS Glue :
    a. Seleccione la Base de datos que desea configurar en la lista desplegable.
    b. Seleccione la Tabla que desea configurar en la lista desplegable.

> **Note**
>
> Para comprobar que se trata de la tabla correcta, realice una de las siguientes acciones:
>
> - Selecciona Ver en AWS Glue.
> - Active Ver esquema para ver el esquema.

5. En Columnas permitidas en colaboraciones, seleccione Todas las columnas o Lista personalizada.

Si selecciona...	Entonces...
Todas las columnas	Se permite el uso de todas las columnas en AWS Clean Rooms (sujeto a las reglas de análisis).
Lista personalizada	Seleccione una o más columnas que desee permitir en la lista desplegable Especificar columnas permitidas.

6. En Detalles de la tabla configurada,

   a. Introduzca un Nombre para la tabla configurada.

      Puede usar el nombre predeterminado o cambiar el nombre de esta tabla.

   b. Introduzca una Descripción de la tabla.

      La descripción ayuda a diferenciarla de otras tablas configuradas con nombres similares.

   c. Si desea habilitar la opción de Etiquetas para el recurso de tabla configurada, seleccione Añadir nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.

7. Seleccione Configurar nuevo cliente.

Siguientes pasos

Ahora que ha creado una tabla configurada, puede hacer lo siguiente:

- Configurar una regla de análisis para la tabla configurada
- Asociar la tabla configurada a una colaboración

Configurar una regla de análisis en una tabla configurada

En las secciones siguientes se describe cómo configurar una regla de análisis en una tabla configurada. Al definir las reglas de análisis, puede autorizar al miembro que puede realizar consultas a ejecutar consultas que coincidan con una regla de análisis específica admitida en AWS Clean Rooms.

AWS Clean Rooms admite los siguientes tipos de reglas de análisis: de agregación, de lista y personalizadas.

Puede haber una sola regla de análisis por tabla configurada.

> **Important**
>
> Si utiliza la computación criptográfica para Clean Rooms y tiene tablas de datos cifrados en la colaboración, la regla de análisis que añada a la tabla configurada cifrada debe ser coherente con la forma en que se cifraron los datos. Por ejemplo, si ha cifrado los datos para SELECT (regla de análisis de agregación), no debe agregar la regla de análisis para JOIN (regla de análisis de lista).

Para comprender los tipos de reglas de análisis disponibles en AWS Clean Rooms, consulte Reglas de análisis en AWS Clean Rooms.

Para obtener más información acerca de la regla de análisis de agregación, consulte Regla de análisis de agregación.

Para obtener más información acerca de la regla de análisis de lista, consulte Regla de análisis de lista.

Para obtener más información sobre la regla de análisis personalizada, consulte Regla de análisis personalizada en AWS Clean Rooms.

Una vez que revise y comprenda estas secciones, podrá realizar los siguientes procedimientos:

Temas

Configurar una regla de análisis de agregación en una tabla (flujo guiado)

La regla de análisis de agregación permite realizar consultas que agreguen estadísticas sin revelar información de nivel de fila utilizando las funciones COUNT, SUM y AVG en dimensiones opcionales.

Este procedimiento describe el proceso de añadir una regla de análisis de agregación a la tabla configurada mediante la opción Flujo guiado de la consola de AWS Clean Rooms.

Para añadir la regla de análisis de agregación a una tabla (flujo guiado)

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Tablas configuradas.
3. Seleccione la tabla configurada.
4. En la página de detalles de la tabla configurada, seleccione Configurar regla de análisis.
5. En Paso 1: Elegir el tipo, en Tipo, deje la opción Agregación seleccionada, tal como aparece de forma predeterminada.
6. En Método de creación, seleccione Flujo guiado y, a continuación, seleccione Siguiente.
7. En Paso 2: Especificar controles de consulta, en Funciones de agregación:

    a. Elija una Función de agregación en el menú desplegable:

        - COUNT
        - COUNT DISTINCT
        - SUM
        - SUM DISTINCT
        - AVG

    b. Elija qué columnas se pueden usar en la Función de agregación en el menú desplegable Columnas.

    c. (Opcional) Seleccione Añadir otra función para añadir otra función de agregación y asociar una o más columnas a esa función.

> **Note**
>
> Se requiere al menos una función de agregación.

d. (Opcional) Seleccione Eliminar para eliminar una función de agregación.

8. En Controles de combinación,

a. Seleccione una opción para Permitir que la tabla se consulte por sí misma:

Si selecciona...	Entonces...
No, solo se puede consultar el solapamiento	La tabla solo se puede consultar si está combinada con una tabla propiedad del miembro que puede realizar consultas.
Sí	La tabla se puede consultar por sí misma o cuando se combina con otras tablas.

b. En Especificar columnas de combinación, seleccione las columnas que desea permitir que se utilicen en la instrucción INNER JOIN.

Esto es opcional si ha seleccionado Sí en el paso anterior.

c. En Especificar operadores permitidos para la coincidencia, elija qué operadores (si los hay) se pueden usar para hacer coincidir varias columnas de combinación. Si selecciona dos o más columnas JOIN, será obligatorio el uso de uno de estos operadores.

Si selecciona...	Entonces...
AND	Puede incluir `AND` en las condiciones de coincidencia `INNER JOIN` para combinar una columna con otra entre tablas.
OR	Puede incluir `OR` en las condiciones de coincidencia `INNER JOIN` para combinar varias coincidencias de columna entre tablas. Este operador lógico es útil para obtener una tasa de coincidencia más alta.

9. (Opcional) En Controles de dimensión, en el menú desplegable Especificar columnas de dimensión, seleccione las columnas que desea permitir que se usen en la instrucción SELECT y las partes WHERE, GROUP BY y ORDER BY de la consulta.

> **Note**
>
> No se pueden usar columnas de combinación ni de función de agregación como columnas de dimensión.

10. En Funciones escalares, seleccione una opción para ¿Qué funciones escalares desea permitir?

Si selecciona...	Entonces...
Todas las que admite actualmente AWS Clean Rooms	Se permiten todas las funciones escalares actualmente admitidas por AWS Clean Rooms. • Puede seleccionar Ver lista para ver la lista completa de Funciones escalares admitidas en AWS Clean Rooms.
Una lista personalizada	Puede personalizar las funciones escalares que desea permitir. • Elija una o más opciones del menú desplegable Especificar las funciones escalares permitidas.
Ninguna	No se permite ninguna función escalar.

Para obtener más información, consulte Funciones escalares.

11. Seleccione Siguiente.
12. En Paso 3: Especificar controles de resultados de consulta, en Restricciones de agregación:
    a. Seleccione cada Nombre de columna en la lista desplegable.

b. Seleccione en la lista desplegable cada Número mínimo de valores diferenciados que se debe cumplir para que se devuelva cada fila de salida después de aplicarle la función COUNT DISTINCT.

c. Seleccione Añadir restricción para añadir más restricciones de agregación.

d. (Opcional) Seleccione Eliminar para eliminar una restricción de agregación.

13. Elija Siguiente.
14. En Paso 4: Revisar y configurar, revise las selecciones que realizó en los pasos anteriores, edítelas si es necesario y, a continuación, seleccione Configurar regla de análisis.

Verá un mensaje de confirmación en el que se indica que ha configurado correctamente una regla de análisis de agregación en la tabla.

Configurar una regla de análisis de lista en una tabla (flujo guiado)

La regla de análisis de lista permite realizar consultas que generen listas de nivel de fila del solapamiento entre la tabla asociada y una tabla del miembro que puede realizar consultas.

Este procedimiento describe el proceso de añadir la regla de análisis de lista a la tabla configurada mediante la opción Flujo guiado de la consola de AWS Clean Rooms.

Para añadir una regla de análisis de lista a una tabla (flujo guiado)

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Tablas configuradas.
3. Seleccione la tabla configurada.
4. En la página de detalles de la tabla configurada, seleccione Configurar regla de análisis.
5. En Paso 1: Elegir tipo, en Tipo, seleccione la opción Lista.
6. En Método de creación, seleccione Flujo guiado y, a continuación, seleccione Siguiente.
7. En Paso 2: Especificar controles de consulta, en Controles de combinación:

   a. En Especificar columnas de combinación, seleccione las columnas que desea permitir que se utilicen en la instrucción INNER JOIN.

b. En Especificar operadores permitidos para la coincidencia, elija qué operadores (si los hay) se pueden usar para hacer coincidir varias columnas de combinación. Si selecciona dos o más columnas JOIN, será obligatorio el uso de uno de estos operadores.

Si selecciona...	Entonces...
AND	Puede incluir `AND` en las condiciones de coincidencia `INNER JOIN` para combinar una columna con otra entre tablas.
OR	Puede incluir `OR` en las condiciones de coincidencia `INNER JOIN` para combinar varias coincidencias de columna entre tablas. Este operador lógico es útil para obtener una tasa de coincidencia más alta.

8. (Opcional) En Controles de lista, en el menú desplegable Especificar columnas de la lista, seleccione las columnas que desea permitir que se utilicen en el resultado de la consulta (es decir, que se usen en la instrucción SELECT) o que se usen para filtrar los resultados (es decir, en la instrucción WHERE).
9. Elija Siguiente.
10. En Paso 3: Revisar y configurar, revise las selecciones que realizó en los pasos anteriores, edítelas si es necesario y, a continuación, seleccione Configurar regla de análisis.

Verá un mensaje de confirmación en el que se indica que ha configurado correctamente una regla de análisis de lista en la tabla.

Configurar una regla de análisis personalizada en una tabla (flujo guiado)

La regla de análisis personalizada permite realizar consultas SQL personalizadas en una tabla configurada. La regla de análisis personalizada es obligatoria cuando se utilizan plantillas de análisis o la privacidad diferencial.

Este procedimiento describe el proceso de añadir la regla de análisis personalizada a la tabla configurada mediante la opción Flujo guiado de la consola de AWS Clean Rooms.

Para añadir una regla de análisis personalizada a una tabla (flujo guiado)

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Tablas configuradas.
3. Seleccione la tabla configurada.
4. En la página de detalles de la tabla configurada, seleccione Configurar regla de análisis.
5. En Paso 1: Elegir tipo, en Tipo, seleccione la opción Personalizada.
6. En Método de creación, seleccione Flujo guiado y, a continuación, seleccione Siguiente.
7. En el Paso 2: Configuración de la privacidad diferencial, determine si desea activar o desactivar la privacidad diferencial. La privacidad diferencial es una técnica probada matemáticamente para proteger sus datos de los ataques de reidentificación.

   a. Para una privacidad diferencial:

Si...	Entonces seleccione...
Tiene datos en el nivel de usuario y desea protegerse contra los intentos de reidentif icación	Activar
No tiene datos en el nivel de usuario o no necesita protección contra los intentos de reidentificación	Desactivar

   b. Si ha optado por activar la privacidad diferencial, seleccione la columna Identificador de usuario que contiene el identificador único de sus usuarios, como la columna `user_id`, cuya privacidad desea proteger. Si desea activar la privacidad diferencial para dos o más tablas de una colaboración, debe configurar la misma columna que la columna Identificador de usuario en ambas reglas de análisis para mantener una definición coherente de los usuarios en todas las tablas. Si la configuración es incorrecta, el miembro que puede realizar la consulta recibe un mensaje de error que indica que hay dos columnas entre las que elegir para calcular el número de contribuciones de los usuarios (por ejemplo, el número de impresiones de anuncios realizadas por un usuario) al ejecutar la consulta.

   c. Elija Siguiente.

8. En Paso 3: Especificar controles de consulta,

a. En Tipo de control:

Si desea…	Entonces seleccione...
Revisar cada nueva plantilla de análisis antes de ejecutarla en la tabla configurada	Revisar cada nuevo análisis antes de permitir que se ejecute en esta tabla
Permitir que se ejecute cualquier plantilla de análisis o consulta directa en la tabla configurada	Permitir que cualquier consulta creada por determinados colaboradores se ejecute sin revisión en esta tabla

b. Seleccione una de las siguientes opciones:

Si ha seleccionado...	Entonces...
Revisar cada nuevo análisis antes de permitir que se ejecute en esta tabla	En Plantillas de análisis que se pueden ejecutar, seleccione Añadir plantilla de análisis y, a continuación, seleccione la Colaboración y la Plantilla de análisis que corresponda en las listas desplegables.
Permitir que cualquier consulta creada por determinados colaboradores se ejecute sin revisión en esta tabla	En Cuentas de AWS autorizadas a crear cualquier consulta, seleccione Añadir Cuenta de AWS y, a continuación, seleccione el ID de Cuenta de AWS que corresponda.

9. Elija Siguiente.
10. En Paso 4: Revisar y configurar, revise las selecciones que realizó en los pasos anteriores, edítelas si es necesario y, a continuación, seleccione Configurar regla de análisis.

Ve un mensaje de confirmación en el que se indica que ha configurado correctamente una regla de análisis personalizada en la tabla.

Configurar una regla de análisis en una tabla (editor JSON)

El siguiente procedimiento muestra cómo añadir una regla de análisis a una tabla mediante la opción Editor JSON de la consola de AWS Clean Rooms.

Para configurar una regla de análisis de agregación, de lista o personalizada en una tabla (editor JSON)

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Tablas configuradas.
3. Seleccione la tabla configurada.
4. En la página de detalles de la tabla configurada, seleccione Configurar regla de análisis.
5. En Paso 1: Elegir tipo, en Tipo, seleccione la opción Agregación, Lista o Personalizada.
6. En Método de creación, seleccione Editor JSON y, a continuación, seleccione Siguiente.
7. En Paso 2: Especificar controles, puede optar por insertar una estructura de consulta (Insertar plantilla) o insertar un archivo (Importar desde archivo).

Si selecciona...	Entonces...
Insertar plantilla	1. Especifique los parámetros de la regla de análisis seleccionada en Definición de la regla de análisis. 2. Puede pulsar Ctrl + barra espaciadora para habilitar la función de autocompletar. Para obtener más información acerca de los parámetros de la regla de análisis de agregación, consulte Regla de análisis de agregación: controles de consulta. Para obtener más información acerca de los parámetros de la regla de análisis de lista, consulte Regla de análisis de lista: controles de consulta.

Si selecciona...	Entonces...
Importar desde archivo	1. Seleccione el archivo JSON en su unidad local. 2. Elija Open. La Definición de la regla de análisis muestra la regla de análisis del archivo cargado.

8. Elija Siguiente.
9. En Paso 3: Revisar y configurar, revise las selecciones que realizó en los pasos anteriores, edítelas si es necesario y, a continuación, seleccione Configurar regla de análisis.

Recibe un mensaje de confirmación en el que se indica que ha configurado correctamente una regla de análisis en la tabla.

Siguientes pasos

Ahora que ha configurado una regla de análisis para la tabla configurada, ya puede:

- Asociar una tabla configurada a una colaboración
- Consultar las tablas de datos (como miembro que puede realizar consultas)

Asociar una tabla configurada a una colaboración

Una vez que haya creado una tabla configurada y le haya añadido una regla de análisis, podrá asociarla a una colaboración.

Important

Antes de asociar las AWS Glue tablas configuradas a la colaboración, la ubicación de la AWS Glue tabla debe apuntar a una carpeta de Amazon Simple Storage Service (Amazon S3) y no a un único archivo. Puede verificar esta ubicación consultando la tabla de la AWS Glue consola en https://console.aws.amazon.com/glue/.

Note

Si ha configurado el cifrado AWS Glue y creado un rol de servicio, debe conceder acceso a ese rol para que lo utilice AWS KMS keys para descifrar AWS Glue tablas.
Si asoció una tabla configurada respaldada por un conjunto de datos de Amazon S3 AWS KMS cifrado, debe conceder al rol acceso para usar la clave de KMS para descifrar los datos de Amazon S3.
Para obtener más información, consulte Configuración del cifrado en AWS Glue, en la Guía del desarrollador de AWS Glue .

En los temas siguientes se describe cómo asociar una tabla configurada a una colaboración mediante la AWS Clean Rooms consola:

Temas

Para obtener información sobre cómo asociar sus tablas configuradas a la colaboración mediante los SDK de AWS , consulte Referencia de la API de AWS Clean Rooms .

Asociar una tabla configurada desde la página de detalles de la tabla configurada

Para asociar AWS Glue tablas a la colaboración desde la página de detalles de la tabla configurada

1. Inicie sesión en la consola AWS Management Console y abra la AWS Clean Rooms consola con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Tablas configuradas.
3. Seleccione la tabla configurada.
4. En la página de detalles de la tabla configurada, seleccione Asociar a colaboración.
5. En el cuadro de diálogo Asociar tabla a colaboración, seleccione la Colaboración en la lista desplegable.
6. Seleccione Elegir colaboración.

   En la página Asociar tabla, el nombre de la tabla configurada que ha seleccionado aparece en la sección Elegir tabla configurada.
7. En Elegir tabla configurada, haga lo siguiente:

Si desea…	Entonces...
Configurar una nueva tabla	Seleccione Configurar tabla y siga las indicaciones de la página Configurar tabla.
Ver el esquema y la regla de análisis de la tabla configurada	Active Ver esquema y regla de análisis.

8. Especifique los permisos de Acceso a servicios seleccionando Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

Si selecciona...	Entonces...
Crear y usar un nuevo rol de servicio	• AWS Clean Rooms crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `cleanrooms-<timestamp>`

Si selecciona...	Entonces...
	• Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, puede seleccionar Estos datos están cifrados con una clave KMS y, a continuación, introducir una AWS KMS key que se utilizará para descifrar los datos introducidos.
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable. Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. 2. Para ver la función de servicio, seleccione el enlace externo Ver en IAM. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. De forma predeterminada, AWS Clean Rooms no intenta actualizar la política de rol existente para añadir los permisos necesarios. 3. (Opcional) Seleccione la casilla de verificación Agregar una política preconfigurada con los permisos necesarios para este rol para adjuntar los permisos necesarios al rol. Debe tener permisos para modificar roles y crear políticas.

> **Note**
>
> - AWS Clean Rooms requiere permisos para realizar consultas de acuerdo con las reglas de análisis. Para obtener más información sobre los permisos para AWS Clean Rooms, consulteAWS políticas gestionadas para AWS Clean Rooms.
> - Si el rol no tiene permisos suficientes AWS Clean Rooms, recibirá un mensaje de error que indica que el rol no tiene permisos suficientes AWS Clean Rooms. Debe agregar la política de rol antes de continuar.
> - Si no puede modificar la política de rol, recibirá un mensaje de error que indica que AWS Clean Rooms no ha podido encontrar la política del rol de servicio.

9. Si desea habilitar Etiquetas para el recurso de asociación de tablas configuradas, seleccione Agregar nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.
10. Seleccione Asociar tabla.

Asociar una tabla configurada desde la página de detalles de la colaboración

Para asociar AWS Glue tablas a la colaboración desde la página de detalles de la colaboración

1. Inicie sesión en la consola AWS Management Console y abra la AWS Clean Rooms consola con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. En la pestaña Tablas, seleccione Asociar tabla.
5. En Elegir tabla configurada, haga lo siguiente:

Si desea…	Entonces...
Elegir una tabla configurada existente	Seleccione el Nombre de la tabla configura da que desea asociar a la colaboración en la lista desplegable.

Si desea…	Entonces...
Configurar una nueva tabla	Seleccione Configurar tabla y siga las indicaciones de la página Configurar tabla.
Ver el esquema y la regla de análisis de la tabla configurada	Active Ver esquema y regla de análisis.

6. En Detalles de asociación de tablas,

   a. Introduzca un Nombre para la tabla asociada.

      Puede usar el nombre predeterminado o cambiar el nombre de esta tabla.

   b. (Opcional) Ingrese una Descripción de la tabla.

      La descripción ayuda a escribir las consultas.

7. Especifique los permisos de Acceso a servicios seleccionando Crear y usar un nuevo rol de servicio o Usar un rol de servicio existente.

Si selecciona...	Entonces...
Crear y usar un nuevo rol de servicio	• AWS Clean Rooms crea un rol de servicio con la política requerida para esta tabla. • El Nombre del rol de servicio predeterminado es `cleanrooms-<timestamp>` . • Debe tener permisos para crear roles y adjuntar políticas. • Si los datos de entrada están cifrados, puede seleccionar Estos datos están cifrados con una clave KMS y, a continuación, introducir una AWS KMS key que se utilizará para descifrar los datos introducidos.
Usar un rol de servicio existente	1. Seleccione un Nombre de rol de servicio existente en la lista desplegable.

Si selecciona...	Entonces...
	Si tiene permisos de listas de roles, se mostrará la lista de roles. Si no tiene permisos de listas de roles, puede ingresar el nombre de recurso de Amazon (ARN) del rol que desea usar. 2. Para ver la función de servicio, seleccione el enlace externo Ver en IAM. Si no hay ningún rol de servicio existente, la opción Usar un rol de servicio existente no estará disponible. De forma predeterminada, AWS Clean Rooms no intenta actualizar la política de roles existente para añadir los permisos necesarios. 3. (Opcional) Seleccione la casilla de verificación Agregar una política preconfig urada con los permisos necesarios para este rol para adjuntar los permisos necesarios al rol. Debe tener permisos para modificar roles y crear políticas.

Note

- AWS Clean Rooms requiere permisos para realizar consultas de acuerdo con las reglas de análisis. Para obtener más información sobre los permisos para AWS Clean Rooms, consulteAWS políticas gestionadas para AWS Clean Rooms.
- Si el rol no tiene permisos suficientes AWS Clean Rooms, recibirá un mensaje de error que indica que el rol no tiene permisos suficientes AWS Clean Rooms. Debe agregar la política de rol antes de continuar.

- Si no puede modificar la política de rol, recibirá un mensaje de error que indica que AWS Clean Rooms no ha podido encontrar la política del rol de servicio.

8. Si desea habilitar Etiquetas para el recurso de asociación de tablas configuradas, seleccione Agregar nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.
9. Seleccione Asociar tabla.

Siguientes pasos

Ahora que ha asociado la tabla de datos configurada a la colaboración, ya puede:

- Editar la colaboración (si es el creador de la colaboración)
- Consultar las tablas de datos (como miembro que puede realizar consultas)

Configuración de la política de privacidad diferencial

Este procedimiento describe el proceso de configuración de la política de privacidad diferencial en una colaboración mediante la opción Flujo guiado de la AWS Clean Rooms consola. Este paso solo se ejecuta una vez para todas las tablas con protección de privacidad diferencial.

Para configurar los ajustes de privacidad diferencial (flujo guiado)

1. Inicie sesión en la AWS Clean Rooms consola AWS Management Console y ábrala con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. En la pestaña Tablas de la página de colaboración, elija Configuración de la política de privacidad diferencial.
5. En la página Configuración de la política de privacidad diferencial, elija valores para las siguientes propiedades:

   - Presupuesto de privacidad
   - Actualizar mensualmente el presupuesto de privacidad
   - Ruido agregado por consulta

   Puede utilizar los valores predeterminados o introducir valores personalizados que admitan su caso de uso específico. Tras elegir los valores de Presupuesto de privacidad y Ruido añadido por consulta, puede obtener una vista previa de la utilidad resultante en lo que respecta al número de agregaciones posibles en todas las consultas de sus datos.
6. Elija Configurar.

Verá un mensaje de confirmación en el que se indica que ha configurado correctamente la política de privacidad diferencial para la colaboración.

Siguientes pasos

Ahora que ha configurado la privacidad diferencial, puede hacer lo siguiente:

- Consultar las tablas de datos (como miembro que puede realizar consultas)

- Administrar la colaboración (si es el creador de la colaboración)

Trabajar con plantillas de análisis

Las plantillas de análisis funcionan con Regla de análisis personalizada en AWS Clean Rooms. Con una plantilla de análisis, puede definir parámetros que le ayuden a reutilizar la misma consulta. AWS Clean Rooms admite un subconjunto de parametrización con valores literales.

Las plantillas de análisis son específicas de la colaboración. En cada colaboración, los miembros pueden ver solo las consultas de dicha colaboración. Si tiene previsto utilizar la privacidad diferencial en una colaboración, debe asegurarse de que sus plantillas de análisis sean compatibles con la estructura de consultas de uso general de la privacidad diferencial de AWS Clean Rooms .

Temas

Crear una plantilla de análisis

Para obtener información sobre cómo crear una plantilla de análisis mediante los AWS SDK, consulte la referencia de la AWS Clean Rooms API.

Para crear una plantilla de análisis mediante la consola AWS Clean Rooms

1. Inicie sesión en la AWS Clean Rooms consola AWS Management Console y ábrala con la Cuenta de AWS que funcionará como creador de colaboraciones.
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. En la pestaña Plantillas, vaya a la sección Plantillas de análisis creadas por usted.
5. Seleccione Crear plantilla de análisis.
6. En la página Crear plantilla de análisis, en Detalles, introduzca un nombre y una Descripción opcional.
7. En Tablas, consulte las tablas configuradas asociadas a la colaboración.
8. En Definición,

    a. Introduzca la definición de la plantilla de análisis.

b. Seleccione Importar desde para importar una definición.

c. (Opcional) Especifique un parámetro en el editor SQL introduciendo dos puntos (`:`) delante del nombre del parámetro.

   Por ejemplo:

   ```
   WHERE table1.date + :date_period > table1.date
   ```

9. Si ha añadido parámetros anteriormente, en Parámetros: opcional, para cada Nombre de parámetro, elija el Tipo y el Valor predeterminado (opcional).
10. Si desea habilitar la opción de Etiquetas para el recurso de tabla configurada, seleccione Añadir nueva etiqueta y, a continuación, introduzca el par de Clave y Valor.
11. Seleccione Crear.

Ya puede hacer lo siguiente:

- Informar al miembro colaborador de que puede Revisar una plantilla de análisis (opcional si desea consultar sus propios datos).

Revisar una plantilla de análisis

Una vez que un miembro de la colaboración haya creado una plantilla de análisis, puede revisarla y aprobarla. Una vez aprobada la plantilla de análisis, se puede incluir una consulta AWS Clean Rooms.

Para revisar una plantilla de análisis mediante la AWS Clean Rooms consola

1. Inicie sesión en la AWS Clean Rooms consola AWS Management Console y ábrala con la Cuenta de AWS que funcionará como creador de colaboraciones.
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. En la pestaña Plantillas, vaya a la sección Plantillas de análisis creadas por usted.
5. Elija la plantilla de análisis que tenga el estado Puede ejecutarse (No requiere su revisión).
6. Elija Revisar.
7. Revise la Descripción general, la definición y los Parámetros de la regla de análisis (si procede).

8. Revise las tablas configuradas que se enumeran en Tablas a las que se hace referencia en la definición.

   El Estado que aparece junto a cada tabla indicará Plantilla no permitida.

9. Elija una tabla.

En el caso de	Entonces elija...
Aprueba la plantilla de análisis	plantilla en la tabla. Confirme su aprobación eligiendo.
No aprueba la plantilla de análisis	No permitir

Ahora puede utilizar la plantilla de análisis para consultar las tablas de datos (como miembro que puede realizar consultas).

Consulta de tablas configuradas mediante una plantilla de análisis

Este procedimiento muestra cómo utilizar una plantilla de análisis en la AWS Clean Rooms consola para consultar las tablas configuradas con la regla de análisis personalizada.

Para utilizar una plantilla de análisis para consultar tablas configuradas con la regla de análisis Personalizada

1. Inicie sesión en la AWS Clean Rooms consola AWS Management Console y ábrala con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración cuyo estado de Sus capacidades como miembro sea Consultar.
4. En la pestaña Consultas, en Tablas, consulte las tablas y su tipo de regla de análisis asociada (Regla de análisis personalizada).

> **Note**
>
> Si no ve las tablas que esperaba en la lista, puede deberse a los siguientes motivos:
>
> - Las tablas no se han asociado.

- Las tablas no tienen una regla de análisis configurada.

5. En la sección Análisis, seleccione la plantilla de análisis en la lista desplegable.
6. Introduzca el valor de los parámetros de la plantilla de análisis que desea utilizar en la consulta. El valor debe estar en el tipo de datos especificado para el parámetro. Puede utilizar valores diferentes cada vez que ejecute la plantilla de análisis. Está vacío o no se admiten los NULL valores del parámetro. Tampoco se admite el uso de parámetros en la LIMIT cláusula.
7. Elija Ejecutar.

> **Note**
>
> No podrá ejecutar la consulta si el miembro que puede recibir los resultados no ha configurado los ajustes de resultados de consulta.

8. Siga ajustando los parámetros y vuelva a ejecutar la consulta, o pulse el botón + para iniciar una nueva consulta en una pestaña nueva.

Consultar datos en una colaboración

Como miembro que puede realizar consultas, puede hacer una de las cosas siguientes opciones:

- Crear una consulta SQL manualmente con el editor de código SQL.
- Usar la interfaz de usuario del creador de análisis para crear una consulta sin tener que escribir código SQL.
- Usar una plantilla de análisis aprobada.

Cuando el miembro que puede realizar consultas ejecuta una consulta SQL en las tablas de la colaboración, AWS Clean Rooms asume las funciones pertinentes para acceder a las tablas en su nombre. AWS Clean Rooms aplica las reglas de análisis necesarias a la consulta de entrada y a su salida.

AWS Clean Rooms admite consultas SQL que pueden ser diferentes a las de otros motores de consultas. Para ver las especificaciones, consulte la Referencia de SQL de AWS Clean Rooms. Si desea ejecutar consultas en tablas de datos protegidas con privacidad diferencial, debe asegurarse de que sus consultas sean compatibles con la estructura de consultas de uso general de la privacidad diferencial de AWS Clean Rooms .

> **Note**
>
> Cuando se utiliza la computación criptográfica para Clean Rooms, no todas las operaciones SQL generan resultados válidos. Por ejemplo, puede realizar una operación COUNT en una columna cifrada, pero realizar una operación SUM en números cifrados generará errores. Además, las consultas también pueden arrojar resultados incorrectos. Por ejemplo, las consultas SUM de columnas selladas producen errores. Sin embargo, una consulta GROUP BY en columnas selladas parece ejecutarse correctamente, pero produce grupos diferentes a los que genera una consulta GROUP BY en texto sin formato.

En los siguientes temas se explica cómo consultar datos en una colaboración mediante la consola de AWS Clean Rooms .

Temas

- Usar el editor de código SQL

- Usar el creador de análisis
- Consulta de datos con privacidad diferencial
- Vista de consultas recientes
- Visualización de detalles de consultas

Para obtener información sobre cómo consultar datos o ver consultas llamando directamente a la operación de la AWS Clean Rooms `StartProtectedQuery` API o mediante los AWS SDK, consulta la referencia de la AWS Clean Rooms API.

Para obtener más información sobre el registro de consultas, consulte Inicio de sesión de consultas AWS Clean Rooms.

> **Note**
>
> Si ejecuta una consulta en tablas de datos cifrados, los resultados de las columnas cifradas se cifran.

Para obtener información acerca de recibir resultados de consultas, consulte Recibir resultados de consultas.

Usar el editor de código SQL

Como miembro que puede realizar consultas, puede crear una consulta manualmente escribiendo código SQL en el editor de código SQL. El editor de código SQL se encuentra en la sección Análisis de la pestaña Consultas de la AWS Clean Rooms consola.

El editor de código SQL se muestra de forma predeterminada. Si desea usar el creador de análisis para crear consultas, consulteUsar el creador de análisis.

> **Important**
>
> Si empieza a escribir una consulta SQL en el editor de código y luego activa la interfaz de usuario del creador de análisis, la consulta no se guarda.

AWS Clean Rooms admite muchos comandos, funciones y condiciones de SQL. Para obtener más información, consulte la Referencia de SQL de AWS Clean Rooms.

> **Tip**
>
> Si se lleva a cabo un mantenimiento programado mientras se está ejecutando una consulta, esta se termina y se revierte. Deberá reiniciar la consulta.

Para crear la consulta manualmente con el editor de código SQL

1. Inicie sesión en AWS Management Console y abra la AWS Clean Rooms consola con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración cuyo estado de Sus capacidades como miembro sea Consultar.
4. En la pestaña Consultas, vaya a la sección Análisis.

   > **Note**
   >
   > La sección Análisis solo se muestra si el miembro que puede recibir los resultados y el miembro responsable de pagar los costos de computación de las consultas se han unido a la colaboración como miembros activos.

5. En la pestaña Consultas, en Tablas, consulte la lista de tablas y su tipo de regla de análisis asociado (regla de análisis de agregación, regla de análisis de lista o regla de análisis personalizada).

   > **Note**
   >
   > Si no ve las tablas que esperaba en la lista, puede deberse a los siguientes motivos:
   >
   > - Las tablas no se han asociado.
   > - Las tablas no tienen una regla de análisis configurada.

6. (Opcional) Para ver el esquema de la tabla y los controles de las reglas de análisis, amplíe la tabla seleccionando el icono del signo más (+).
7. Cree la consulta escribiéndola en el editor de código SQL.

(Opcional) Si desea utilizar una consulta de ejemplo	(Opcional) Si desea insertar nombres de columnas o funciones
1. Elija los tres puntos verticales que aparecen junto al nombre de la tabla. 2. En Insertar en el editor, elija Consulta de ejemplo. **Note** Insertar una Consulta de ejemplo anexa la consulta que ya está en el editor. Aparece el ejemplo de consulta. Todas las tablas que aparecen en Tablas se incluyen en la consulta. 3. Edite los valores de marcadores de posición de la consulta.	1. Seleccione los tres puntos verticales situados junto a una columna. 2. En Insertar en el editor, elija Nombre de columna. 3. Para insertar manualmente una función permitida en una columna, seleccione los tres puntos verticales situados junto a la columna, seleccione Insertar en el editor y, a continuación, seleccione el nombre de la función permitida (por ejemplo INNER JOIN, SUM, SUM DISTINCT o COUNT). 4. Pulse Ctrl + Espacio para ver los esquemas de la tabla en el editor de código. **Note** Los miembros que pueden realizar consultas pueden ver y usar las columnas de partición de cada asociación de tablas configuradas. Asegúrese de que la columna de particiones esté etiquetada como columna de particiones

(Opcional) Si desea utilizar una consulta de ejemplo	(Opcional) Si desea insertar nombres de columnas o funciones
	en la AWS Glue tabla subyacente a la tabla configurada. 5. Edite los valores de marcadores de posición de la consulta.

8. Elija Ejecutar.

> **Note**
>
> No podrá ejecutar la consulta si el miembro que puede recibir los resultados no ha configurado los ajustes de resultados de consulta.

9. Siga ajustando los parámetros y vuelva a ejecutar la consulta, o pulse el botón + para iniciar una nueva consulta en una pestaña nueva.

> **Note**
>
> AWS Clean Rooms tiene como objetivo proporcionar mensajes de error claros. Si un mensaje de error no contiene detalles suficientes para ayudarle a solucionar el problema, póngase en contacto con el equipo de cuentas. Proporcióneles una descripción de cómo se produjo el error y el mensaje de error (incluidos los identificadores). Para obtener más información, consulte Solución de problemas AWS Clean Rooms.

Usar el creador de análisis

Puede usar el creador de análisis para crear consultas sin tener que escribir código SQL. Con el creador de análisis, puede crear una consulta para una colaboración que tenga:

- Una sola tabla que utilice la regla de análisis de agregación sin necesidad de usar JOIN
- Dos tablas (una de cada miembro) que utilicen la regla de análisis de agregación
- Dos tablas (una de cada miembro) que utilicen la regla de análisis de lista

- Dos tablas (una de cada miembro) que utilicen la regla de análisis de agregación y dos tablas (una de cada miembro) que utilicen la regla de análisis de lista

Si desea escribir consultas SQL manualmente, consulte Usar el editor de código SQL.

El creador de análisis aparece como la opción Interfaz de usuario del creador de análisis en la sección Análisis de la pestaña Consultas de la consola de AWS Clean Rooms .

> **Important**
>
> Si activa Interfaz de usuario del creador de análisis, comienza a crear una consulta en el creador de análisis y, a continuación, desactiva la Interfaz de usuario del creador de análisis, la consulta no se guarda.

> **Tip**
>
> Si se lleva a cabo un mantenimiento programado mientras se está ejecutando una consulta, esta se termina y se revierte. Deberá reiniciar la consulta.

En los siguientes temas se explica cómo utilizar el creador de análisis.

Temas

- Uso del creador de análisis para consultar una sola tabla (agregación)
- Uso del creador de análisis para consultar dos tablas (agregación o lista)

Uso del creador de análisis para consultar una sola tabla (agregación)

Este procedimiento muestra cómo utilizar la interfaz de usuario de Analysis Builder en la AWS Clean Rooms consola para crear una consulta. La consulta se refiere a una colaboración que tiene una sola tabla que utiliza la regla de análisis de agregación sin necesidad de JOIN.

Para usar el creador de análisis para consultar una sola tabla

1. Inicie sesión en la AWS Clean Rooms consola AWS Management Console y ábrala con la suya Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.

3. Elija la colaboración cuyo estado de Sus capacidades como miembro sea Consultar.
4. En la pestaña Consultas, en Tablas, consulte la tabla y su tipo de regla de análisis asociada (el tipo de regla de análisis debe ser Regla de análisis de agregación).

> **Note**
>
> Si no ve la tabla que esperaba, puede deberse a los siguientes motivos:
>
> - La tabla no se ha asociado.
> - La tabla no tiene una regla de análisis configurada.

5. En la sección Análisis, active la Interfaz de usuario del creador de análisis.
6. Cree una consulta.

   Si desea ver todas las métricas de agregación, vaya al paso 9.

   a. En Elegir métricas, revise las métricas agregadas que se han preseleccionado de forma predeterminada y elimine cualquier métrica si es necesario.

   b. (Opcional) En Añadir segmentos: opcional, elija uno o varios parámetros.

   > **Note**
   >
   > Añadir segmentos: opcional solo se muestra si se especifican las dimensiones para la tabla.

   c. (Opcional) En Añadir filtros: opcional, elija Añadir filtro y, a continuación, elija un Parámetro, un operador y un Valor.

   Para añadir más filtros, elija Añadir otro filtro.

   Para eliminar un filtro, elija Eliminar.

   > **Note**
   >
   > ORDER BY no se admite en las consultas de agregación.
   > En los filtros, solo se admite el operador AND.

   d. (Opcional) En Añadir descripción: opcional, introduzca una descripción que ayude a identificar la consulta en la lista de consultas.

7. Amplíe Vista previa del código SQL.

   a. Vea el código SQL que se genera a partir del creador de análisis.

   b. Para copiar el código SQL, elija Copiar.

   c. Para editar el código SQL, elija Editar en el editor de código SQL.

8. Elija Ejecutar.

> **Note**
>
> No podrá ejecutar la consulta si el miembro que puede recibir los resultados no ha configurado los ajustes de resultados de consulta.

9. Siga ajustando los parámetros y vuelva a ejecutar la consulta, o pulse el botón + para iniciar una nueva consulta en una pestaña nueva.

> **Note**
>
> AWS Clean Rooms tiene como objetivo proporcionar mensajes de error claros. Si un mensaje de error no contiene detalles suficientes para ayudarle a solucionar el problema, póngase en contacto con el equipo de cuentas. Proporcióneles una descripción de cómo se produjo el error y el mensaje de error (incluidos los identificadores). Para obtener más información, consulte Solución de problemas AWS Clean Rooms.

Uso del creador de análisis para consultar dos tablas (agregación o lista)

Este procedimiento describe cómo utilizar el generador de análisis de la AWS Clean Rooms consola para crear una consulta para una colaboración que tenga:

- Dos tablas (una de cada miembro) que utilicen la regla de análisis de agregación
- Dos tablas (una de cada miembro) que utilicen la regla de análisis de lista
- Dos tablas (una de cada miembro) que utilicen la regla de análisis de agregación y dos tablas (una de cada miembro) que utilicen la regla de análisis de lista

Para usar el creador de análisis para consultar dos tablas

1. Inicie sesión en la AWS Clean Rooms consola AWS Management Console y ábrala con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración cuyo estado de Sus capacidades como miembro sea Consultar.
4. En la pestaña Consultas, en Tablas, consulte las dos tablas y su tipo de regla de análisis asociada (Regla de análisis de agregación o Regla de análisis de lista).

> **Note**
>
> Si no ve las tablas que espera en la lista, puede deberse a los siguientes motivos:
>
> - Las tablas no se han asociado.
> - Las tablas no tienen una regla de análisis configurada.

5. En la sección Análisis, active la Interfaz de usuario del creador de análisis.
6. Cree una consulta.

   Si la colaboración contiene dos tablas que utilizan la Regla de análisis de agregación y dos tablas que utilizan la Regla de análisis de lista, elija primero Agregación o Lista y, a continuación, siga las instrucciones según la regla de análisis seleccionada.

Si las dos tablas utilizan la regla de análisis de agregación	Si las dos tablas utilizan la regla de análisis de lista
1. En Elegir métricas, revise las métricas agregadas que se han preseleccionado de forma predeterminada y elimine cualquier métrica si es necesario. 2. En Registros de coincidencia, elija uno o más registros.	1. En Elegir atributos, revise la lista de atributos que se han preseleccionado de forma predeterminada y elimine cualquier métrica si es necesario. 2. En Registros de coincidencia, elija uno o más registros.

Si las dos tablas utilizan la regla de análisis de agregación	Si las dos tablas utilizan la regla de análisis de lista
Note Al utilizar el creador de análisis, solo puede hacer coincidir un único par de columnas.	**Note** Al utilizar el creador de análisis, solo puede hacer coincidir un único par de columnas.
3. (Opcional) En Añadir segmentos: opcional, elija uno o varios parámetros.	3. (Opcional) En Añadir filtros: opcional, elija Añadir filtro y, a continuación, elija un parámetro, un operador y un valor. Para añadir más filtros, elija Añadir otro filtro. Para eliminar un filtro, elija Eliminar.
Note Añadir segmentos : opcional solo se muestra si se especific an las dimensiones para la tabla.	**Note** Las consultas de lista no admiten LIMIT. En los filtros, solo se admite el operador AND.
4. (Opcional) En Añadir filtros: opcional, elija Añadir filtro y, a continuación, elija un parámetro , un operador y un valor. Para añadir más filtros, elija Añadir otro filtro. Para eliminar un filtro, elija Eliminar.	4. (Opcional) En Añadir descripci ón: opcional, introduzca una descripción que ayude a identificar la consulta en la lista de consultas recientes.
Note ORDER BY no se admite en las consultas de agregación.	

Si las dos tablas utilizan la regla de análisis de agregación	Si las dos tablas utilizan la regla de análisis de lista
En los filtros, solo se admite el operador AND. 5. (Opcional) En Añadir descripción: opcional, introduzca una descripción que ayude a identificar la consulta en la lista de consultas recientes.	

7. Amplíe Vista previa del código SQL.

   a. Vea el código SQL que se genera a partir del creador de análisis.

   b. Para copiar el código SQL, elija Copiar.

   c. Para editar el código SQL, elija Editar en el editor de código SQL.

8. Elija Ejecutar.

> **Note**
>
> No podrá ejecutar la consulta si el miembro que puede recibir los resultados no ha configurado los ajustes de resultados de consulta.

9. Siga ajustando los parámetros y vuelva a ejecutar la consulta, o pulse el botón + para iniciar una nueva consulta en una pestaña nueva.

> **Note**
>
> AWS Clean Rooms tiene como objetivo proporcionar mensajes de error claros. Si un mensaje de error no contiene detalles suficientes para ayudarle a solucionar el problema, póngase en contacto con el equipo de cuentas. Proporcióneles una descripción de cómo se produjo el error y el mensaje de error (incluidos los identificadores). Para obtener más información, consulte Solución de problemas AWS Clean Rooms.

Consulta de datos con privacidad diferencial

En general, la escritura y la ejecución de consultas no cambian cuando se activa la privacidad diferencial. Sin embargo, no puede ejecutar una consulta si no queda suficiente presupuesto de privacidad. A medida que ejecuta consultas y consume el presupuesto de privacidad, puede ver aproximadamente cuántas agregaciones puede ejecutar y cómo podrían afectar a las consultas futuras.

Para ver el impacto de la privacidad diferencial en una colaboración

1. Inicie sesión AWS Management Console y abra la AWS Clean Rooms consola con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración cuyo estado de Sus detalles de miembro sea Ejecutar consultas.
4. En la pestaña Consultas, en Tablas, vea el presupuesto de privacidad restante. Se muestra como el número estimado de funciones de agregación restantes y la utilidad utilizada (representada como porcentaje).

   > **Note**
   >
   > El número estimado de funciones de agregación restantes y el porcentaje de la utilidad utilizada solo muestran para el miembro que puede realizar la consulta.

5. Seleccione Ver impacto para ver cuánto ruido se inyecta en los resultados y aproximadamente cuántas funciones de agregación puede ejecutar.

Vista de consultas recientes

Puede ver las consultas que se han ejecutado en los últimos 90 días en la pestaña Consultas recientes.

> **Note**
>
> Si su única capacidad como miembro es Contribuir con datos y no es el miembro que paga los costos de computación de consultas, la pestaña Consultas no aparecerá en la consola.

Para ver consultas recientes

1. Inicia sesión en la AWS Clean Rooms consola AWS Management Console y ábrela con la tuya Cuenta de AWS (si aún no lo has hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija una colaboración.
4. En la pestaña Consultas, en Consultas, vea las consultas que se han ejecutado en los últimos 90 días.
5. Para ordenar las consultas recientes por Estado, seleccione un estado en la lista desplegable Todos los estados.

   Los estados son: Enviada, Iniciada, Cancelada, Éxito, Error y Agotado tiempo de espera.

Visualización de detalles de consultas

Puede ver los detalles de la consulta como miembro que puede realizar consultas o como miembro que puede recibir los resultados.

Para ver los detalles de la consulta

1. Inicia sesión en la AWS Clean Rooms consola AWS Management Console y ábrela con la tuya Cuenta de AWS (si aún no lo has hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija una colaboración.
4. En la pestaña Consultas, realice una de las siguientes acciones:
   - Elija el botón de opción correspondiente a la consulta específica que desea ver y, a continuación, elija Ver detalles.
   - Elija el ID de consulta protegida.
5. En la página de Detalles de la consulta,
   - Si es el miembro que puede realizar consultas, vea los Detalles de la consulta, el Texto SQL y los Resultados.

     Ve un mensaje que confirma que los resultados de la consulta se entregaron al miembro que puede recibir los resultados.

- Si usted es el miembro que puede recibir los resultados, vea los Detalles de la consulta y los Resultados.

Recibir resultados de consultas

Como miembro que puede recibir resultados, puede recibir el resultado de la consulta desde AWS Clean Rooms en el bucket de Amazon S3 que haya especificado al unirse a la colaboración.

En los siguientes temas se explica cómo recibir resultados de consultas mediante la consola de AWS Clean Rooms.

Temas

- Recepción de resultados de consultas
- Edición de los ajustes predeterminados de los resultados de las consultas
- Usar el resultado de la consulta en otros Servicios de AWS

Para obtener información sobre cómo consultar datos o ver consultas llamando a la API de AWS Clean Rooms directamente o utilizando los SDK de AWS, consulte la Referencia de API de AWS Clean Rooms.

Para obtener más información sobre el registro de consultas, consulte Inicio de sesión de consultas AWS Clean Rooms.

> **Note**
>
> Si ejecuta una consulta en tablas de datos cifrados, los resultados de las columnas cifradas se cifran.

Recepción de resultados de consultas

Los resultados de la consulta se encuentran en la sección Ajustes predeterminados de resultados de consultas y en la sección Consultas de la pestaña Consultas de la consola de AWS Clean Rooms.

Para recibir resultados de consultas

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.

3. Elija la colaboración cuyo estado de Sus capacidades como miembro sea Recibir resultados.
4. Para recibir los resultados de las consulta directamente de AWS Clean Rooms, en la pestaña Consultas, en Consultas, en la columna ID de consulta protegida, seleccione la consulta.
5. En la página Detalles de la consulta, en Resultados, realice una de las siguientes acciones:

Si desea...	Entonces elija...
Copiar los resultados.	Copiar
Descargar los resultados.	Descargar **Note** De forma predeterminada, el nombre del archivo descargado es el `Query id` correspondiente que se mostró cuando al ejecutar la consulta en AWS Clean Rooms.
Consulte los resultados en Amazon S3.	Ver en Amazon S3 Se abre la consola de Amazon S3 en una pestaña aparte.

6. Si utiliza datos cifrados, ahora puede descifrar las tablas de datos.

   Para obtener más información, consulte Descifrar tablas de datos con el cliente de cifrado de C3R.

Edición de los ajustes predeterminados de los resultados de las consultas

Como miembro que puede recibir resultados, puede editar los ajustes predeterminados de los resultados de las consultas en la consola de AWS Clean Rooms.

Para editar los ajustes predeterminados de los resultados de las consultas

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración cuyo estado de Sus capacidades como miembro sea Recibir resultados.
4. En la pestaña Consultas, en Configuración de resultados de la consulta, seleccione Editar.
5. En la página Editar ajustes predeterminados de los resultados de las consultas, modifique cualquiera de las siguientes opciones según proceda:

   a. En Ajustes de los resultados de consultas, modifique el Destino de los resultados en Amazon S3 o el Formato de los resultados.
   b. En Acceso al servicio, modifique el Método para autorizar a AWS Clean Rooms para escribir en el bucket de Amazon S3 y en el formato que haya especificado.

   Los Ajustes de los resultados de las consultas aparecen en la página de detalles de la colaboración.

Usar el resultado de la consulta en otros Servicios de AWS

El resultado de la consulta de AWS Clean Rooms está disponible en la consola (si la consola se utiliza para ejecutar consultas) y se descarga en un bucket de Amazon S3 especificado. A partir de ahí, puede utilizar el resultado de la consulta en otros Servicios de AWS, como Amazon QuickSight y Amazon SageMaker, dependiendo de cómo esos servicios hagan uso de los datos de Amazon S3.

Para obtener más información sobre Amazon QuickSight, consulte la Documentación de Amazon QuickSight.

Para obtener más información acerca de Amazon SageMaker, consulte la Documentación de Amazon SageMaker.

Descifrar tablas de datos con el cliente de cifrado de C3R

Siga este procedimiento para las colaboraciones que utilizan la computación criptográfica para Clean Rooms y el cliente de cifrado de C3R para cifrar tablas de datos. Utilice este procedimiento después de haber consultado datos de la colaboración.

La clave secreta compartida y el ID de colaboración son necesarios para este procedimiento.

El miembro que puede recibir los resultados descifra los datos con la misma clave secreta compartida y el mismo ID de colaboración que se utilizaron para cifrar los datos de la colaboración.

> **Note**
>
> Las colaboraciones de AWS Clean Rooms ya imponen límites en cuanto a quién puede realizar consultas y ver sus resultados. Para realizar el descifrado, quien tenga acceso a estos resultados necesita la misma clave secreta compartida y el mismo ID de colaboración que se utilizaron para cifrar los datos.

Para descifrar una tabla de datos cifrada

1. (Opcional) Consulte los comandos disponibles en el cliente de cifrado de C3R.
2. (Opcional) Desplácese hasta el directorio deseado y ejecute `ls` (macOS) o `dir` (Windows).
   - Compruebe que el archivo c3r-cli.jar y el archivo de datos de resultados de la consulta cifrados están en el directorio deseado.

     > **Note**
     >
     > Si los resultados de la consulta se descargan desde la interfaz de la consola de AWS Clean Rooms, es probable que se encuentren en la carpeta Descargas de su cuenta de usuario (por ejemplo, la carpeta Descargas de su directorio de usuario en Windows y macOS). Se recomienda mover el archivo de resultados de la consulta a la misma carpeta que el c3r-cli.jar.
3. Guarde la clave secreta compartida en la variable de entorno `C3R_SHARED_SECRET`. Para obtener más información, consulte Paso 6: guardar la clave secreta compartida en la variable de entorno.

4. Desde la AWS Command Line Interface (AWS CLI), ejecute el siguiente comando.

   java -jar c3r-cli.jar decrypt ***<name of input .csv file>*** --id=***<collaboration id>*** --output=***<output file name>***

5. Reemplace cada *marcador de posición de entrada del usuario* con su propia información.

   a. En `id=`, introduzca el ID de la colaboración.

   b. En `output=`, introduzca el nombre del archivo de salida (por ejemplo, `results-decrypted.csv`).

      Si no especifica un nombre de salida, se mostrará un nombre predeterminado en el terminal.

   c. Vea los datos descifrados del archivo de salida especificado utilizando la aplicación de visualización de CSV o Parquet de su preferencia (como Microsoft Excel, un editor de texto u otra aplicación).

Administrar AWS Clean Rooms

En los siguientes temas se describe cómo gestionar una colaboración, los miembros y las tablas configuradas AWS Clean Rooms mediante la AWS Clean Rooms consola.

Para obtener información sobre cómo administrar el AWS Clean Rooms uso de los AWS SDK, consulta la referencia de la AWS Clean Rooms API.

Temas

- Administrar colaboraciones en AWS Clean Rooms
- Administrar tablas configuradas en AWS Clean Rooms

Administrar colaboraciones en AWS Clean Rooms

En los siguientes temas se describe cómo el creador de una colaboración puede administrar la colaboración en AWS Clean Rooms mediante la consola de AWS Clean Rooms.

Para obtener información sobre cómo administrar una colaboración con los SDK de AWS, consulte la Referencia de API de AWS Clean Rooms.

Temas

- Editar colaboraciones
- Eliminar colaboraciones
- Ver colaboraciones
- Ver tablas y reglas de análisis
- Visualización de los registros de uso de la privacidad diferencial
- Monitorización del estado de los miembros
- Eliminar un miembro de una colaboración
- Abandonar una colaboración
- Editar asociaciones de tablas configuradas
- Disociar tablas configuradas
- Edición de una política de privacidad diferencial

- Eliminación de una política de privacidad diferencial
- Visualización de los parámetros de privacidad diferencial calculados

Editar colaboraciones

Aprenda a editar las distintas partes de una colaboración.

Temas

- Edición del nombre y la descripción de la colaboración
- Editar etiquetas de colaboración
- Edición de etiquetas de pertenencia
- Editar las etiquetas de tablas asociadas
- Edición de etiquetas de plantilla de análisis
- Edición de las etiquetas de la política de privacidad diferencial

Edición del nombre y la descripción de la colaboración

Una vez creada una colaboración, solo su nombre y descripción serán editables.

> **Note**
>
> Si ha habilitado el Registro de consultas, puede editar si los registros de consultas se almacenan en su cuenta de Registros de Amazon CloudWatch.

Para editar el nombre y la descripción de la colaboración

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración que ha creado.
4. En la página de detalles de la colaboración, elija Acciones y, a continuación, elija Editar colaboración.
5. En Detalles, edite el Nombre y la Descripción de la colaboración.

6. Elija Guardar cambios.

Editar etiquetas de colaboración

Como creador de la colaboración, una vez creada una colaboración, puede administrar las etiquetas del recurso de colaboración.

Para editar las etiquetas de la colaboración

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración que ha creado.
4. Seleccione una de las siguientes opciones:

Si usted es...	Entonces...
Un miembro de la colaboración	Elija la pestaña Detalles.
El creador de la colaboración, pero no un miembro de la colaboración	Desplácese hacia abajo por la página hasta la sección Etiquetas.

5. Para ver los Detalles de la colaboración, elija Administrar etiquetas.
6. En la página Administrar etiquetas, puede hacer lo siguiente:

   - Para eliminar una etiqueta, elija Eliminar.
   - Para añadir una etiqueta, elija Añadir nueva etiqueta.
   - Para guardar los cambios, elija Guardar cambios.

Edición de etiquetas de pertenencia

Como creador de colaboraciones, una vez que haya creado una colaboración, puede administrar las etiquetas del recurso de pertenencia.

Para editar las etiquetas de pertenencia

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).

2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración que ha creado.
4. Elija la pestaña Detalles.
5. En Detalles de pertenencia, elija Administrar etiquetas.
6. En la página Administrar etiquetas de pertenencia, puede hacer lo siguiente:

   - Para eliminar una etiqueta, elija Eliminar.
   - Para añadir una etiqueta, elija Añadir nueva etiqueta.
   - Para guardar los cambios, elija Guardar cambios.

Editar las etiquetas de tablas asociadas

Como creador de la colaboración, después de asociar tablas a una colaboración, puede administrar las etiquetas del recurso de tabla asociado.

Para editar las etiquetas de tabla asociadas

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración que ha creado.
4. Seleccione la pestaña Tablas.
5. En Tablas asociadas por usted, elija una tabla.
6. En la página de detalles de la tabla configurada, en Etiquetas, elija Administrar etiquetas.

   En la página Administrar etiquetas, puede hacer lo siguiente:

   - Para eliminar una etiqueta, elija Eliminar.
   - Para añadir una etiqueta, elija Añadir nueva etiqueta.
   - Para guardar los cambios, elija Guardar cambios.

Edición de etiquetas de plantilla de análisis

Como creador de la colaboración, una vez creada una colaboración, puede administrar las etiquetas del recurso de plantilla de análisis.

Para editar las etiquetas de pertenencia

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración que ha creado.
4. Elija la pestaña Plantillas.
5. En la sección Plantillas de análisis creadas por usted, elija la plantilla de análisis.
6. En la página de detalles de la tabla de plantillas de análisis, desplácese hacia abajo hasta la sección Etiquetas.
7. Elija Administrar etiquetas.
8. En la página Administrar etiquetas, puede hacer lo siguiente:
   - Para eliminar una etiqueta, elija Eliminar.
   - Para añadir una etiqueta, elija Añadir nueva etiqueta.
   - Para guardar los cambios, elija Guardar cambios.

Edición de las etiquetas de la política de privacidad diferencial

Como creador de la colaboración, una vez creada una colaboración, puede administrar las etiquetas del recurso de plantilla de análisis.

Para editar las etiquetas de pertenencia

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración que contiene la política de privacidad diferencial que desea editar.
4. Seleccione la pestaña Tablas.
5. En la pestaña Etiquetas, elija Administrar etiquetas.
6. En la página Administrar etiquetas, puede hacer lo siguiente:
   - Para eliminar una etiqueta, elija Eliminar.
   - Para añadir una etiqueta, elija Añadir nueva etiqueta.

- Para guardar los cambios, elija Guardar cambios.

Eliminar colaboraciones

Como creador de la colaboración, puede eliminar una colaboración que haya creado.

> **Note**
>
> Al eliminar una colaboración, ni usted ni el resto de miembros pueden realizar consultas, recibir resultados o aportar datos. Cada miembro de la colaboración sigue teniendo acceso a sus propios datos como parte de su pertenencia.

Para eliminar una colaboración

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración que desea eliminar.
4. En Acciones, selecciona Eliminar colaboración.
5. Confirme la eliminación y luego elija Eliminar.

Ver colaboraciones

Como creador de la colaboración, puede ver todas las colaboraciones que ha creado.

Para ver colaboraciones

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. En la página Colaboraciones, en Usadas por última vez, consulte las últimas 5 colaboraciones utilizadas.
4. En la pestaña Con pertenencia activa, consulte la lista de colaboraciones con pertenencia activa.

   Puede ordenar por Nombre, Fecha de creación de la pertenencia y Sus detalles de miembro.

Puede utilizar la barra de búsqueda para buscar una colaboración.

5. En la pestaña Disponibles para unirse, consulte la lista de Colaboraciones disponibles para unirse.
6. En la pestaña Ya no están disponibles, consulte la lista de colaboraciones eliminadas y Pertenencias a colaboraciones que ya no están disponibles (pertenencias eliminadas).

Ver tablas y reglas de análisis

Para ver las tablas asociadas a la colaboración y a las reglas de análisis

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. Seleccione la pestaña Tablas.
5. Seleccione una de las siguientes opciones:
    a. Para ver las tablas asociadas a la colaboración, en Tablas asociadas por usted, elija una tabla (texto azul).
    b. Para ver otras tablas asociadas a la colaboración, en Tablas asociadas por colaboradores, elija una tabla (texto azul).
6. Vea los detalles de la tabla y las reglas de análisis en la página de detalles de la tabla.

Visualización de los registros de uso de la privacidad diferencial

Como miembro de una colaboración que protege los datos con privacidad diferencial, después de haber creado una colaboración con privacidad diferencial, puede supervisar el uso del presupuesto de privacidad.

Para ver cuántas agregaciones se ejecutaron y qué parte del presupuesto de privacidad se utilizó

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.

3. Seleccione la colaboración.
4. Seleccione la pestaña Tablas.
5. Seleccione Ver registros de uso (texto azul).
6. Consulte los detalles de uso, incluido el presupuesto de privacidad y cuánta utilidad se ha proporcionado.

Monitorización del estado de los miembros

Como creador de una colaboración, una vez creada la colaboración, puede monitorizar el estado de todos los miembros en la pestaña Miembros.

Para comprobar el estado de un miembro

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración que ha creado.
4. Seleccione la pestaña Miembros.
5. Vea el Estado de miembro de cada miembro.

Eliminar un miembro de una colaboración

> **Note**
>
> Al eliminar a un miembro, también se eliminan todos sus conjuntos de datos asociados de la colaboración.

Para eliminar un miembro de una colaboración

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Elija la colaboración que ha creado.

4. Seleccione la pestaña Miembros.
5. Seleccione el botón de opción situado junto al miembro que desea eliminar.

> **Note**
>
> El creador de una colaboración no puede elegir su propio ID de cuenta.

6. Elija Eliminar.
7. En el cuadro de diálogo, confirme la decisión de eliminar al miembro escribiendo **`confirm`** en el campo de entrada de texto.

> **Note**
>
> Si elimina al miembro que paga los costos de computación de consultas, no se permite ejecutar más consultas en la colaboración.

Abandonar una colaboración

Como miembro de una colaboración, puede abandonar una colaboración eliminando tu pertenencia. Si es el creador de la colaboración, solo puede abandonarla si elimina la colaboración.

> **Note**
>
> Al eliminar su pertenencia, abandonará la colaboración y no podrá volver a unirse a ella. Si es el miembro que paga los costos de computación de consultas y elimina su pertenencia, no se permite que se ejecuten más consultas.

Para abandonar una colaboración

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. En Con pertenencia activa, elija la colaboración de la que es miembro.
4. Elija Acciones.
5. Seleccione Eliminar pertenencia.

6. En el cuadro de diálogo, confirme la decisión de abandonar la colaboración escribiendo **`confirm`** en el campo de entrada de texto y, a continuación, seleccione Vaciar y eliminar pertenencia.

   En la consola, verá un mensaje que indica que se ha eliminado la pertenencia.

   El creador de la colaboración ve el Estado de miembro como Abandonado.

Editar asociaciones de tablas configuradas

Como miembro de una colaboración, puede editar las asociaciones de tablas configuradas que ha creado.

Para editar asociaciones de tablas configuradas

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. Seleccione la pestaña Tablas.
5. En Tablas asociadas por usted, elija una tabla.
6. En la página de detalles de la tabla, desplácese hacia abajo para ver los Detalles de asociación de tablas.
7. Elija Editar.
8. En la página Editar asociaciones de tablas configuradas, actualice la Descripción o la Información de acceso al servicio.
9. Elija Guardar cambios.

Disociar tablas configuradas

Como miembro de la colaboración, puede disociar una tabla configurada de la colaboración. Esta acción impide que el miembro que puede realizar consultas consulte la tabla.

Para disociar una tabla configurada

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. Seleccione la pestaña Tablas.
5. En Tablas asociadas por usted, elija el botón de opción situado junto a la tabla que desea disociar.
6. Elija Disociar.
7. En el cuadro de diálogo, confirme la decisión de disociar la tabla configurada, y seleccione Disociar para impedir que el miembro que puede realizar consultas consulte la tabla.

Edición de una política de privacidad diferencial

Después de configurar la política de privacidad diferencial, puede actualizarla en cualquier momento para que refleje mejor sus necesidades de privacidad.

Para editar la política de privacidad diferencial

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. En la pestaña Tablas de la página de colaboración, en Tablas asociadas por usted, elija Editar.
5. En la página Editar privacidad diferencial, elija nuevos valores para las siguientes propiedades:

   - Presupuesto de privacidad: mueva la barra del control deslizante para aumentar o disminuir el presupuesto en cualquier momento de una colaboración. No puede reducir el presupuesto después de que el miembro que puede realizar la consulta haya empezado a consultar sus datos. Si se aumenta el Presupuesto de privacidad, AWS Clean Rooms seguirá utilizando el presupuesto existente hasta que se agote por completo antes de utilizar el presupuesto de privacidad recién agregado.
   - Ruido añadido por consulta: mueva la barra de control deslizante para aumentar o disminuir el ruido añadido por consulta en cualquier momento durante una colaboración.

> **Note**
>
> Puedes elegir ejemplos interactivos para ver cómo los distintos valores del Presupuesto de privacidad y Ruido añadido por consulta afectan al número de funciones agregadas que puede ejecutar.

No se puede cambiar el valor de la Actualización del presupuesto de privacidad. Para cambiar su selección, debe eliminar la política de privacidad diferencial y crear una nueva.

6. Elija Guardar cambios.

Aparece un mensaje de confirmación en el que se indica que ha editado correctamente la política de privacidad diferencial.

Eliminación de una política de privacidad diferencial

Puede eliminar la política de privacidad diferencial desde la pestaña Tablas de una colaboración.

Para eliminar la política de privacidad diferencial:

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. En la pestaña Tablas de la página de colaboración, junto a la Política de privacidad diferencial, seleccione Eliminar.
5. Si tiene la certeza de que desea eliminar la política de privacidad diferencial, seleccione Eliminar.

Tras eliminar una política de privacidad diferencial, no podrá acceder a los registros de uso del presupuesto de privacidad de esa política. Las tablas con la privacidad diferencial activada no se pueden consultar si se elimina la política de privacidad diferencial.

Visualización de los parámetros de privacidad diferencial calculados

Los usuarios con experiencia en privacidad diferencial pueden ver los parámetros de privacidad diferencial calculados en la pestaña Consultas de una colaboración.

Para ver los parámetros de privacidad diferencial calculados

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Clean Rooms con su Cuenta de AWS (si aún no lo ha hecho).
2. En el panel de navegación izquierdo, elija Colaboraciones.
3. Seleccione la colaboración.
4. En la pestaña Consultas, en la sección Resultados, seleccione Ver los parámetros de privacidad diferencial calculados.

En la tabla Parámetros de privacidad diferencial calculados, puede ver los valores de confidencialidad de las funciones agregadas, que se definen como la cantidad máxima en la que el resultado de una función puede cambiar si se añaden, eliminan o modifican los registros de un solo usuario. La lista incluye los siguientes parámetros de privacidad diferencial:

- El límite de contribución del usuario (UCL) es el número máximo de filas que aporta un usuario en una consulta SQL. Por ejemplo, si quiere contar el número total de impresiones coincidentes en una campaña específica en la que cada usuario puede tener varias impresiones, la privacidad diferencial de AWS Clean Rooms debe limitar el número de impresiones de un solo usuario para garantizar que el cálculo de la privacidad diferencial sea preciso. En otras palabras, si algún usuario tiene más impresiones que el límite, AWS Clean Rooms efectúa automáticamente una muestra aleatoria uniforme de las impresiones de ese usuario según el valor de UCL calculado y excluye las impresiones restantes de ese usuario al ejecutar la consulta. El valor de la UCL es igual a 1 si se cuenta el número de usuarios únicos. Esto se debe a que la adición, eliminación o modificación de un solo usuario puede cambiar el recuento de usuarios distintos en 1 como máximo.
- El valor mínimo es el límite inferior de una expresión que se utiliza en una función de agregación, como `sum()`. Por ejemplo, si la expresión es una columna denominada `purchase_value`, el valor mínimo es el límite inferior de la columna.
- El valor máximo es el límite superior de una expresión que se utiliza en una función de agregación, como `sum()`. Por ejemplo, si la expresión es una columna denominada `purchase_value`, el valor máximo es el límite superior de la columna.

En la tabla Parámetros de privacidad diferencial calculados, puede utilizar estos parámetros para comprender mejor la cantidad total de ruido en los resultados de las consultas. Por ejemplo, cuando el ruido añadido por consulta es de 30 usuarios y se ejecuta una consulta `COUNT DISTINCT (user_id)`, la privacidad diferencial de AWS Clean Rooms añade ruido aleatorio que se encuentra entre -30 y 30 con una alta probabilidad porque la sensibilidad de `COUNT DISTINCT` es 1. En el caso de una consulta `COUNT` con la misma configuración, la privacidad diferencial de AWS Clean Rooms añade ruido estadístico que se escala según el límite de contribución del usuario, ya que un solo usuario podría añadir varias filas al resultado de la consulta. En el caso de una consulta `SUM` como `SUM (purchase_value)`, donde todos los valores de las columnas son positivos, el ruido total se escala en función del límite de contribución del usuario multiplicado por el valor máximo. AWS Clean Rooms La privacidad diferencial calcula automáticamente los parámetros de sensibilidad para añadir ruido en el tiempo de ejecución de la consulta y agota el presupuesto de privacidad. Es necesario reducir el presupuesto de privacidad porque los parámetros de sensibilidad dependen de los datos.

Administrar tablas configuradas en AWS Clean Rooms

En los temas siguientes se describe cómo administrar las tablas configuradas AWS Clean Rooms mediante la AWS Clean Rooms consola.

Para obtener información sobre cómo administrar las tablas configuradas mediante los AWS SDK, consulta la referencia de la AWS Clean Rooms API.

Temas

- Editar detalles de tablas configuradas
- Editar etiquetas de tablas configuradas
- Editar la regla de análisis de tablas configuradas
- Eliminar la regla de análisis de tablas configuradas

Editar detalles de tablas configuradas

Como miembro de la colaboración, puede editar los detalles de la tabla configurada.

Para editar detalles de tablas configuradas

1. Inicie sesión en la consola AWS Management Console y abra la AWS Clean Rooms consola con su Cuenta de AWS (si aún no lo ha hecho).

2. En el panel de navegación izquierdo, elija Tablas configuradas.
3. Elija la tabla configurada que creó.
4. En la página de detalles de la tabla configurada, desplácese hacia abajo hasta Detalles de tabla configurada.
5. Elija Editar.
6. Actualice el Nombre o la Descripción de la tabla configurada.
7. Elija Guardar cambios.

Editar etiquetas de tablas configuradas

Como miembro de la colaboración, después de crear una tabla configurada, puede administrar las etiquetas del recurso de tabla configurada en la pestaña Tablas configuradas.

Para editar las etiquetas de tablas configuradas

1. Inicia sesión en la AWS Clean Rooms consola AWS Management Console y ábrela con la tuya Cuenta de AWS (si aún no lo has hecho).
2. En el panel de navegación izquierdo, elija Tablas configuradas.
3. Elija la tabla configurada que creó.
4. En la página de detalles de la tabla configurada, desplácese hacia abajo hasta la sección Etiquetas.
5. Elija Administrar etiquetas.
6. En la página Administrar etiquetas, puede hacer lo siguiente:
   - Para eliminar una etiqueta, elija Eliminar.
   - Para añadir una etiqueta, elija Añadir nueva etiqueta.
   - Para guardar los cambios, elija Guardar cambios.

Editar la regla de análisis de tablas configuradas

Para editar la regla de análisis de tablas configuradas

1. Inicia sesión en la AWS Clean Rooms consola AWS Management Console y ábrela con la tuya Cuenta de AWS (si aún no lo has hecho).
2. En el panel de navegación izquierdo, elija Tablas configuradas.

3. Elija la tabla configurada que creó.
4. En la página de detalles de la tabla configurada, desplácese hacia abajo hasta la sección Regla de análisis de agregación, Regla de análisis de lista o Regla de análisis personalizada (su elección dependerá del tipo de regla de análisis que haya elegido para la tabla configurada).
5. Elija Editar.
6. En la página Editar regla de análisis, puede:
   - Modificar la Definición de la regla de análisis de la siguiente manera:
     - Modificando el editor JSON.
     - Seleccione Importar desde archivo para cargar una nueva definición de la regla de análisis.
   - Para obtener una vista previa de lo que verán los miembros de una colaboración, seleccione una de las siguientes opciones:
     - Vista de tabla
     - JSON
     - Consulta de ejemplo
7. Elija Guardar cambios para guardar los cambios.

Eliminar la regla de análisis de tablas configuradas

> **Warning**
>
> Esta acción no se puede deshacer y afecta a todos los recursos relacionados.

Para eliminar la regla de análisis de tablas configuradas

1. Inicia sesión en la AWS Clean Rooms consola AWS Management Console y ábrela con la tuya Cuenta de AWS (si aún no lo has hecho).
2. En el panel de navegación izquierdo, elija Tablas configuradas.
3. Elija la tabla configurada que creó.
4. En la página de detalles de la tabla configurada, desplácese hacia abajo hasta la sección Regla de análisis de agregación, Regla de análisis de lista o Regla de análisis personalizada (su elección dependerá del tipo de regla de análisis que haya elegido para la tabla configurada).
5. Elija Eliminar.

6. Si tiene la certeza de que desea eliminar la regla de análisis, elija Eliminar.

Solución de problemas AWS Clean Rooms

En esta sección se describen algunos problemas comunes que pueden surgir al utilizarlos AWS Clean Rooms y cómo solucionarlos.

Problemas

Una o más tablas a las que hace referencia la consulta no están accesibles para el rol de servicio asociado. El propietario de la tabla/rol debe conceder al rol de servicio acceso a la tabla.

- Asegúrese de que los permisos del rol de servicio estén configurados como corresponda. Para obtener más información, consulte Con AWS Clean Rooms figuración.

Uno de los conjuntos de datos subyacentes tiene un formato de archivo no compatible.

- Asegúrese de que su conjunto de datos esté en uno de los formatos de archivo compatibles:
  - Parquet
  - RCFile
  - TextFile
  - SequenceFile
  - RegexSerde
  - OpenCSV
  - AVRO
  - JSON

Para obtener más información, consulte Formatos de datos para AWS Clean Rooms.

Los resultados de la consulta no son los esperados cuando se utiliza la computación criptográfica para Clean Rooms.

Si utiliza la computación criptográfica para Clean Rooms (C3R), compruebe que la consulta utiliza correctamente las columnas cifradas:

- Las columnas sealed solo se utilizan en cláusulas SELECT.
- Las columnas de fingerprint solo se utilizan en cláusulas JOIN (y en cláusulas GROUP BY en ciertas condiciones).
- Solo está JOINing columnas fingerprint con el mismo nombre si los ajustes de la colaboración lo requieren.

Para obtener más información, consulte Computación criptográfica y the section called “Tipos de columnas”.

Seguridad en AWS Clean Rooms

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad aplicables AWS Clean Rooms, consulte Servicios de AWS dentro del alcance por programa de conformidad .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Clean Rooms. Le muestra cómo configurarlo para AWS Clean Rooms cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS Clean Rooms recursos.

Contenido

Protección de datos en AWS Clean Rooms

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Clean Rooms. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja AWS Clean Rooms o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o

diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

AWS Clean Rooms siempre cifra todos los metadatos del servicio en reposo sin necesidad de ninguna configuración adicional. Este cifrado es automático cuando se utiliza AWS Clean Rooms.

Clean Rooms ML cifra todos los datos almacenados en el servicio en reposo. AWS KMS Si decide proporcionar su propia clave KMS, el contenido de sus modelos similares y de los trabajos de generación de segmentos similares se cifra en reposo con su clave KMS.

> **Note**
>
> Puede utilizar las opciones de cifrado de Amazon S3 para proteger sus datos en reposo. Para obtener más información, consulte Especificación del cifrado de Amazon S3 en la Guía del usuario de Amazon S3.

Cifrado en tránsito

AWS Clean Rooms utiliza Transport Layer Security (TLS) y el cifrado del lado del cliente para el cifrado en tránsito. La comunicación siempre AWS Clean Rooms se realiza a través de HTTPS, por lo que sus datos siempre están cifrados en tránsito. Esto incluye todos los datos en tránsito cuando se utiliza Clean Rooms ML.

Cifrado de datos subyacentes

Para obtener más información sobre cómo cifrar sus datos subyacentes, consulte Computación criptográfica para Clean Rooms.

Retención de datos en AWS Clean Rooms

Al crear un modelo similar, Clean Rooms ML lee los datos de entrenamiento, los transforma en un formato adecuado para nuestro modelo de aprendizaje automático y almacena los parámetros del modelo entrenado en Clean Rooms ML. Clean Rooms ML no conserva ninguna copia de sus datos de entrenamiento. AWS Clean Rooms Las consultas SQL no retienen ninguno de sus datos una vez ejecutada la consulta. A continuación, Clean Rooms ML utiliza el modelo entrenado para resumir el

comportamiento de todos sus usuarios. Clean Rooms ML almacena un conjunto de datos a nivel de usuario para cada usuario de sus datos durante el tiempo que su modelo similar esté activo.

Al iniciar un trabajo de generación de segmentos similares, Clean Rooms ML lee los datos iniciales, lee los resúmenes de comportamiento del modelo similar asociado y crea un segmento similar que se almacena en el servicio. AWS Clean Rooms Clean Rooms ML no conserva una copia de sus datos iniciales. Clean Rooms ML almacena el resultado del trabajo a nivel de usuario mientras el trabajo esté activo.

Utilice la API para eliminar los datos del trabajo de generación de segmentos o modelos similares. Clean Rooms ML elimina de forma asíncrona todos los datos asociados al modelo o al trabajo. Una vez completado este proceso, Clean Rooms ML elimina los metadatos del modelo o el trabajo y ya no están visibles en la API. Clean Rooms ML conserva los datos eliminados durante 3 días para evitar la recuperación ante desastres. Una vez que el trabajo o el modelo ya no estén visibles en la API y hayan transcurrido 3 días, todos los datos asociados al modelo o al trabajo se eliminarán permanentemente.

Mejores prácticas para la colaboración de datos en AWS Clean Rooms

En este tema se describen las prácticas recomendadas para realizar colaboraciones de datos en AWS Clean Rooms.

AWS Clean Rooms sigue el modelo de responsabilidad AWS compartida. AWS Clean Rooms ofrece reglas de análisis que puede configurar para reforzar su capacidad de proteger los datos confidenciales en una colaboración. Las reglas de análisis que configure AWS Clean Rooms impondrán las restricciones (controles de consulta y controles de salida de consultas) que haya configurado. Usted es responsable de determinar las restricciones y configurar las reglas de análisis como corresponda.

Las colaboraciones de datos pueden implicar algo más que su uso AWS Clean Rooms. Para ayudarlo a maximizar los beneficios de las colaboraciones de datos, le recomendamos que lleve a cabo las siguientes prácticas recomendadas con el uso de las reglas de análisis AWS Clean Rooms y, específicamente, con ellas.

Temas

Mejores prácticas con AWS Clean Rooms

Usted es responsable de evaluar el riesgo de cada colaboración de datos y compararlo con sus requisitos de privacidad (por ejemplo, con sus programas y políticas de cumplimiento externos e internos). Le recomendamos que tome medidas adicionales con el uso de AWS Clean Rooms. Estas acciones pueden ayudarle a administrar mejor los riesgos y a protegerse de los intentos de reidentificación de los datos por parte de terceros (por ejemplo, ataques diferenciales o ataques de canal lateral).

Por ejemplo, considere la posibilidad de realizar comprobaciones de diligencia debida en sus otros colaboradores y de formalizar acuerdos legales con ellos antes de iniciar una colaboración. Para monitorizar el uso de sus datos, considere también la posibilidad de adoptar otros mecanismos de auditoría cuando utilice AWS Clean Rooms.

Prácticas recomendadas para utilizar reglas de análisis en AWS Clean Rooms

Las reglas de análisis AWS Clean Rooms permiten restringir las consultas que se pueden ejecutar configurando los controles de consulta en una tabla configurada. Por ejemplo, puede definir un control de consulta sobre cómo se puede combinar una tabla configurada y qué columnas se pueden seleccionar. También puede restringir el resultado de la consulta configurando controles de resultados de consulta, como umbrales de agregación en las filas de salida. El servicio rechaza cualquier consulta y elimina las filas que no cumplen las reglas de análisis establecidas por los miembros en sus tablas configuradas de la consulta.

Es aconsejable que siga estas 10 prácticas recomendadas a la hora de usar reglas de análisis en su tabla configurada:

- Cree tablas configuradas distintas para distintos casos de uso de consultas (por ejemplo, planificación de audiencias o atribución). Puede crear varias tablas configuradas con la misma tabla de AWS Glue subyacente.
- Especifique las columnas de la regla de análisis (por ejemplo, columnas de dimensión, columnas de lista, columnas de combinación) que sean necesarias para las consultas de una colaboración. Esto puede contribuir a mitigar el riesgo de ataques diferenciales o de que otros miembros apliquen técnicas de ingeniería inversa a sus datos. Use la característica de lista de columnas permitidas para anotar otras columnas que quizás desee habilitar para consulta en el futuro. Para personalizar las columnas que se pueden usar para una colaboración determinada, cree tablas configuradas adicionales con la misma AWS Glue tabla subyacente.

- Especifique las funciones de la regla de análisis que son necesarias para el análisis en la colaboración. Esto puede contribuir a mitigar el riesgo derivado de errores de función poco frecuentes que puedan presentar información sobre un punto de datos concreto. Para personalizar las funciones que se pueden utilizar en una determinada colaboración, cree tablas configuradas adicionales con la misma tabla de AWS Glue subyacente.
- Añada restricciones de agregación a aquellas columnas cuyos valores a nivel de fila sean confidenciales. Esto incluye las columnas de la tabla configurada que también existen en las tablas y reglas de análisis de otros miembros de la colaboración como una restricción de agregación. También incluye las columnas de su tabla configurada que no se pueden consultar; es decir, las columnas que figuran en su tabla configurada, pero no en la regla de análisis. Las restricciones de agregación pueden contribuir a mitigar el riesgo de correlacionar los resultados de las consultas con datos externos a la colaboración.
- Cree colaboraciones y reglas de análisis de prueba para probar las restricciones creadas con las reglas de análisis especificadas.
- Revise las tablas configuradas de los colaboradores y las reglas de análisis de los miembros en las tablas configuradas para comprobar que coinciden con las condiciones acordadas para la colaboración. Esto puede contribuir a mitigar el riesgo de que otros miembros manipulen sus propios datos para ejecutar consultas no acordadas.
- Revise la consulta de ejemplo proporcionada (solo en la consola) que se habilita en la tabla configurada después de configurar la regla de análisis.

> **Note**
>
> Además de la consulta de ejemplo proporcionada, es posible realizar otras consultas en función de la regla de análisis y de otras tablas y reglas de análisis de los miembros de la colaboración.

- Puede agregar o actualizar una regla de análisis para una tabla configurada en una colaboración. Cuando lo haga, revise todas las colaboraciones a las que está asociada la tabla configurada y el efecto resultante. Esto le ayuda a asegurarse de que ninguna colaboración utilice reglas de análisis obsoletas.
- Revise las consultas ejecutadas en la colaboración para comprobar que coincidan con los casos de uso o con las consultas acordados para la colaboración (las consultas están disponibles en los registros de consultas cuando la característica Registro de consultas está activada). Esto puede contribuir a mitigar el riesgo de que los miembros ejecuten análisis no acordados y de que se produzcan posibles ataques (por ejemplo, ataques de canal lateral).

- Revise las columnas de la tabla configurada que se utilizan en las reglas de análisis de los miembros de la colaboración y en las consultas para asegurarse de que coinciden con lo acordado en la colaboración (las consultas están disponibles en los registros de consultas cuando la característica está activada). Esto puede contribuir a mitigar el riesgo de que otros miembros manipulen sus propios datos para ejecutar consultas no acordadas.

Identity and Access Management para AWS Clean Rooms

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Clean Rooms La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS Clean Rooms

Usuario del servicio: si utiliza el AWS Clean Rooms servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS Clean Rooms funciones para realizar su trabajo, es posible que necesite permisos

adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS Clean Rooms, consulte Solución de problemas AWS Clean Rooms de identidad y acceso.

Administrador de servicios: si estás a cargo de AWS Clean Rooms los recursos de tu empresa, probablemente tengas acceso total a ellos AWS Clean Rooms. Su trabajo consiste en determinar a qué AWS Clean Rooms funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM AWS Clean Rooms, consulte¿Cómo AWS Clean Rooms funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS. Para ver ejemplos de políticas AWS Clean Rooms basadas en la identidad que puede utilizar en IAM, consulte. Ejemplos de políticas basadas en la identidad para AWS Clean Rooms

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM) o la autenticación de inicio de sesión único de su empresa son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre el uso del método recomendado para firmar las solicitudes usted mismo, consulte Proceso de firma de Signature Version 4 en la Referencia general de AWS.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos que no utilice el usuario raíz para las tareas cotidianas. Proteja las credenciales del usuario raíz y utilícelas sólo para las tareas que el usuario raíz pueda realizar. Para obtener la lista completa de tareas que requieren que inicie sesión como usuario raíz, consulte Credenciales de Usuario raíz de la cuenta de AWS e identidades de IAM en la Referencia general de AWS.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como

contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.

- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte el tema sobre el acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener

credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

Cada entidad de IAM (usuario o rol) comienza sin permisos. De forma predeterminada, los usuarios no pueden hacer nada, ni siquiera cambiar sus propias contraseñas. Para conceder permiso a un usuario para hacer algo, el administrador debe asociar una política de permisos a un usuario. O bien el administrador puede agregar al usuario a un grupo que tenga los permisos necesarios. Cuando el administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una identidad. Los permisos resultantes son la intersección de las políticas basadas en identidad de la entidad y los límites de sus permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations

AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Clean Rooms funciona con IAM

Antes de utilizar IAM para gestionar el acceso AWS Clean Rooms, infórmese sobre las funciones de IAM disponibles para su uso. AWS Clean Rooms

Funciones de IAM que puede utilizar con AWS Clean Rooms

Característica de IAM	AWS Clean Rooms soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Parcial
Acciones de políticas	Sí
Recursos de políticas	Sí

Característica de IAM	AWS Clean Rooms soporte
Claves de condición de política (específicas del servicio)	Parcial
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	No

Para obtener una visión general de cómo AWS Clean Rooms y otras funciones Servicios de AWS funcionan con la mayoría de las funciones de IAM, consulte Servicios de AWS la Guía del usuario de IAM sobre cómo funcionan con IAM.

Políticas basadas en la identidad para AWS Clean Rooms

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para AWS Clean Rooms

Para ver ejemplos de políticas AWS Clean Rooms basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Clean Rooms

Políticas basadas en recursos incluidas AWS Clean Rooms

Compatibilidad con las políticas basadas en recursos	Parcial

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

El AWS Clean Rooms servicio solo admite un tipo de política basada en recursos denominada política de recursos gestionados de modelo similar configurada, que se adjunta a un modelo similar configurado. Esta política define qué entidades principales pueden realizar acciones en el modelo similar configurado.

Para obtener información sobre cómo adjuntar una política basada en recursos a un modelo similar configurado, consulte. Comportamientos de IAM para ML AWS Clean Rooms

Acciones políticas para AWS Clean Rooms

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de AWS Clean Rooms acciones, consulta las acciones definidas AWS Clean Rooms en la Referencia de autorización del servicio.

Las acciones políticas AWS Clean Rooms utilizan el siguiente prefijo antes de la acción.

```
cleanrooms
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "cleanrooms:action1",
      "cleanrooms:action2"
         ]
```

Para ver ejemplos de políticas AWS Clean Rooms basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Clean Rooms

Recursos de políticas para AWS Clean Rooms

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de AWS Clean Rooms recursos y sus ARN, consulte los recursos definidos AWS Clean Rooms en la Referencia de autorización de servicios. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Clean Rooms.

Para ver ejemplos de políticas AWS Clean Rooms basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS Clean Rooms

Claves de condición de la política para AWS Clean Rooms

Admite claves de condición de políticas específicas del servicio	Parcial

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para saber cómo AWS Clean Rooms ML utiliza las claves de condición de las políticas, consulte Comportamientos de IAM para ML AWS Clean Rooms.

ACL en AWS Clean Rooms

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AWS Clean Rooms

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AWS Clean Rooms

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para AWS Clean Rooms

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para realizar acciones en AWSél, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre las políticas a la hora de realizar solicitudes de FAS, consulte Forward access sessions.

Roles de servicio para AWS Clean Rooms

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio puede interrumpir AWS Clean Rooms la funcionalidad. Edite las funciones de servicio solo cuando se AWS Clean Rooms proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AWS Clean Rooms

Compatible con roles vinculados al servicio	No

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio

aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya Yes en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para AWS Clean Rooms

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de AWS Clean Rooms . Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por cada uno de los tipos de recursos AWS Clean Rooms, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de la Referencia de autorización de servicios. AWS Clean Rooms

Temas

- Prácticas recomendadas sobre las políticas
- Mediante la consola de AWS Clean Rooms
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear AWS Clean Rooms recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de AWS Clean Rooms

Para acceder a la AWS Clean Rooms consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS Clean Rooms recursos de su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la AWS Clean Rooms consola, adjunte también la política *ReadOnly* AWS gestionada AWS Clean Rooms *FullAccess* o la política gestionada a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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 gestionadas para AWS Clean Rooms

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: **`AWSCleanRoomsReadOnlyAccess`**

Puede adjuntar `AWSCleanRoomsReadOnlyAccess` a sus entidades principales de IAM.

Esta política otorga permisos de solo lectura a recursos y metadatos de una colaboración de `AWSCleanRoomsReadOnlyAccess`.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `CleanRoomsRead`: concede a las entidades principales acceso de solo lectura al servicio.
- `ConsoleDisplayTables`— Permite a los directores acceder de solo lectura a los AWS Glue metadatos necesarios para mostrar los datos sobre AWS Glue las tablas subyacentes en la consola.
- `ConsoleLogSummaryQueryLogs`: concede a las entidades principales permiso para ver los registros de consultas.
- `ConsoleLogSummaryObtainLogs`: concede a las entidades principales permiso para recuperar los resultados de registro.

```
{
 "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 gestionada: **AWSCleanRoomsFullAccess**

Puede adjuntar `AWSCleanRoomsFullAccess` a sus entidades principales de IAM.

Esta política otorga permisos administrativos que permiten el acceso total (lectura, escritura y actualización) a los recursos y metadatos de una AWS Clean Rooms colaboración. Esta política incluye el acceso para realizar consultas.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `CleanRoomsAccess`— Otorga acceso total a todas las acciones de todos los recursos para AWS Clean Rooms.
- `PassServiceRole`: concede acceso para transferir un rol de servicio únicamente al servicio (condición `PassedToService`) cuyo nombre contenga "cleanrooms".
- `ListRolesToPickServiceRole`— Permite a los directores enumerar todas sus funciones para poder elegir una función de servicio cuando la utilicen AWS Clean Rooms.

- `GetRoleAndListRolePoliciesToInspectServiceRole`: permite a las entidades principales ver el rol de servicio y la política correspondiente en IAM.
- `ListPoliciesToInspectServiceRolePolicy`: permite a las entidades principales ver el rol de servicio y la política correspondiente en IAM.
- `GetPolicyToInspectServiceRolePolicy`: permite a las entidades principales ver el rol de servicio y la política correspondiente en IAM.
- `ConsoleDisplayTables`— Permite a los directores acceder de solo lectura a los AWS Glue metadatos necesarios para mostrar los datos sobre AWS Glue las tablas subyacentes de la consola.
- `ConsolePickQueryResultsBucketListAll`: permite a las entidades principales elegir, de una lista de todos los buckets de S3 disponibles, un bucket de Amazon S3 en el que se escriban los resultados de sus consultas.
- `SetQueryResultsBucket`: permite a las entidades principales elegir un bucket de S3 en el que se escriban los resultados de sus consultas.
- `ConsoleDisplayQueryResults`: permite a las entidades principales mostrar al cliente los resultados de las consultas, leídos desde el bucket de S3.
- `WriteQueryResults`: permite a las entidades principales escribir los resultados de las consultas en un bucket de S3 propiedad del cliente.
- `EstablishLogDeliveries`— Permite a los directores enviar registros de consultas al grupo de registros de Amazon CloudWatch Logs de un cliente.
- `SetupLogGroupsDescribe`— Permite a los directores utilizar el proceso de creación de grupos de CloudWatch registros de Amazon Logs.
- `SetupLogGroupsCreate`— Permite a los directores crear un grupo de CloudWatch registros de Amazon Logs.
- `SetupLogGroupsResourcePolicy`— Permite a los directores configurar una política de recursos en el grupo de CloudWatch registros de Amazon Logs.
- `ConsoleLogSummaryQueryLogs`: concede a las entidades principales permiso para ver los registros de consultas.
- `ConsoleLogSummaryObtainLogs`: concede a las entidades principales permiso para recuperar los resultados de registro.

```
{
 "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 gestionada: **AWSCleanRoomsFullAccessNoQuerying**

Puede adjuntar `AWSCleanRoomsFullAccessNoQuerying` a sus IAM principals.

Esta política otorga permisos administrativos que permiten el acceso total (lectura, escritura y actualización) a los recursos y metadatos de una AWS Clean Rooms colaboración. Esta política no incluye el acceso para realizar consultas.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `CleanRoomsAccess`— Otorga acceso total a todas las acciones de todos los recursos AWS Clean Rooms, excepto para las consultas en las colaboraciones.
- `CleanRoomsNoQuerying`: deniega explícitamente `StartProtectedQuery` y `UpdateProtectedQuery` para impedir las consultas.
- `PassServiceRole`: concede acceso para transferir un rol de servicio únicamente al servicio (condición `PassedToService`) cuyo nombre contenga "cleanrooms".
- `ListRolesToPickServiceRole`— Permite a los directores enumerar todas sus funciones para poder elegir una función de servicio cuando la utilicen. AWS Clean Rooms
- `GetRoleAndListRolePoliciesToInspectServiceRole`: permite a las entidades principales ver el rol de servicio y la política correspondiente en IAM.
- `ListPoliciesToInspectServiceRolePolicy`: permite a las entidades principales ver el rol de servicio y la política correspondiente en IAM.
- `GetPolicyToInspectServiceRolePolicy`: permite a las entidades principales ver el rol de servicio y la política correspondiente en IAM.

- `ConsoleDisplayTables`— Permite a los directores acceder de solo lectura a los AWS Glue metadatos necesarios para mostrar los datos sobre AWS Glue las tablas subyacentes de la consola.
- `EstablishLogDeliveries`— Permite a los directores enviar registros de consultas al grupo de registros de Amazon CloudWatch Logs de un cliente.
- `SetupLogGroupsDescribe`— Permite a los directores utilizar el proceso de creación de grupos de CloudWatch registros de Amazon Logs.
- `SetupLogGroupsCreate`— Permite a los directores crear un grupo de CloudWatch registros de Amazon Logs.
- `SetupLogGroupsResourcePolicy`— Permite a los directores configurar una política de recursos en el grupo de CloudWatch registros de Amazon Logs.
- `ConsoleLogSummaryQueryLogs`: concede a las entidades principales permiso para ver los registros de consultas.
- `ConsoleLogSummaryObtainLogs`: concede a las entidades principales permiso para recuperar los resultados de registro.
- `cleanrooms`— Gestione las colaboraciones, las plantillas de análisis, las tablas configuradas, las membresías y los recursos asociados dentro del servicio. AWS Clean Rooms Realice diversas operaciones, como crear, actualizar, eliminar, enumerar y recuperar información sobre estos recursos.
- `iam`— Transfiera al servicio las funciones de AWS Clean Rooms servicio cuyos nombres contengan `cleanrooms` «». Enumere las funciones y políticas e inspeccione las funciones y políticas de servicio relacionadas con el AWS Clean Rooms servicio.
- `glue`— Recupere información sobre bases de datos, tablas, particiones y esquemas de AWS Glue. Esto es necesario para que el AWS Clean Rooms servicio muestre las fuentes de datos subyacentes e interactúe con ellas.
- `logs`— Gestione las entregas de registros, los grupos de registros y las políticas de recursos para CloudWatch los registros. Consulte y recupere los registros relacionados con el AWS Clean Rooms servicio. Estos permisos son necesarios para la supervisión, la auditoría y la solución de problemas dentro del servicio.

La política también deniega explícitamente las acciones `cleanrooms:StartProtectedQuery` e impide `cleanrooms:UpdateProtectedQuery` que los usuarios ejecuten o actualicen directamente las consultas protegidas, lo que debe hacerse a través de los mecanismos AWS Clean Rooms controlados.

```
{
 "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 gestionada: **AWSCleanRoomsMLReadOnlyAccess**

Puede adjuntar `AWSCleanRoomsMLReadOnlyAccess` a sus entidades principales de IAM.

Esta política otorga permisos de solo lectura a recursos y metadatos de una colaboración de `AWSCleanRoomsMLReadOnlyAccess`.

Esta política incluye los permisos siguientes:

- `CleanRoomsConsoleNavigation`— Otorga acceso para ver las pantallas de la AWS Clean Rooms consola.
- `CleanRoomsMLRead`— Permite a los directores acceder de solo lectura al servicio 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 gestionada: **AWSCleanRoomsMLFullAccess**

Puede adjuntar `AWSCleanRoomsMLFullAcces` a sus entidades principales de IAM. Esta política otorga permisos administrativos que permiten el acceso total (lectura, escritura y actualización) a los recursos y metadatos que necesita Clean Rooms ML.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `CleanRoomsMLFullAccess`— Otorga acceso a todas las acciones de Clean Rooms ML.
- `PassServiceRole`: concede acceso para transferir un rol de servicio únicamente al servicio (condición `PassedToService`) cuyo nombre contenga "cleanrooms-ml".
- `CleanRoomsConsoleNavigation`— Otorga acceso para ver las pantallas de la AWS Clean Rooms consola.
- `CollaborationMembershipCheck`— Al iniciar un trabajo de generación de audiencia (segmento similar) dentro de una colaboración, el servicio Clean Rooms ML llama `ListMembers` para comprobar que la colaboración es válida, que la persona que llama es un miembro activo y que el propietario del modelo de audiencia configurado es un miembro activo. Este permiso siempre es obligatorio; el SID de navegación de la consola solo es necesario para los usuarios de la consola.
- `AssociateModels`— Permite a los directores asociar un modelo de aprendizaje automático de salas limpias a su colaboración.
- `TagAssociations`: permite a las entidades principales añadir etiquetas a la asociación entre un modelo similar y una colaboración.
- `ListRolesToPickServiceRole`— Permite a los directores enumerar todas sus funciones para poder elegir una función de servicio cuando la utilicen. AWS Clean Rooms
- `GetRoleAndListRolePoliciesToInspectServiceRole`: permite a las entidades principales ver el rol de servicio y la política correspondiente en IAM.
- `ListPoliciesToInspectServiceRolePolicy`: permite a las entidades principales ver el rol de servicio y la política correspondiente en IAM.
- `GetPolicyToInspectServiceRolePolicy`: permite a las entidades principales ver el rol de servicio y la política correspondiente en IAM.
- `ConsoleDisplayTables`— Permite a los directores acceder de solo lectura a los AWS Glue metadatos necesarios para mostrar los datos sobre AWS Glue las tablas subyacentes de la consola.
- `ConsolePickOutputBucket`: permite a las entidades principales seleccionar buckets de Amazon S3 para las salidas configuradas del modelo de audiencia.
- `ConsolePickS3Location`: permite a las entidades principales seleccionar la ubicación dentro de un bucket para los resultados configurados del modelo de audiencia.

```
{
```

```
    "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 actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS Clean Rooms desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS Clean Rooms documento.

Cambio	Descripción	Fecha
AWSCleanRoomsFullAccessNoQuerying: actualización de una política actual	Se agregó cleanrooms:BatchGetSchemaAnalysisRule a CleanRoomsAccess.	13 de mayo de 2024
AWSCleanRoomsFullAccess: actualización de una política actual	Se actualizó el identificador de la declaración AWSCleanRoomsFullAccess de ConsolePickQueryResultsBucket a a SetQueryResultsBucket en esta política para representar mejor los permisos, ya que los permisos son necesarios para configurar el grupo de resultados de las	21 de marzo de 2024

Cambio	Descripción	Fecha
	consultas tanto con la consola como sin ella.	
AWSCleanRoomsMLReadOnlyAccess: política nueva AWSCleanRoomsMLFullAccess: política nueva	Se ha añadido AWSCleanRoomsMLReadOnlyAccess y AWSCleanRoomsMLFullAccess para admitir AWS Clean Rooms ML.	29 de noviembre de 2023
AWSCleanRoomsFullAccessNoQuerying: actualización de una política actual	Se agregaron cleanrooms:CreateAnalysisTemplate cleanrooms:GetAnalysisTemplatecleanrooms:UpdateAnalysisTemplate, cleanrooms:DeleteAnalysisTemplate,cleanrooms:ListAnalysisTemplates, cleanrooms:GetCollaborationAnalysisTemplatecleanrooms:BatchGetCollaborationAnalysisTemplate, y cleanrooms:ListCollaborationAnalysisTemplates to CleanRoomsAccess para habilitar la nueva función de plantillas de análisis.	31 de julio de 2023
AWSCleanRoomsFullAccessNoQuerying: actualización de una política actual	Se ha añadido cleanrooms:ListTagsForResource, cleanrooms:UntagResource y cleanrooms:TagResource a CleanRoomsAccess para habilitar el etiquetado de recursos.	21 de marzo de 2023
AWS Clean Rooms comenzó a rastrear los cambios	AWS Clean Rooms comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	12 de enero de 2023

Solución de problemas AWS Clean Rooms de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con un AWS Clean Rooms IAM.

Temas

No estoy autorizado a realizar ninguna acción en AWS Clean Rooms

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `cleanrooms:`*`GetWidget`*.

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

En este caso, la política de Mateo se debe actualizar para permitirle acceder al recurso *`my-example-widget`* mediante la acción `cleanrooms:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS Clean Rooms.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Clean Rooms. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AWS Clean Rooms recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol.

Para más información, consulte lo siguiente:

- Para saber si AWS Clean Rooms es compatible con estas funciones, consulte¿Cómo AWS Clean Rooms funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición global `aws:SourceArn` en las políticas de recursos para limitar los permisos que AWS Clean Rooms concede a otro servicio para el recurso. Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. En AWSClean Rooms, también tienes que compararla con la clave de condición. `sts:ExternalId`

El valor de `aws:SourceArn` debe definirse con el ARN de pertenencia del rol asumido.

El siguiente ejemplo muestra cómo usar la clave de contexto de condición global `aws:SourceArn` en AWS Clean Rooms para evitar el problema del suplente confuso.

> **Note**
>
> La política de ejemplo se aplica a la política de confianza del rol de servicio que utiliza AWS Clean Rooms para acceder a los datos de los clientes.
> El valor de *membershipID* es su ID de pertenencia a AWS Clean Rooms en la colaboración.

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

Comportamientos de IAM para ML AWS Clean Rooms

Trabajos entre cuentas

Clean Rooms ML permite que otra Cuenta de AWS persona acceda de forma segura Cuenta de AWS a determinados recursos creados por una persona en su cuenta. Cuando un cliente de Cuenta de AWS A llama `StartAudienceGenerationJob` a un `ConfiguredAudienceModel` recurso propiedad de Cuenta de AWS B, Clean Rooms ML crea dos ARN para la tarea. Un ARN en Cuenta de AWS A y otro en B. Cuenta de AWS Los ARN son idénticos excepto por sus. Cuenta de AWS

Clean Rooms ML crea dos ARN para el trabajo a fin de garantizar que ambas cuentas puedan aplicar sus propias políticas de IAM a los trabajos. Por ejemplo, ambas cuentas pueden usar el control de acceso basado en etiquetas y aplicar las políticas de su organización. AWS El trabajo procesa los datos de ambas cuentas, de modo que ambas cuentas pueden eliminar el trabajo y sus datos asociados. Ninguna de las dos cuentas puede impedir que la otra elimine el trabajo.

Solo hay una ejecución de trabajo y ambas cuentas pueden ver la tarea cuando llaman a `ListAudienceGenerationJobs`. Ambas cuentas pueden llamar a las API `GetDelete`, y a `Export` las API en el trabajo mediante el ARN con su propio Cuenta de AWS ID.

Ninguno de los dos Cuenta de AWS puede acceder al trabajo cuando se utiliza un ARN con el otro Cuenta de AWS ID.

El nombre del trabajo debe ser único dentro de una Cuenta de AWS. El nombre en Cuenta de AWS B es *`$accounta-$name`*. El nombre elegido por Cuenta de AWS A lleva el prefijo A cuando el trabajo Cuenta de AWS se visualiza en B. Cuenta de AWS

Para que una cuenta cruzada `StartAudienceGenerationJob` tenga éxito, Cuenta de AWS B debe permitir esa acción tanto en el nuevo trabajo de B como `ConfiguredAudienceModel` en el de Cuenta de AWS Cuenta de AWS B mediante una política de recursos similar a la del siguiente ejemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Clean-Rooms-<CAMA ID>",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "accountA"
                ]
            },
            "Action": [
                "cleanrooms-ml:StartAudienceGenerationJob"
            ],
            "Resource": [
                "arn:aws:cleanrooms-ml:us-west-1:AccountB:configured-audience-
model/id",
                "arn:aws:cleanrooms-ml:us-west-1:AccountB:audience-generation-job/*"
            ],
            // optional - always set by AWS Clean Rooms
"Condition":{"StringEquals":{"cleanrooms-ml:CollaborationId":"UUID"}}
        }
    ]
}
```

Si utilizas la API de AWS Clean Rooms ML para crear un modelo similar `manageResourcePolicies` configurado con el valor true, AWS Clean Rooms crea esta política automáticamente.

Además, la política de identidad de la persona que llama en Cuenta de AWS A necesita `StartAudienceGenerationJob` permiso. `arn:aws:cleanrooms-ml:us-west-1:AccountA:audience-generation-job/*` Por lo tanto, hay tres recursos de acción de IAM`StartAudienceGenerationJob`: el trabajo Cuenta de AWS A, el trabajo Cuenta de AWS B y el Cuenta de AWS trabajo B. `ConfiguredAudienceModel`

> **Warning**
>
> El Cuenta de AWS que inició el trabajo recibe un evento de registro de AWS CloudTrail auditoría sobre el trabajo. La Cuenta de AWS propietaria de `ConfiguredAudienceModel` no recibe ningún evento de registro de auditoría de AWS CloudTrail .

Etiquetado de trabajos

Al establecer el parámetro `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` de `CreateConfiguredAudienceModel`, todos los trabajos de generación de segmentos similares de su cuenta que se creen a partir de ese modelo similar configurado tendrán de forma predeterminada las mismas etiquetas que el modelo similar configurado. El modelo similar configurado es el principal y el trabajo de generación de segmentos similares es el secundario.

Si está creando un trabajo en su propia cuenta, las etiquetas de solicitud del trabajo anulan las etiquetas principales. Los trabajos creados por otras cuentas nunca crean etiquetas en su cuenta. Si establece `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` y otra cuenta crea un trabajo, hay dos copias del trabajo. La copia de su cuenta tiene las etiquetas del recurso principal y la copia de la cuenta del remitente del trabajo tiene las etiquetas de la solicitud.

Validación de colaboradores

Al conceder permisos a otros miembros de una AWS Clean Rooms colaboración, la política de recursos debe incluir la clave de condición`cleanrooms-ml:CollaborationId`. Esto exige que el `collaborationId` parámetro esté incluido en la StartAudienceGenerationJobsolicitud. Cuando el `collaborationId` parámetro se incluye en la solicitud, Clean Rooms ML valida que la colaboración existe, que el remitente del trabajo es un miembro activo de la colaboración y que el propietario del modelo similar configurado es un miembro activo de la colaboración.

Cuando AWS Clean Rooms gestione la política de recursos del modelo similar configurada (el `manageResourcePolicies` parámetro es una `TRUE` CreateConfiguredAudienceModelAssociation solicitud), esta clave de condición se establecerá en la política de recursos. Por lo tanto, debe especificar la entrada`collaborationId`. StartAudienceGenerationJob

Acceso entre cuentas

Solo se puede llamar a `StartAudienceGenerationJob` entre cuentas. Todas las demás API de aprendizaje automático de Clean Rooms solo se pueden usar con los recursos de su propia cuenta. Esto garantiza que sus datos de entrenamiento, la configuración del modelo similar y otra información permanezcan privados.

Clean Rooms ML nunca revela Amazon S3 ni AWS Glue las ubicaciones de las cuentas. La ubicación de los datos de entrenamiento, la ubicación de salida del modelo similar configurado y la ubicación inicial del trabajo de generación de segmentos similar nunca están visibles entre cuentas. Si `Get` un trabajo de generación de audiencia enviado por otra cuenta, el servicio no mostrará la ubicación inicial.

Validación de conformidad para AWS Clean Rooms

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Clean Rooms

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las

zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura AWS global.

Seguridad de la infraestructura en AWS Clean Rooms

Como servicio gestionado, AWS Clean Rooms está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Clean Rooms través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Seguridad de la red

Cuando se AWS Clean Rooms lee desde el bucket de S3 durante la ejecución de la consulta, el tráfico entre Amazon S3 AWS Clean Rooms y Amazon S3 se enruta de forma segura a través de la red AWS privada. El tráfico en tránsito se firma con el protocolo Signature Version 4 (SIGv4) de Amazon y se cifra mediante HTTPS. Este tráfico se autoriza en función del rol de servicio de IAM que se haya configurado para la tabla configurada.

Puede conectarse mediante programación a AWS Clean Rooms través de un punto final. Para obtener una lista de puntos de conexión de servicio, consulte Puntos de conexión y cuotas de AWS Clean Rooms en la Referencia general de AWS.

Todos los puntos de conexión de servicio son únicamente HTTPS. Puede utilizar los puntos de conexión de Amazon Virtual Private Cloud (VPC) en caso de que desee conectarse desde AWS Clean Rooms su VPC y no desee tener conectividad a Internet. Para obtener más información, consulte Acceder a AWS los servicios AWS PrivateLink en la Guía.AWS PrivateLink

Puede asignar políticas de IAM a sus directores de IAM que utilicen las claves aws: SourceVpce context para restringir a su director de IAM a fin de que solo pueda realizar llamadas a través de AWS Clean Rooms un punto final de VPC y no a través de Internet.

Acceda al aprendizaje AWS Clean Rooms automático mediante AWS Clean Rooms un punto final de interfaz ()AWS PrivateLink

Puede usarlo AWS PrivateLink para crear una conexión privada entre su nube privada virtual (VPC) y ML AWS Clean Rooms . AWS Clean Rooms Puede acceder a nuestro AWS Clean Rooms AWS Clean Rooms ML como si estuviera en su VPC, sin el uso de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect una conexión. Las instancias de la VPC no necesitan direcciones IP públicas para acceder a AWS Clean Rooms.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a AWS Clean Rooms.

Para obtener más información, consulte Acceso a los Servicios de AWS a través de AWS PrivateLink en la Guía de AWS PrivateLink .

Consideraciones sobre AWS Clean Rooms

Antes de configurar un punto final de interfaz para AWS Clean Rooms, consulte las consideraciones de la AWS PrivateLink guía.

AWS Clean Rooms y AWS Clean Rooms ML permiten realizar llamadas a todas sus acciones de API a través del punto final de la interfaz.

Las políticas de puntos de conexión de VPC no son compatibles con el ML AWS Clean Rooms . AWS Clean Rooms De forma predeterminada, se permite el acceso total AWS Clean Rooms y el AWS Clean Rooms aprendizaje automático a través del punto final de la interfaz. Como alternativa, puede asociar un grupo de seguridad a las interfaces de red de los puntos finales para controlar el

tráfico hacia AWS Clean Rooms o el aprendizaje AWS Clean Rooms automático a través del punto final de la interfaz.

Cree un punto final de interfaz para AWS Clean Rooms

Puede crear un punto de enlace de interfaz para AWS Clean Rooms el AWS Clean Rooms aprendizaje automático mediante la consola de Amazon VPC o el AWS Command Line Interface ()AWS CLI. Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Cree un punto final de interfaz para AWS Clean Rooms usar el siguiente nombre de servicio.

```
com.amazonaws.region.cleanrooms
```

Cree un punto final de interfaz para AWS Clean Rooms ML con el siguiente nombre de servicio.

```
com.amazonaws.region.cleanrooms-ml
```

Si habilita DNS privado para el punto de conexión de interfaz, puede realizar solicitudes a la API para AWS Clean Rooms usando su nombre de DNS predeterminado para la región. Por ejemplo, `cleanrooms-ml.us-east-1.amazonaws.com`.

Monitorización AWS Clean Rooms

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS Clean Rooms AWS las demás soluciones. AWS proporciona las siguientes herramientas de monitoreo para observar AWS Clean Rooms, informar cuando algo anda mal y tomar medidas automáticas cuando sea apropiado:

- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde instancias de Amazon EC2 y otras fuentes. AWS CloudTrail Amazon CloudWatch Logs puede supervisar la información de los archivos de registro y notificarle cuando se alcancen determinados umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.

  Clean Rooms ML permite realizar tareas entre cuentas para determinadas acciones de la API. La Cuenta de AWS persona que inició el trabajo recibe el evento del registro de AWS CloudTrail auditoría del trabajo. Para obtener más información, consulte Comportamientos de IAM para ML AWS Clean Rooms.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por usted o en su nombre Cuenta de AWS y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Registrar llamadas a la API de AWS Clean Rooms mediante AWS CloudTrail

AWS Clean Rooms se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un Servicio de AWS en AWS Clean Rooms. CloudTrail captura las llamadas a la API de AWS Clean Rooms como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de AWS Clean Rooms y las llamadas desde el código a las operaciones de la API de AWS Clean Rooms. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para AWS Clean Rooms. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada

por CloudTrail, puede determinar la solicitud que se realizó a AWS Clean Rooms, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de AWS Clean Rooms en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando la crea. Cuando se produce una actividad en AWS Clean Rooms, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de Servicio de AWS en Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de AWS Clean Rooms, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros Servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte lo siguiente:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de varias regiones
- Recepción de archivos de registro de CloudTrail de varias cuentas

Todas las acciones de AWS Clean Rooms las registra CloudTrail y se documentan en la Referencia de la API de AWS Clean Rooms.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de registro de AWS Clean Rooms

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

Ejemplos de eventos de CloudTrail en AWS Clean Rooms

Los siguientes ejemplos demuestran eventos de CloudTrail para:

Temas

- StartProtectedQuery (correcto)
- StartProtectedQuery (error)

StartProtectedQuery (correcto)

```
{
    "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 (error)

```
{
    "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"
}
```

Creación de AWS Clean Rooms recursos con AWS CloudFormation

AWS Clean Rooms está integrado con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos. Como resultado de esta integración, puede dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Usted crea una plantilla que describe todos los AWS recursos que desea y los AWS CloudFormation aprovisiona y configura automáticamente. Algunos ejemplos de recursos son las colaboraciones, las tablas configuradas, las asociaciones de tablas configuradas y las pertenencias.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar los AWS Clean Rooms recursos de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos una y otra vez en varios Cuentas de AWS y Regiones de AWS.

AWS Clean Rooms y AWS CloudFormation plantillas

Para aprovisionar y configurar recursos AWS Clean Rooms y servicios relacionados, debe conocer AWS CloudFormation las plantillas. Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus AWS CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar AWS CloudFormation Designer para ayudarte a empezar con AWS CloudFormation las plantillas. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation ? en la Guía del usuario de AWS CloudFormation .

AWS Clean Rooms permite crear colaboraciones, tablas configuradas, asociaciones de tablas configuradas y membresías en ellas. AWS CloudFormation Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para colaboraciones, tablas configuradas, asociaciones de tablas configuradas y pertenencias, consulte la Referencia de tipos de recursos de AWS Clean Rooms en la Guía del usuario de AWS CloudFormation .

Están disponibles las siguientes plantillas:

- Plantilla de análisis

  Especifique una plantilla de AWS Clean Rooms análisis, que incluya el nombre, la descripción, el formato, la fuente, los parámetros y las etiquetas.

  Para obtener más información, consulte los temas siguientes:

AWS::CleanRooms::AnalysisTemplate en la Guía del usuario de AWS Clean Rooms .

CreateAnalysisTemplate en la Referencia de la API de AWS Clean Rooms

- Colaboración

  Especifique una AWS Clean Rooms colaboración, incluidos el nombre, la descripción, el tipo, los parámetros y las etiquetas.

  Para obtener más información, consulte los temas siguientes:

  AWS::CleanRooms::Collaboration en la Guía del usuario de AWS CloudFormation .

  CreateCollaboration en la Referencia de la API de AWS Clean Rooms

- Tabla configurada

  Especifique una tabla configurada AWS Clean Rooms, incluidas las columnas permitidas, el método de análisis, la descripción, el nombre, la referencia de la tabla, el presupuesto de privacidad y las etiquetas. Las tablas configuradas representan una referencia a una tabla existente en la AWS Glue Data Catalog que se ha configurado para su uso en AWS Clean Rooms. Una tabla configurada contiene una regla de análisis que determina cómo se pueden utilizar los datos.

  Para obtener más información, consulte los temas siguientes:

  AWS::CleanRooms::ConfiguredTable en la Guía del usuario de AWS CloudFormation .

  CreateConfiguredTable en la Referencia de la API de AWS Clean Rooms

- Asociación de tablas configuradas

  Especifique una asociación de tabla configurada en AWS Clean Rooms, incluidos el ID, la descripción, el ID de membresía, el nombre, el rol, el nombre de recurso de Amazon (ARN) y las etiquetas. Una asociación de tablas configuradas vincula una tabla configurada a una colaboración.

  Para obtener más información, consulte los temas siguientes:

  AWS::CleanRooms::ConfiguredTableAssociation en la Guía del usuario de AWS CloudFormation .

  CreateConfiguredTableAssociation en la Referencia de la API de AWS Clean Rooms

- Pertenencia

  Especifique la pertenencia para un identificador de colaboración específico y únase a la colaboración en AWS Clean Rooms.

  Para obtener más información, consulte los temas siguientes:

  AWS::CleanRooms::Membership en la Guía del usuario de AWS CloudFormation .

  CreateMembership en la Referencia de la API de AWS Clean Rooms
- Plantilla de presupuesto de privacidad

  Especifica una plantilla de presupuesto de AWS Clean Rooms privacidad, que incluya un presupuesto de privacidad, el ruido añadido por consulta y una actualización mensual del presupuesto de privacidad.

  Para obtener más información, consulte los temas siguientes:

  AWS::CleanRooms::PrivacyBudgetTemplate en la Guía del usuario de AWS CloudFormation .

  CreatePrivacyBudgetTemplate en la Referencia de la API de AWS Clean Rooms
- Crea un conjunto de datos de entrenamiento

  Especifique un conjunto de datos de entrenamiento para un modelo de aprendizaje automático de salas limpias a partir de una AWS Glue tabla.

  Para obtener más información, consulte los temas siguientes:

  AWS::CleanRoomsML::TrainingDataset en la Guía del usuario de AWS CloudFormation .

  CreateTrainingDataseten la referencia de la API de ML para salas limpias

Obtenga más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormation Guía del usuario
- AWS CloudFormation Referencia de la API

- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

Cuotas para AWS Clean Rooms

Tienes Cuenta de AWS cuotas predeterminadas, antes denominadas límites, para cada una de ellas Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de un Región de AWS. Puede solicitar aumentos para algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas AWS Clean Rooms, abra la consola Service Quotas. En el panel de navegación, elija Servicios de AWS y seleccione AWS Clean Rooms.

Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si la cuota aún no está disponible en Service Quotas, utilice el formulario de aumento del límite de servicio.

Cuenta de AWS Tiene las siguientes cuotas relacionadas con AWS Clean Rooms.

Recurso	Predeterminado	Descripción
Miembros invitados por colaboración	5	Número máximo de miembros invitados por colaboración
Pertenencias por cuenta de	100	Número máximo de pertenencias de una cuenta
Colaboraciones creadas por cuenta	10	Número máximo de colaboraciones creadas por cuenta
Tablas configuradas por cuenta	60	Número máximo de tablas configuradas que puede crear una cuenta
Asociaciones de tablas por pertenencia	25	Número máximo de tablas asociadas por pertenencia activa
Consultas simultáneas en curso por pertenencia	5	Número máximo de consultas simultáneas en curso por pertenencia

Recurso	Predeterminado	Descripción
Lista permitida de columnas por tabla configurada	100	Número máximo de columnas que se pueden incluir en la lista permitida por tabla configurada
Tablas configuradas por consulta protegida	15	Número máximo de tablas configuradas en una consulta protegida
Plantillas de análisis por pertenencia	25	Número máximo de plantillas de análisis por pertenencia
Asociaciones de modelos similares (modelo de audiencia) configuradas por pertenencia	5	Número máximo de asociaciones de modelos similares configuradas por pertenencia.

Límites de parámetros de recurso

Recurso	Predeterminado	Descripción
Tamaño de regla de análisis	100 KB	Tamaño máximo de JSON de una regla de análisis
Longitud del texto de consulta	90 KB (8 KB para consultas de privacidad diferencial)	Longitud máxima del texto de una instrucción de consulta SQL
Tiempo de ejecución de consultas	12 horas	Tiempo máximo que se ejecuta una consulta antes de que se agote el tiempo de espera
Tamaño de salida del archivo de datos de consulta	6,2 GB	Tamaño máximo de un archivo de salida de una consulta protegida

Cuenta de AWS Tiene las siguientes cuotas de transacciones de API por segundo (TPS) por cuenta y punto final.

Cuotas de limitación controlada de la API

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `BatchGetCollaborationAnalysisTemplate`	5 TPS	Número máximo de llamadas a la API `BatchGetCollaborationAnalysisTemplate` por segundo
Tasa de solicitudes `BatchGetSchema`	5 TPS	Número máximo de llamadas a la API `BatchGetSchema` por segundo
Tasa de solicitudes `CreateAnalysisTemplate`	5 TPS	Número máximo de llamadas a la API `CreateAnalysisTemplate` por segundo
Tasa de solicitudes `CreateCollaboration`	5 TPS	Número máximo de llamadas a la API `CreateCollaboration` por segundo
Tasa de solicitudes `CreateConfiguredAudienceModelAssociation`	5 TPS	Número máximo de llamadas `CreateConfiguredAudienceModelAssociation` por segundo
Tasa de solicitudes `CreateConfiguredTable`	5 TPS	Número máximo de llamadas `CreateConfiguredTable` por segundo
Tasa de solicitudes `CreateConfiguredTableAnalysisRule`	5 TPS	Número máximo de llamadas `CreateConfiguredTableAnalysisRule` por segundo

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `CreateConfiguredTableAssociation`	5 TPS	Número máximo de llamadas `CreateConfiguredTableAssociation` por segundo
Tasa de solicitudes `CreateMembership`	5 TPS	Número máximo de llamadas `CreateMembership` por segundo
Tasa de solicitudes `CreatePrivacyBudgetTempate`	5 TPS	Número máximo de llamadas `CreatePrivacyBudgetTemplate` por segundo
Tasa de solicitudes `DeleteAnalysisTemplate`	5 TPS	Número máximo de llamadas `DeleteAnalysisTemplate` por segundo
Tasa de solicitudes `DeleteCollaboration`	5 TPS	Número máximo de llamadas `DeleteCollaboration` por segundo
Tasa de solicitudes `DeleteConfiguredAudienceModelAssociation`	5 TPS	Número máximo de llamadas `DeleteConfiguredAudienceModelAssociation` por segundo
Tasa de solicitudes `DeleteConfiguredTable`	5 TPS	Número máximo de llamadas `DeleteConfiguredTable` por segundo
Tasa de solicitudes `DeleteConfiguredTableAnalysisRule`	5 TPS	Número máximo de llamadas `DeleteConfiguredTableAnalysisRule` por segundo

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `DeleteConfiguredTableAssociation`	5 TPS	Número máximo de llamadas `DeleteConfiguredTableAssociation` por segundo
Tasa de solicitudes `DeleteMember`	5 TPS	Número máximo de llamadas `DeleteMember` por segundo
Tasa de solicitudes `DeleteMembership`	5 TPS	Número máximo de llamadas `DeleteMembership` por segundo
Tasa de solicitudes `DeletePrivacyBudgetTemplate`	5 TPS	Número máximo de llamadas `DeletePrivacyBudgetTemplate` por segundo
Tasa de solicitudes `GetAnalysisTemplate`	5 TPS	Número máximo de llamadas `GetAnalysisTemplate` por segundo
Tasa de solicitudes `GetCollaboration`	5 TPS	Número máximo de llamadas `GetCollaboration` por segundo
Tasa de solicitudes `GetCollaborationConfiguredAudienceModelAssociation`	5 TPS	Número máximo de llamadas `GetCollaborationConfiguredAudienceModelAssociation` por segundo
Tasa de solicitudes `GetCollaborationPrivacyBudgetTemplate`	5 TPS	Número máximo de llamadas `GetCollaborationPrivacyBudgetTemplate` por segundo

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `GetConfiguredAudienceModelAssociation`	5 TPS	Número máximo de llamadas `GetConfiguredAudienceModelAssociation` por segundo
Tasa de solicitudes `GetConfiguredTable`	5 TPS	Número máximo de llamadas `GetConfiguredTable` por segundo
Tasa de solicitudes `GetConfiguredTableAnalysisRule`	5 TPS	Número máximo de llamadas `GetConfiguredTableAnalysisRule` por segundo
Tasa de solicitudes `GetConfiguredTableAssociation`	20 TPS	Número máximo de llamadas `GetConfiguredTableAssociation` por segundo
Tasa de solicitudes `GetMembership`	5 TPS	Número máximo de llamadas `GetMembership` por segundo
Tasa de solicitudes `GetPrivacyBudgetTemplate`	5 TPS	Número máximo de llamadas `GetPrivacyBudgetTemplate` por segundo
Tasa de solicitudes `GetProtectedQuery`	20 TPS	Número máximo de llamadas `GetProtectedQuery` por segundo
Tasa de solicitudes `GetSchema`	5 TPS	Número máximo de llamadas `GetSchema` por segundo
Tasa de solicitudes `GetSchemaAnalysisRule`	5 TPS	Número máximo de llamadas `GetSchemaAnalysisRule` por segundo

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `ListAnalysisTemplates`	5 TPS	Número máximo de llamadas `ListAnalysisTemplates` por segundo
Tasa de solicitudes `ListCollaborationConfiguredAudienceModelAssociations`	5 TPS	Número máximo de llamadas `ListCollaborationConfiguredAudienceModelAssociations` por segundo
Tasa de solicitudes `ListCollaborationPrivacyBudgets`	5 TPS	Número máximo de llamadas `ListCollaborationPrivacyBudgets` por segundo
Tasa de solicitudes `ListCollaborationPrivacyBudgetTemplates`	5 TPS	Número máximo de llamadas `ListCollaborationPrivacyBudgetTemplates` por segundo
Tasa de solicitudes `ListCollaborations`	5 TPS	Número máximo de llamadas `ListCollaborations` por segundo
Tasa de solicitudes `ListConfiguredAudienceModelAssociations`	5 TPS	Número máximo de llamadas `ListConfiguredAudienceModelAssociations` por segundo
Tasa de solicitudes `ListConfiguredTableAssociations`	5 TPS	Número máximo de llamadas `ListConfiguredTableAssociations` por segundo

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `ListConfiguredTables`	5 TPS	Número máximo de llamadas `ListConfiguredTables` por segundo
Tasa de solicitudes `ListMembers`	5 TPS	Número máximo de llamadas `ListMembers` por segundo
Tasa de solicitudes `ListMemberships`	5 TPS	Número máximo de llamadas `ListMemberships` por segundo
Tasa de solicitudes `ListPrivacyBudgets`	5 TPS	Número máximo de llamadas `ListPrivacyBudgets` por segundo
Tasa de solicitudes `ListPrivacyBudgetTemplates`	5 TPS	Número máximo de llamadas `ListPrivacyBudgetTemplates` por segundo
Tasa de solicitudes `ListProtectedQueries`	5 TPS	Número máximo de llamadas `ListProtectedQueries` por segundo
Tasa de solicitudes `ListSchemas`	5 TPS	Número máximo de llamadas `ListSchemas` por segundo
Tasa de solicitudes `StartProtectedQuery`	5 TPS	Número máximo de llamadas `StartProtectedQuery` por segundo
Tasa de solicitudes `UpdateAnalysisTemplate`	5 TPS	Número máximo de llamadas `UpdateAnalysisTemplate` por segundo
Tasa de solicitudes `UpdateCollaboration`	5 TPS	Número máximo de llamadas `UpdateCollaboration` por segundo

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `UpdateConfiguredAudienceModelAssociation`	5 TPS	Número máximo de llamadas `UpdateConfiguredAudienceModelAssociation` por segundo
Tasa de solicitudes `UpdateConfiguredTable`	5 TPS	Número máximo de llamadas `UpdateConfiguredTable` por segundo
Tasa de solicitudes `UpdateConfiguredTableAnalysisRule`	5 TPS	Número máximo de llamadas `UpdateConfiguredTableAnalysisRule` por segundo
Tasa de solicitudes `UpdateConfiguredTableAssociation`	5 TPS	Número máximo de llamadas `UpdateConfiguredTableAssociation` por segundo
Tasa de solicitudes `UpdatePrivacyBudgetTemplate`	5 TPS	Número máximo de llamadas `UpdatePrivacyBudgetTemplate` por segundo

AWS Clean Rooms Cuotas de limitación de API de ML

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes de `CreateAudienceModel`	Tasa de 1 TPS, ráfaga de 3 TPS	Número máximo de llamadas a la API `CreateAudienceModel` por segundo
Tasa de solicitudes `CreateConfiguredAudienceModel`	10 TPS	Número máximo de llamadas a la API `CreateConfiguredAudienceModel` por segundo

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `CreateTrainingDataset`	10 TPS	Número máximo de llamadas a la API `CreateTrainingDataset` por segundo
Tasa de solicitudes `DeleteAudienceGenerationJob`	Tasa de 2 TPS, ráfaga de 10 TPS	Número máximo de llamadas a la API `DeleteAudienceGenerationJob` por segundo
Tasa de solicitudes `DeleteAudienceModel`	Tasa de 2 TPS, ráfaga de 10 TPS	Número máximo de llamadas a la API `DeleteAudienceModel` por segundo
Tasa de solicitudes `DeleteConfiguredAudienceModel`	10 TPS	Número máximo de llamadas a la API `DeleteConfiguredAudienceModel` por segundo
Tasa de solicitudes `DeleteConfiguredAudienceModelPolicy`	25 TPS	Número máximo de llamadas a la API `DeleteConfiguredAudienceModelPolicy` por segundo
Tasa de solicitudes `DeleteTrainingDataset`	10 TPS	Número máximo de llamadas a la API `DeleteTrainingDataset` por segundo
Tasa de solicitudes `GetAudienceGenerationJob`	50 TPS	Número máximo de llamadas a la API `GetAudienceGenerationJob` por segundo

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `GetAudienceModel`	50 TPS	Número máximo de llamadas a la API `GetAudienceModel` por segundo
Tasa de solicitudes `GetConfiguredAudienceModel`	50 TPS	Número máximo de llamadas a la API `GetConfiguredAudienceModel` por segundo
Tasa de solicitudes `GetConfiguredAudienceModelPolicy`	50 TPS	Número máximo de llamadas a la API `GetConfiguredAudienceModelPolicy` por segundo
Tasa de solicitudes `GetTrainingDataset`	50 TPS	Número máximo de llamadas a la API `GetTrainingDataset` por segundo
Tasa de solicitudes `ListAudienceExportJobs`	50 TPS	Número máximo de llamadas a la API `ListAudienceExportJobs` por segundo
Tasa de solicitudes `ListAudienceGenerationJobs`	50 TPS	Número máximo de llamadas a la API `ListAudienceGenerationJobs` por segundo
Tasa de solicitudes `ListAudienceModels`	50 TPS	Número máximo de llamadas a la API `ListAudienceModels` por segundo
Tasa de solicitudes `ListConfiguredAudienceModels`	50 TPS	Número máximo de llamadas a la API `ListConfiguredAudienceModels` por segundo

Recurso	Límite de frecuencia	Descripción
Tasa de solicitudes `ListTagsForResource`	50 TPS	Número máximo de llamadas a la API `ListTagsForResource` por segundo
Tasa de solicitudes `ListTrainingDatasets`	50 TPS	Número máximo de llamadas a la API `ListTrainingDatasets` por segundo
Tasa de solicitudes `PutConfiguredAudienceModelPolicy`	25 TPS	Número máximo de llamadas a la API `PutConfiguredAudienceModelPolicy` por segundo
Tasa de solicitudes `StartAudienceExportJob`	Tasa de 1 TPS, ráfaga de 3 TPS	Número máximo de llamadas a la API `StartAudienceExportJob` por segundo
Tasa de solicitudes `StartAudienceGenerationJob`	Tasa de 1 TPS, ráfaga de 5 TPS	Número máximo de llamadas a la API `StartAudienceGenerationJob` por segundo
Tasa de solicitudes `TagResource`	10 TPS	Número máximo de llamadas a la API `TagResource` por segundo
Tasa de solicitudes `UntagResource`	50 TPS	Número máximo de llamadas a la API `UntagResource` por segundo
Tasa de solicitudes `UpdateConfiguredAudienceModel`	10 TPS	Número máximo de llamadas a la API `UpdateConfiguredAudienceModel` por segundo

Nombre	Valor predeterminado	Ajusta	Descripción
Trabajos de exportación de audiencia activa por trabajo de generación de audiencia	Cada región admitida: 25	No	El número máximo de trabajos de exportación de audiencia activa para un trabajo de generación de audiencia
Los trabajos de exportación de la audiencia pendientes o en curso por cliente	Cada región admitida: 20	No	El número máximo de trabajos de exportación pendientes o en curso por cliente
Trabajos de generación de audiencia pendientes o en curso por cliente	Cada región admitida: 10	Sí	El número máximo de trabajos de generación de audiencia pendientes o en curso por cliente
Modelos de audiencia pendientes o en curso por cliente	Cada región admitida: 2	Sí	El número máximo de trabajos de formación sobre modelos de audiencia pendientes o en curso por cliente

Cuotas de aprendizaje automático para salas limpias

Recurso	Predeterminado	Descripción
Conjuntos de datos	por trabajo	
Número máximo de interacciones	20 mil millones	Número máximo de interacciones permitidas en los datos de entrenamiento. Las entradas más grandes se muestrean.

Recurso	Predeterminado	Descripción
Número mínimo de interacciones	1 millón	
Número máximo de usuarios distintos para el entrenamiento de modelos similares	1 millón	Si se incluyen más, solo se utilizan los primeros 100 millones, ordenados por número de interacciones.
Número mínimo de usuarios distintos para el entrenamiento de modelos similares	100 000	
Número máximo de usuarios para exportar un trabajo de segmento similar (audiencia)	10 000	
Número máximo de elementos distintos que se utilizan para el entrenamiento de modelos.	1 millón	Puede incluir hasta 50 millones de artículos, pero solo se utiliza el 1 millón más popular.
Número máximo de columnas de características en el conjunto de datos de entrenamiento.	10	
Número mínimo de elementos distintos por usuario	2	AWS Clean Rooms El aprendizaje automático requiere que cada fila o usuario tenga dos o más elementos, incluidos los elementos repetidos.
Tamaño máximo de la audiencia inicial	500.000	

Recurso	Predeterminado	Descripción
Tamaño mínimo de la audiencia inicial	500	El proveedor de datos de entrenamiento puede establecer este valor tan bajo como 25.
API	por cliente	
Número total de conjuntos de datos de entrenamiento activos.	500	
Número total de modelos similares activos (modelos de audiencia)	500	
Número total de modelos similares configurados y activos (modelos de audiencia)	10 000	
Número total de trabajos de generación de segmentos similares (audiencia) completados	Sin límite	
Número total de trabajos de segmentos similares de exportación (audiencia) completados	Sin límite	
Duración máxima de un trabajo de generación de modelos similares (modelo de audiencia)	1 día (24 horas)	

Recurso	Predeterminado	Descripción
Duración máxima de un trabajo de generación de segmentos similares (audiencia)	10 horas	Tras proporcionar una semilla, Clean Rooms ML tarda un máximo de 10 horas en generar un segmento similar.
Porcentaje mínimo para el tamaño de la papelera de un segmento (audiencia)	1%	
Porcentaje máximo para el tamaño de la papelera de un segmento (audiencia)	20%	
Tamaño absoluto mínimo para el tamaño de la papelera de un segmento (audiencia)	El 1 % del número de usuarios distintos	
Tamaño absoluto máximo para el tamaño de la papelera de un segmento (audiencia)	El 20 % del número de usuarios distintos	

Historial de documentos de la Guía AWS Clean Rooms del usuario

En la siguiente tabla se describen las versiones de la documentación de AWS Clean Rooms.

Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a la fuente RSS. Para suscribirse a las actualizaciones RSS, debe tener un complemento de RSS habilitado para el navegador que esté utilizando.

Cambio	Descripción	Fecha
Actualización de una política existente	Se ha agregado el permiso nuevo siguiente a la política administrada `AWSCleanRoomsFullAccessNoQuerying` : `cleanrooms:BatchGetSchemaAnalysisRule` .	13 de mayo de 2024
AWS Clean Rooms ML ya está completamente disponible	AWS Clean Rooms El aprendizaje automático proporciona un método que mejora la privacidad para que dos partes identifiquen a usuarios similares en sus datos sin necesidad de compartir sus datos entre sí.	3 de abril de 2024
Actualización de una política existente	El identificador de la declaración de la política `AWSCleanRoomsFullAccess` gestionada se ha actualizado de ConsolePickQueryResultsBucket SetQueryResultsBucket a para represent	21 de marzo de 2024

	ar mejor los permisos desde los permisos.	
Nuevas políticas gestionadas para el aprendizaje AWS Clean Rooms automático	Se han añadido dos nuevas políticas administradas: `AWSCleanRoomsMLReadOnlyAccess` y `AWSCleanRoomsMLFullAccess`.	29 de noviembre de 2023
AWS Clean Rooms ML (versión preliminar)	AWS Clean Rooms El aprendizaje automático proporciona un método que mejora la privacidad para que dos partes identifiquen a usuarios similares en sus datos sin necesidad de compartir sus datos entre sí.	29 de noviembre de 2023
AWS Clean Rooms Privacidad diferencial (versión preliminar)	Los clientes ahora pueden usar AWS Clean Rooms Differential Privacy para ayudar a proteger la privacidad de sus usuarios.	29 de noviembre de 2023
Configuración de pagos	El creador de la colaboración ahora puede designar al miembro que puede ejecutar consultas o a otro miembro de la colaboración para que se le facturen los costos de computación de las consultas.	14 de noviembre de 2023
Tiempo de ejecución de consulta: actualización	El tiempo máximo que se ejecuta una consulta antes de que se agote el tiempo de espera se ha actualizado de 4 a 12 horas.	6 de octubre de 2023

AWS CloudFormation recursos: actualización	AWS Clean Rooms ha agregado los siguiente s recursos nuevos: `AWS::CleanRooms::M embership Protected QueryOutputConfigu ration AWS::Clea nRooms::Membership ProtectedQueryResu ltConfiguration , yAWS::CleanRooms::M embership Protected QueryS3OutputConfi guration .`	7 de septiembre de 2023
AWS CloudFormation recursos: actualizar	AWS Clean Rooms ha añadido los siguientes recursos nuevos: `AWS::Clea nRooms::AnalysisTe mplate yAWS::Clea nRooms::Configured Table AnalysisR uleCustom .`	31 de agosto de 2023
Capacidades independientes de los miembros	El creador de la colaborac ión ahora puede designar a un miembro que realice las consultas y a otro miembro que reciba los resultados. Esto permite al creador de la colaboración asegurarse de que el miembro que puede realizar las consultas no tenga acceso a los resultados de la consulta.	30 de agosto de 2023

AWS Clean Rooms Glosario	Actualización exclusiva de la documentación para añadir un glosario de términos. AWS Clean Rooms	30 de agosto de 2023
Compatibilidad para tablas de Apache Iceberg (vista previa)	AWS Clean Rooms ahora admite Apache Iceberg tablas (vista previa).	25 de agosto de 2023
Actualización de cuotas	La sección Cuotas se ha actualizado para reflejar la nueva cuota predeterminada de pertenencias por cuenta.	9 de agosto de 2023
Actualización de la política existente	Se han añadido los siguiente s nuevos permisos a la política administrada de `AWSCleanRoomsFullAccessNoQuerying` : `cleanrooms:CreateAnalysisTemplate` , `cleanrooms:GetAnalysisTemplate` , `cleanrooms:UpdateAnalysisTemplate` , `cleanrooms:DeleteAnalysisTemplate` , `cleanrooms:ListAnalysisTemplates` , `cleanrooms:GetCollaborationAnalysisTemplate` , `cleanrooms:BatchGetCollaborationAnalysisTemplate` y `cleanrooms:ListCollaborationAnalysisTemplates` .	31 de julio de 2023

Plantillas de análisis y regla de análisis personalizada	AWS Clean Rooms ahora admite plantillas de análisis y la regla de análisis personalizada. Las plantillas de análisis permiten a los colaboradores crear o importar su propia consulta SQL personalizada para utilizarla en la colaboración. Con la regla de análisis personalizada, el propietario de la tabla puede aprobar consultas SQL personalizadas en sus tablas configuradas.	31 de julio de 2023
Las reglas de análisis admiten la condición lógica `OR`	AWS Clean Rooms las reglas de análisis ahora admiten la condición `OR` lógica de la `JOIN` cláusula.	29 de junio de 2023
CloudFormation integración	AWS Clean Rooms ahora se integra con AWS CloudFormation.	15 de junio de 2023
Creador de análisis	Los miembros que pueden realizar consultas y recibir resultados ahora tienen la posibilidad de ejecutar consultas en algunas tablas sin escribir código SQL utilizando la interfaz de usuario del creador de análisis.	15 de junio de 2023
Funciones SQL	Actualización solo de la documentación para aclarar las funciones SQL admitidas.	5 de mayo de 2023

Solución de problemas	Actualización solo de la documentación para añadir una sección de solución de problemas para los problemas más frecuentes.	27 de abril de 2023
Tipos de datos compatibles para AWS Clean Rooms	Actualización exclusiva de la documentación para añadir una nueva sección que muestre los tipos de AWS Glue Data Catalog datos compatibles.	26 de abril de 2023
Ejemplos de eventos AWS CloudTrail	Actualización solo de la documentación para agregar ejemplos de CloudTrail eventos StartProtectedQuery (exitosos) y StartProtectedQuery (fallidos).	20 de abril de 2023
Actualización de la política existente	Se han añadido los siguientes nuevos permisos a la política administrada `AWSCleanRoomsFullAccessNoQuerying` : `cleanrooms:ListTagsForResource` , `cleanrooms:UntagResource` y `cleanrooms:TagResource` . Para obtener más información, consulte Políticas administradas de AWS.	21 de marzo de 2023
Disponibilidad general	AWS Clean Rooms ahora está disponible de forma general.	21 de marzo de 2023

Versión de prueba	Versión preliminar de la Guía AWS Clean Rooms del usuario	12 de enero de 2023

AWS Clean Rooms Glosario

Consulte este glosario para familiarizarse con la terminología utilizada en AWS Clean Rooms.

Regla de análisis de agregación

La restricción de consultas que permite realizar consultas que agreguen análisis utilizando funciones COUNT, SUM o AVG en dimensiones opcionales. Estas consultas no revelarán información de nivel de fila.

Admite casos de uso como la planificación de campañas, el alcance mediático, la frecuencia y la medición de conversiones.

Otros tipos de reglas de análisis son las personalizadas y las de lista.

Reglas de análisis

Las restricciones de consulta que autorizan un tipo específico de consulta.

El tipo de regla de análisis determina qué tipo de análisis se puede ejecutar en la tabla configurada. Cada tipo tiene una estructura de consulta predefinida. Usted controla cómo se pueden utilizar las columnas de la tabla en la estructura mediante los controles de consulta.

Los tipos de reglas de análisis son de agregación, de lista y personalizadas.

Plantilla de análisis

Una consulta preaprobada y específica de la colaboración que se puede reutilizar.

Admite consultas SQL personalizadas compatibles en. AWS Clean Rooms

Puede contener parámetros en cualquier lugar donde normalmente aparecería un valor literal en una consulta SQL. Para obtener más información sobre los tipos de parámetros admitidos, consulte Tipos de datos en la Referencia de SQL de AWS Clean Rooms .

Las plantillas de análisis solo funcionan con la regla de análisis personalizada.

Cliente de cifrado de S3

El cliente de cifrado de computación criptográfica para Clean Rooms (C3R).

C3R, que se utiliza para cifrar y descifrar datos, es un SDK de cifrado del cliente con una interfaz de línea de comandos.

Columna de texto sin cifrar

Columna que no está protegida criptográficamente para un constructo SQL JOIN ni SELECT

Las columnas de texto sin cifrar se pueden usar en cualquier parte de la consulta SQL.

Colaboración

Un límite lógico seguro AWS Clean Rooms en el que los miembros pueden realizar consultas SQL en tablas configuradas.

Las colaboraciones las crea el creador de la colaboración.

Solo los miembros que hayan sido invitados a la colaboración pueden unirse a ella.

Una colaboración solo puede tener un miembro que pueda realizar consultas de datos, un miembro que pueda recibir los resultados y un miembro que pague los costos de computación de las consultas.

Todos los miembros pueden ver la lista de participantes invitados a la colaboración antes de unirse a ella.

Creador de la colaboración

El miembro que crea una colaboración.

Solo hay un creador por colaboración.

El creador de la colaboración es el único que puede eliminar miembros de la colaboración o eliminar la colaboración.

Tabla configurada

Cada tabla configurada representa una referencia a una tabla existente en la AWS Glue Data Catalog que se ha configurado para su uso en AWS Clean Rooms. Una tabla configurada contiene una regla de análisis que determina cómo se pueden utilizar los datos.

Actualmente, AWS Clean Rooms admite la asociación de datos almacenados en Amazon Simple Storage Service (Amazon S3) que están catalogados mediante. AWS Glue

Para obtener más información al respecto AWS Glue, consulte la Guía para AWS Glue desarrolladores.

Las tablas configuradas se pueden asociar a una o más colaboraciones.

> **Note**
>
> AWS Clean Rooms actualmente no admite las ubicaciones de bucket de Amazon S3 en las que esté registrado AWS Lake Formation.

Regla de análisis personalizada

La restricción de consultas que permite un conjunto específico de consultas previamente aprobadas (plantillas de análisis) o que permite que un conjunto específico de cuentas pueda realizar consultas que utilicen sus datos.

Admite casos de uso como la atribución de primer toque, los análisis incrementales y los análisis de detección de audiencia.

Admite la privacidad diferencial.

Descifrado

El proceso de transformar los datos cifrados para devolverles su forma original. El descifrado solo se puede realizar si se tiene el acceso a la clave secreta.

Privacidad diferencial

Una técnica matemáticamente rigurosa que protege los datos de la colaboración para que el miembro pueda obtener resultados al aprender sobre una persona específica.

Cifrado

Proceso de codificación de datos en un formato aparentemente aleatorio utilizando un valor secreto denominado clave. Es imposible determinar el texto sin formato original sin tener acceso a la clave.

Columna de huella digital

Columna protegida criptográficamente para un constructo SQL JOIN.

Regla de análisis de lista

La restricción de consultas que permite realizar consultas que generen un análisis de atributos de nivel de fila del solapamiento entre esta tabla y las tablas del miembro que puede realizar consultas.

Admite casos de uso como el enriquecimiento y la creación o supresión de audiencias.

Miembro

Un AWS cliente que participa en una colaboración.

Un miembro se identifica mediante su Cuenta de AWS.

Todos los miembros pueden contribuir con datos.

Miembro que puede realizar consultas

El miembro que puede consultar los datos de la colaboración.

Solo hay un miembro que puede realizar consultas por colaboración y ese miembro es inmutable.

Un usuario administrativo puede usar los permisos AWS Identity and Access Management (de IAM) para controlar cuáles de sus directores de IAM (como los usuarios o las funciones) pueden consultar los datos de la colaboración. Para obtener más información, consulte Creación de rol de servicio para leer datos.

Miembro que puede recibir los resultados

El miembro que puede recibir los resultados de la consulta. El miembro que puede recibir los resultados especifica la configuración de los resultados de consulta para el destino de Amazon S3 y el formato de los resultados de la consulta.

Solo hay un miembro que puede recibir los resultados por colaboración y ese miembro es inmutable.

Miembro que paga los costos de computación de consultas

El miembro responsable de pagar los costos de computación de consultas.

Solo hay un miembro responsable de pagar los costos de computación de consultas por colaboración, y ese miembro es inmutable.

Si el creador de la colaboración no ha designado a nadie como miembro que paga los costos de computación de consultas, el miembro que puede realizar consultas es el pagador predeterminado.

El miembro que paga los costos de computación de las consultas recibe una factura por las consultas que se han ejecutado en la colaboración.

Pertenencia

Un recurso que se crea cuando un miembro se une a una colaboración.

Todos los recursos que el miembro asocia a una colaboración forman parte de la pertenencia o están asociados a ella.

Solo el miembro propietario de la pertenencia puede añadir, eliminar o editar los recursos de esa pertenencia.

Columna sellada

Columna protegida criptográficamente para un constructo SQL SELECT.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.