Panduan Pengguna

AWS Clean Rooms

AWS Clean Rooms: Panduan Pengguna

Table of Contents

Apa itu AWS Clean Rooms?

AWS Clean Rooms membantu Anda dan mitra Anda menganalisis dan berkolaborasi dalam kumpulan data kolektif Anda untuk mendapatkan wawasan baru tanpa mengungkapkan data yang mendasarinya satu sama lain. Anda dapat menggunakan AWS Clean Rooms, ruang kerja kolaborasi yang aman, untuk membuat kamar bersih Anda sendiri dalam hitungan menit, dan mulai menganalisis kumpulan data kolektif Anda hanya dengan beberapa langkah. Anda dapat memilih mitra yang ingin Anda ajak berkolaborasi, memilih kumpulan data mereka, dan mengonfigurasi batasan untuk peserta.

Dengan AWS Clean Rooms, Anda dapat berkolaborasi dengan ribuan perusahaan yang sudah menggunakan AWS. Kolaborasi tidak memerlukan pemindahan data dari AWS atau memuatnya ke platform lain. Saat Anda menjalankan kueri, AWS Clean Rooms membaca data dari lokasi aslinya dan menerapkan aturan analisis bawaan untuk membantu Anda mempertahankan kontrol atas datanya.

AWS Clean Rooms menyediakan kontrol akses data bawaan dan kontrol dukungan audit yang dapat Anda konfigurasi. Kontrol ini meliputi:

- Aturan analisis untuk membatasi kueri SQL dan memberikan kendala keluaran
- Komputasi Kriptografi Clean Rooms untuk menjaga data terenkripsi, bahkan saat kueri diproses, untuk mematuhi kebijakan penanganan data yang ketat
- Log kueri untuk meninjau kueri dan membantu mendukung audit
- Privasi diferensial untuk melindungi dari upaya identifikasi pengguna. AWS Clean Rooms Privasi Diferensial adalah kemampuan yang dikelola sepenuhnya yang melindungi privasi pengguna Anda dengan teknik yang didukung secara matematis dan kontrol intuitif yang dapat Anda terapkan dalam beberapa klik.
- AWS Clean Rooms ML memungkinkan dua pihak untuk mengidentifikasi pengguna serupa dalam data mereka tanpa perlu berbagi data mereka satu sama lain. Pihak pertama membuat dan mengonfigurasi model yang mirip dari data pelatihan mereka. Pihak kedua membawa data benih mereka ke kolaborasi dan menciptakan segmen mirip yang menyerupai data pelatihan.

Video berikut menjelaskan lebih lanjut tentang AWS Clean Rooms.

AWS Clean Rooms

Apakah Anda AWS Clean Rooms pengguna pertama kali?

Jika Anda adalah pengguna pertama kali AWS Clean Rooms, kami sarankan Anda mulai dengan membaca bagian berikut:

- Bagaimana cara AWS Clean Rooms kerja
- Mengakses AWS Clean Rooms
- Menyiapkan AWS Clean Rooms
- AWS Clean Rooms Glosarium

Bagaimana cara AWS Clean Rooms kerja

Alur kerja berikut mengasumsikan bahwa:

- Anggota kolaborasi telah mengunggah tabel data mereka ke Amazon S3 dan membuat AWS Glue tabel.
- (Opsional) Hanya untuk tabel data terenkripsi, anggota kolaborasi telah menyiapkan tabel data terenkripsi menggunakan klien enkripsi C3R.

Singkatnya, alur kerja untuk AWS Clean Rooms adalah sebagai berikut:

1. Pembuat kolaborasi melakukan tugas-tugas berikut:
   - Menciptakan kolaborasi.
   - Mengundang satu atau lebih anggota untuk kolaborasi.
   - Menetapkan kemampuan kepada anggota, seperti anggota yang dapat meminta dan anggota yang dapat menerima hasil.

     Jika pembuat kolaborasi juga anggota yang dapat menerima hasil, mereka menentukan tujuan dan format hasil kueri. Mereka juga menyediakan peran layanan Amazon Resource Name (ARN) untuk menulis hasil ke tujuan hasil kueri.
   - Mengkonfigurasi anggota mana yang bertanggung jawab untuk membayar biaya komputasi kueri dalam kolaborasi.
2. Anggota yang diundang bergabung dengan kolaborasi dengan membuat sumber daya keanggotaan.

Jika anggota yang diundang adalah anggota yang dapat menerima hasil, mereka menentukan tujuan dan format hasil kueri. Mereka juga menyediakan peran layanan ARN untuk menulis ke tujuan hasil kueri.

Jika anggota yang diundang adalah anggota yang bertanggung jawab untuk membayar biaya komputasi kueri, mereka menerima tanggung jawab pembayaran mereka sebelum bergabung dengan kolaborasi.

3. Anggota mengonfigurasi AWS Glue tabel yang ada untuk digunakan di AWS Clean Rooms. (Langkah ini dapat dilakukan sebelum atau sesudah bergabung dengan kolaborasi, kecuali menggunakan Cryptographic Computing untukClean Rooms.)

> **Note**
>
> AWS Clean Rooms mendukung AWS Glue tabel. Untuk informasi selengkapnya tentang memasukkan data Anda AWS Glue, lihatLangkah 3: Unggah tabel data Anda ke Amazon S3.

1. Anggota menamai tabel yang dikonfigurasi dan memilih kolom mana yang akan digunakan dalam kolaborasi.
2. Anggota mengonfigurasi salah satu aturan analisis berikut ke tabel yang dikonfigurasi:
   - Aturan analisis agregasi atau aturan analisis daftar — Untuk mengontrol jenis analisis yang dapat dijalankan di atas meja.
   - Aturan analisis kustom — Untuk mengizinkan serangkaian kueri tertentu yang telah disetujui sebelumnya atau kumpulan akun tertentu yang dapat memberikan kueri yang menggunakan data Anda. Memungkinkan anggota mengaktifkan privasi diferensial untuk melindungi dari upaya identifikasi pengguna.

> **Note**
>
> Anggota dapat mengonfigurasi aturan analisis kapan saja sebelum mereka mengaitkan tabel yang dikonfigurasi dengan kolaborasi.

4. Anggota mengaitkan tabel yang dikonfigurasi dengan kolaborasi dan memberikan AWS Clean Rooms peran layanan untuk mengakses AWS Glue tabel mereka.

> **Note**
>
> Peran layanan ini memiliki izin untuk tabel. Peran layanan hanya dapat diasumsikan AWS Clean Rooms untuk menjalankan kueri yang diizinkan atas nama anggota yang dapat melakukan kueri. Tidak ada anggota kolaborasi (selain pemilik data) yang memiliki akses ke tabel yang mendasarinya dalam kolaborasi. Pemilik data dapat mengaktifkan privasi diferensial untuk membuat tabel mereka tersedia untuk kueri oleh anggota lain.

5. Anggota yang dapat melakukan kueri menjalankan kueri SQL pada tabel yang dikonfigurasi.

   Pertanyaan hanya dapat dijalankan jika anggota yang bertanggung jawab untuk membayar biaya komputasi kueri telah bergabung dengan kolaborasi sebagai anggota aktif.

   Aturan analisis dan kendala keluaran diberlakukan secara otomatis. AWS Clean Rooms hanya mengembalikan hasil yang sesuai dengan aturan analisis yang ditentukan dalam Langkah 3.b.

   Untuk kueri pada data terenkripsi, anggota yang dapat menerima hasil menerima output terenkripsi dari AWS Clean Rooms itu harus didekripsi (lihat Langkah 8).
6. Anggota yang dapat menerima hasil akan meninjau hasilnya di AWS Clean Rooms konsol atau di bucket Amazon S3 yang mereka tentukan.
7. Anggota yang membayar biaya komputasi kueri dibebankan untuk kueri yang dijalankan dalam kolaborasi.
8. (Opsional) Hanya untuk tabel data terenkripsi, anggota yang dapat menerima hasil mendekripsi hasil kueri dengan menjalankan klien enkripsi C3R dalam mode dekripsi.

Layanan terkait

Layanan AWS Berikut ini terkait dengan AWS Clean Rooms:

- Amazon S3

  Anggota kolaborasi dapat menyimpan data yang mereka bawa AWS Clean Rooms di Amazon S3.

  Untuk informasi selengkapnya, lihat topik berikut.

  Mempersiapkan tabel data untuk kueri di AWS Clean Rooms

  Apa itu Amazon S3? di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon

- AWS Glue

  Anggota kolaborasi dapat membuat AWS Glue tabel dari data mereka di Amazon S3 untuk digunakan. AWS Clean Rooms

  Untuk informasi selengkapnya, lihat topik berikut.

  Mempersiapkan tabel data untuk kueri di AWS Clean Rooms

  Apa itu AWS Glue? di Panduan Developer AWS Glue
- AWS CloudFormation

  Buat sumber daya berikut di AWS CloudFormation: kolaborasi, tabel yang dikonfigurasi, asosiasi tabel yang dikonfigurasi, dan keanggotaan

  Untuk informasi selengkapnya, lihat Menciptakan AWS Clean Rooms sumber daya dengan AWS CloudFormation.
- AWS CloudTrail

  Gunakan AWS Clean Rooms dengan CloudTrail log untuk meningkatkan analisis Layanan AWS aktivitas Anda.

  Untuk informasi selengkapnya, lihat Mencatat panggilan API AWS Clean Rooms menggunakan AWS CloudTrail.

Mengakses AWS Clean Rooms

Anda dapat mengakses AWS Clean Rooms melalui opsi berikut:

- Langsung melalui AWS Clean Rooms konsol di https://console.aws.amazon.com/cleanrooms/.
- Secara terprogram melalui API. AWS Clean Rooms Untuk informasi lebih lanjut, lihat Referensi API AWS Clean Rooms .

Harga untuk AWS Clean Rooms

Untuk informasi harga, lihat Harga AWS Clean Rooms.

Tagihan untuk AWS Clean Rooms

AWS Clean Rooms memberi pembuat kolaborasi kemampuan untuk mengonfigurasi anggota mana yang membayar biaya komputasi kueri dalam kolaborasi.

Dalam kebanyakan kasus, anggota yang dapat menanyakan dan anggota yang membayar biaya komputasi kueri adalah sama. Namun, jika anggota yang dapat melakukan kueri dan anggota yang membayar biaya komputasi kueri berbeda, maka, ketika anggota yang dapat melakukan kueri menjalankan kueri terhadap sumber daya keanggotaan mereka sendiri, sumber daya keanggotaan anggota yang membayar biaya komputasi kueri akan ditagih.

Anggota yang membayar biaya komputasi kueri tidak melihat peristiwa apa pun untuk kueri yang dijalankan dalam riwayat CloudTrail Acara mereka karena pembayar bukanlah orang yang menjalankan kueri maupun pemilik sumber daya tempat kueri dijalankan. Namun, pembayar memang melihat tagihan yang dihasilkan pada sumber daya keanggotaan mereka untuk semua kueri yang dijalankan oleh anggota yang dapat menjalankan kueri dalam kolaborasi.

Untuk informasi selengkapnya tentang cara membuat kolaborasi dan mengonfigurasi anggota yang membayar biaya komputasi kueri, lihatBuat kolaborasi.

Aturan analisis di AWS Clean Rooms

Sebagai bagian dari mengaktifkan tabel untuk digunakan AWS Clean Rooms untuk analisis kolaborasi, anggota kolaborasi harus mengonfigurasi aturan analisis.

Aturan analisis adalah kontrol peningkatan privasi yang disiapkan oleh setiap pemilik data pada tabel yang dikonfigurasi. Aturan analisis menentukan bagaimana tabel yang dikonfigurasi dapat dianalisis.

Aturan analisis adalah kontrol tingkat akun pada tabel yang dikonfigurasi (sumber daya tingkat akun) dan diberlakukan dalam kolaborasi apa pun di mana tabel yang dikonfigurasi dikaitkan. Jika tidak ada aturan analisis yang dikonfigurasi, tabel yang dikonfigurasi dapat dikaitkan dengan kolaborasi tetapi tidak dapat ditanyakan. Kueri hanya dapat mereferensikan tabel yang dikonfigurasi dengan jenis aturan analisis yang sama.

Untuk mengonfigurasi aturan analisis, pertama-tama Anda memilih jenis analisis dan kemudian menentukan aturan analisis. Untuk kedua langkah tersebut, Anda harus mempertimbangkan kasus penggunaan yang ingin Anda aktifkan dan bagaimana Anda ingin melindungi data yang mendasarinya.

AWS Clean Rooms memberlakukan kontrol yang lebih ketat di semua tabel yang dikonfigurasi yang direferensikan dalam kueri.

Contoh berikut menggambarkan kontrol restriktif.

Example Kontrol restriktif: Kendala keluaran

- Kolaborator A memiliki kendala keluaran pada kolom pengidentifikasi 100.
- Kolaborator B memiliki kendala keluaran pada kolom pengidentifikasi 150.

  Kueri agregasi yang mereferensikan kedua tabel yang dikonfigurasikan memerlukan setidaknya 150 nilai pengidentifikasi yang berbeda dalam baris keluaran agar dapat ditampilkan dalam output kueri. Output kueri tidak menunjukkan bahwa hasil dihapus karena kendala keluaran.

Example Kontrol restriktif: Template analisis tidak disetujui

- Kolaborator A telah mengizinkan templat analisis dengan kueri yang mereferensikan tabel yang dikonfigurasi dari Kolaborator A dan Kolaborator B dalam aturan analisis kustom mereka.
- Kolaborator B tidak mengizinkan template analisis.

Karena Collaborator B tidak mengizinkan templat analisis, anggota yang dapat melakukan kueri tidak dapat menjalankan templat analisis tersebut.

Jenis aturan analisis

Ada tiga jenis aturan analisis: agregasi, daftar, dan kustom. Tabel berikut membandingkan jenis aturan analisis. Setiap jenis memiliki bagian terpisah yang menjelaskan menentukan aturan analisis.

Tabel berikut menunjukkan ringkasan perbandingan jenis aturan analisis.

Kasus penggunaan yang didukung

Tabel berikut menunjukkan ringkasan perbandingan kasus penggunaan yang didukung untuk setiap jenis aturan analisis.

Kasus penggunaan	Agregasi	Daftar	Kustom
Analisis yang didukung	Kueri yang menggabungkan statistik menggunakan fungsi COUNT, SUM, dan AVG sepanjang dimensi opsional	Kueri yang menampilkan daftar tingkat baris dari tumpang tindih antara beberapa tabel	Analisis kustom apa pun selama templat analisis atau pembuat analisis telah ditinjau dan diizinkan
Kasus penggunaan umum	Analisis segmen, pengukuran, atribusi	Pengayaan, pembangunan segmen	Atribusi sentuhan pertama, analisis inkrement

Kasus penggunaan	Agregasi	Daftar	Kustom
			al, penemuan audiens
Konstruksi SQL	• Pernyataan JOIN: INNER JOIN • Fungsi agregat: COUNT/ COUNT DISTINCT, SUM/ SUM DISTINCT, dan AVG • Fungsi skalar: Subset terbatas	• Pernyataan JOIN: INNER JOIN • Fungsi skalar: Tidak ada	Mayoritas fungsi SQL dan konstruksi SQL tersedia dengan perintah SELECT
Subkueri dan ekspresi tabel umum (CTE)	Tidak	Tidak	Ya
Template analisis	Tidak	Tidak	Ya

Kontrol yang didukung

Tabel berikut menunjukkan ringkasan perbandingan bagaimana setiap jenis aturan analisis melindungi data dasar Anda.

Pengendalian	Agregasi	Daftar	Kustom
Mekanisme kontrol	Kontrol bagaimana data dalam tabel dapat digunakan dalam kueri (Misalnya, izinkan COUNT dan SUM kolom hashed_email.)	Kontrol bagaimana data dalam tabel dapat digunakan dalam kueri (Misalnya, izinkan penggunaan kolom hashed_email hanya untuk bergabung.)	Kontrol kueri apa yang diizinkan untuk berjalan di atas meja (Misalnya, izinkan hanya kueri yang ditentukan dalam templat analisis “Kueri khusus 1".)
Teknik peningkatan privasi bawaan	• Pertandingan buta • Diperlukan agregasi • Ambang agregasi min >= • 2 Struktur kueri	• Pertandingan buta • Diperlukan tumpang tindih • Struktur kueri yang telah	Privasi diferensial

Pengendalian	Agregasi	Daftar	Kustom
	yang telah ditentukan sebelumnya	ditentukan sebelumnya	
Tinjau kueri sebelum dapat dijalankan	Tidak	Tidak	Ya, menggunakan templat analisis

Untuk informasi selengkapnya tentang aturan analisis yang tersedia AWS Clean Rooms, lihat topik berikut.

- Aturan analisis agregasi
- Aturan analisis daftar
- Aturan analisis kustom di AWS Clean Rooms

Aturan analisis agregasi

DalamAWS Clean Rooms, aturan analisis agregasi menghasilkan statistik agregat menggunakan fungsi COUNT, SUM, dan/atau AVG di sepanjang dimensi opsional. Ketika aturan analisis agregasi ditambahkan ke tabel yang dikonfigurasi, ini memungkinkan anggota yang dapat melakukan kueri untuk menjalankan kueri pada tabel yang dikonfigurasi.

Aturan analisis agregasi mendukung penggunaan kasus seperti perencanaan kampanye, jangkauan media, pengukuran frekuensi, dan atribusi.

Struktur kueri dan sintaks yang didukung didefinisikan dalamStruktur kueri agregasi dan sintaks.

Parameter aturan analisis, yang didefinisikan dalamAturan analisis agregasi - kontrol kueri, termasuk kontrol kueri dan kontrol hasil kueri. Kontrol kuerinya mencakup kemampuan untuk mengharuskan tabel yang dikonfigurasi digabungkan ke setidaknya satu tabel yang dikonfigurasi yang dimiliki

oleh anggota yang dapat melakukan kueri, baik secara langsung maupun transitif. Persyaratan ini memungkinkan Anda untuk memastikan bahwa kueri dijalankan di persimpangan (INNERJOIN) tabel Anda dan mereka.

Struktur kueri agregasi dan sintaks

Kueri pada tabel yang memiliki aturan analisis agregasi harus mematuhi sintaks berikut.

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

Tabel berikut menjelaskan setiap ekspresi yang tercantum dalam sintaks sebelumnya.

Ekspresi	Definisi	Contoh-contoh
select_aggregate_function_expression	Daftar dipisahkan koma yang berisi ekspresi berikut:	`SELECT SUM(PRICE), user_segment`

Ekspresi	Definisi	Contoh-contoh
	• `select_aggregation_function_expression` • `select_aggregate_expression` **Note** Harus ada setidaknya satu `select_aggregation_function_expression` di `select_aggregate_expression`.	

Ekspresi	Definisi	Contoh-contoh

select_aggregation_function_expression	Satu atau lebih fungsi agregasi yang didukung diterapkan pada satu atau beberapa kolom. Hanya kolom yang diizinkan sebagai argumen fungsi agregasi.
	
	Note
	Harus ada setidaknya satu `select_aggregation_function_expression` diselect_aggregate_expression .
		`AVG(PRICE)`
		
		`COUNT(DISTINCT user_id)`

Ekspresi	Definisi	Contoh-contoh

select_grouping_column_expression	Ekspresi yang dapat berisi ekspresi apa pun menggunakan berikut ini:
	• Nama kolom tabel.
	• Fungsi skalar yang didukung
	• String literal
	• Literal numerik
	
	Note
	`select_aggregate_expression` dapat alias kolom dengan atau tanpa `AS` parameter. Untuk informasi selengkapnya, lihat Referensi AWS Clean Rooms SQL.
		`TRUNC(timestampColumn)`
		
		`UPPER(campaignName)`

Ekspresi	Definisi	Contoh-contoh
table_expression	Sebuah tabel, atau gabungan tabel, menghubungkan menggabungkan ekspresi kondisional dengan`join_condition` . `join_condition` mengembalikan Boolean. `table_expression` Dukungan: • JOINTipe tertentu (INNERJOIN) • Kondisi perbandingan kesetaraan dalam a `join_condition` () = • Operator logis (AND,OR).	`FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2`

Ekspresi	Definisi	Contoh-contoh

where_expression	Ekspresi kondisional yang mengembalikan Boolean. Ini mungkin terdiri dari yang berikut:
	• Nama kolom tabel.
	• Fungsi skalar yang didukung
	• Operator matematika
	• String literal
	• Literal numerik
	
	Kondisi perbandingan yang didukung adalah (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Operator logika yang didukung adalah (`AND, OR`).
	
	`where_expression` Itu opsional.
		`WHERE where_condition`
		
		`WHERE price > 100`
		
		`WHERE TRUNC(timestampColumn) = '1/1/2022'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

group_by_expression	Daftar ekspresi yang dipisahkan koma yang cocok dengan persyaratan untuk. `select_grouping_column_expression`	`GROUP BY TRUNC(timestampColumn), UPPER(campaignName), segment`

Ekspresi	Definisi	Contoh-contoh
having_expression	Ekspresi kondisional yang mengembalikan Boolean. Mereka memiliki fungsi agregasi yang didukung diterapkan ke satu kolom (misalnya,`SUM(price)`) dan dibandingkan dengan literal numerik. Kondisi yang didukung adalah (`=, >, <, <=, >=, <>, !=`). Operator logika yang didukung adalah (`AND, OR`). `having_expression` Itu opsional.	`HAVING SUM(SALES) > 500`

Ekspresi	Definisi	Contoh-contoh
order_by_expression	Daftar ekspresi yang dipisahkan koma yang kompatibel dengan persyaratan yang sama yang ditentukan dalam `select_aggregate_expression` didefinisikan sebelumnya. `order_by_expression` Itu opsional. **Note** `order_by_expression` izin `ASC` dan `DESC` parameter. Untuk informasi selengkapnya, lihat parameter ASC DESC di Referensi AWS Clean RoomsSQL.	`ORDER BY SUM(SALES), UPPER(campaignName)`

Untuk struktur kueri agregasi dan sintaks, perhatikan hal berikut:

- Perintah SQL selain SELECT tidak didukung.
- Sub-kueri dan ekspresi tabel umum (misalnya,WITH) tidak didukung.
- Operator yang menggabungkan beberapa kueri (misalnya,UNION) tidak didukung.
- TOP,LIMIT, dan OFFSET parameter tidak didukung.

Aturan analisis agregasi - kontrol kueri

Dengan kontrol kueri agregasi, Anda dapat mengontrol bagaimana kolom dalam tabel Anda digunakan untuk menanyakan tabel. Misalnya, Anda dapat mengontrol kolom mana yang digunakan untuk bergabung, kolom mana yang dapat dihitung, atau kolom mana yang dapat digunakan dalam WHERE pernyataan.

Bagian berikut menjelaskan setiap kontrol.

Topik

Kontrol agregasi

Dengan menggunakan kontrol agregasi, Anda dapat menentukan fungsi agregasi mana yang akan diizinkan, dan kolom apa yang harus diterapkan. Fungsi agregasi dapat digunakan dalamSELECT,HAVING, dan ORDER BY ekspresi.

Pengendalian	Definisi	Penggunaan
`aggregateColumns`	Kolom kolom tabel dikonfigurasi yang Anda izinkan untuk digunakan dalam fungsi agregasi.	`aggregateColumns` dapat digunakan di dalam fungsi agregasi diSELECT,HAVING, dan ORDER BY ekspresi. Beberapa juga `aggregateColumns` dapat dikategorikan sebagai `joinColumn` (didefinisikan nanti). Diberikan tidak `aggregateColumn` dapat juga dikategorikan sebagai `dimensionColumn` (didefinisikan nanti).

Pengendalian	Definisi	Penggunaan
`function`	Fungsi COUNT, SUM, dan AVG yang Anda izinkan untuk digunakan di atas. `aggregateColumns`	`function`dapat diterapkan pada `aggregateColumns` yang terkait dengannya.

Bergabunglah dengan kontrol

Sebuah `JOIN` klausa digunakan untuk menggabungkan baris dari dua atau lebih tabel, berdasarkan kolom terkait di antara mereka.

Anda dapat menggunakan kontrol Gabung untuk mengontrol bagaimana tabel Anda dapat digabungkan ke tabel lain di`table_expression`. AWS Clean Roomshanya mendukung INNERJOIN. INNERJOINpernyataan hanya dapat menggunakan kolom yang secara eksplisit dikategorikan sebagai `joinColumn` aturan analisis Anda, tunduk pada kontrol yang Anda tentukan.

INNERJOINHarus beroperasi pada `joinColumn` dari tabel yang dikonfigurasi dan `joinColumn` dari tabel lain yang dikonfigurasi dalam kolaborasi. Anda memutuskan kolom mana dari tabel Anda dapat digunakan sebagai`joinColumn`.

Setiap kondisi kecocokan dalam ON klausa diperlukan untuk menggunakan kondisi perbandingan kesetaraan (=) antara dua kolom.

Beberapa kondisi pertandingan dalam suatu ON klausa dapat berupa:

- Dikombinasikan menggunakan operator `AND` logis
- Dipisahkan menggunakan operator `OR` logis

> **Note**
>
> Semua kondisi JOIN pertandingan harus cocok dengan satu baris dari setiap sisiJOIN. Semua kondisional yang dihubungkan oleh `OR` atau operator `AND` logis harus mematuhi persyaratan ini juga.

Berikut ini adalah contoh dari query dengan operator `AND` logis.

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

Berikut ini adalah contoh dari query dengan operator OR logis.

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

Pengendalian	Definisi	Penggunaan
`joinColumns`	Kolom (jika ada) yang ingin Anda izinkan anggota yang dapat kueri untuk digunakan dalam INNER JOIN pernyataan.	Spesifik juga `joinColumn` dapat dikategorikan sebagai `aggregateColumn` (lihatKontrol agregasi). Kolom yang sama tidak dapat digunakan sebagai `joinColumn` dan `dimensionColumns` (lihat nanti). Kecuali itu juga telah dikategorikan sebagai`aggregateColumn`, a tidak `joinColumn` dapat digunakan di bagian lain dari kueri selain. INNER JOIN
`joinRequired`	Kontrol apakah Anda memerlukan tabel INNER JOIN yang dikonfigurasi dari anggota yang dapat melakukan kueri.	Jika Anda mengaktifkan parameter ini, INNER JOIN diperlukan. Jika Anda tidak mengaktifkan parameter ini, INNER JOIN adalah opsional.

Pengendalian	Definisi	Penggunaan
		Dengan asumsi Anda mengaktifkan parameter ini, anggota yang dapat melakukan kueri diminta untuk menyertakan tabel yang mereka miliki di INNERJOIN . Mereka harus meja JOIN Anda dengan mereka, baik secara langsung atau transitif (yaitu, menggabungkan meja mereka ke meja lain, yang dengan sendirinya bergabung dengan meja Anda).

Berikut ini adalah contoh transitivitas.

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

> **Note**
>
> Anggota yang dapat melakukan query juga dapat menggunakan `joinRequired` parameter. Dalam hal ini, kueri harus menggabungkan tabel mereka dengan setidaknya satu tabel lainnya.

Kontrol dimensi

Kontrol dimensi mengontrol kolom di mana kolom agregasi dapat disaring, dikelompokkan, atau digabungkan.

Pengendalian	Definisi	Penggunaan
`dimensionColumns`	Kolom (jika ada) yang Anda izinkan anggota yang dapat kueri untuk digunakanSELECT,WHERE, GROUPBY, dan ORDERBY.	A `dimensionColumn` dapat digunakan dalam SELECT (`select_grouping_column_expression`),WHERE, GROUPBY, dan ORDERBY. Kolom yang sama tidak bisa berupa a`dimensionColumn` , a`joinColumn` , dan/atau a`aggregateColumn` .

Fungsi skalar

Fungsi skalar mengontrol fungsi skalar mana yang dapat digunakan pada kolom dimensi.

Pengendalian	Definisi	Penggunaan
`scalarFunctions`	Fungsi skalar yang dapat digunakan `dimensionColumns` dalam kueri.	Menentukan fungsi skalar (jika ada) yang Anda izinkan (misalnya,CAST) untuk diterapkan pada. `dimensionColumns` Fungsi skalar tidak dapat digunakan di atas fungsi lain atau di dalam fungsi lainnya. Argumen fungsi skalar dapat berupa kolom, literal string, atau literal numerik.

Fungsi skalar berikut didukung:

- Fungsi matematika - ABS, CEILING, FLOOR, LOG, LN, ROUND, SQRT
- Fungsi pemformatan tipe data - CAST, CONVERT, TO_CHAR, TO_DATE, TO_NUMBER, TO_TIMESTAMP
- Fungsi string - BAWAH, ATAS, TRIM, RTRIM, SUBSTRING
  - Untuk RTRIM, set karakter khusus untuk dipangkas tidak diperbolehkan.
- Ekspresi bersyarat - COALESCE
- Fungsi tanggal - EXTRACT, GETDATE, CURRENT_DATE, DATEADD
- Fungsi lainnya - TRUNC

Untuk detail selengkapnya, lihat Referensi AWS Clean Rooms SQL.

Aturan analisis agregasi - kontrol hasil kueri

Dengan kontrol hasil kueri agregasi, Anda dapat mengontrol hasil mana yang dikembalikan dengan menentukan satu atau beberapa kondisi yang harus dipenuhi oleh setiap baris keluaran agar dapat dikembalikan. AWS Clean Roomsmendukung kendala agregasi dalam bentuk. `COUNT (DISTINCT column) >= X` Formulir ini mengharuskan setiap baris menggabungkan setidaknya X nilai pilihan yang berbeda dari tabel Anda yang dikonfigurasi (misalnya, jumlah minimum `user_id` nilai yang berbeda). Ambang batas minimum ini secara otomatis diberlakukan, bahkan jika kueri yang dikirimkan itu sendiri tidak menggunakan kolom yang ditentukan. Mereka diberlakukan secara kolektif di setiap tabel yang dikonfigurasi dalam kueri dari tabel yang dikonfigurasi dari setiap anggota dalam kolaborasi.

Setiap tabel yang dikonfigurasi harus memiliki setidaknya satu batasan agregasi dalam aturan analisisnya. Pemilik tabel yang dikonfigurasi dapat menambahkan beberapa `columnName` dan terkait `minimum` dan mereka ditegakkan secara kolektif.

Kendala agregasi

Batasan agregasi mengontrol baris mana dalam hasil kueri yang dikembalikan. Untuk dikembalikan, baris harus memenuhi jumlah minimum yang ditentukan dari nilai berbeda di setiap kolom yang ditentukan dalam batasan agregasi. Persyaratan ini berlaku bahkan jika kolom tidak disebutkan secara eksplisit dalam kueri atau di bagian lain dari aturan analisis.

Pengendalian	Definisi	Penggunaan
`columnName`	`aggregateColumn` Yang digunakan dalam kondisi bahwa setiap baris output harus memenuhi.	Dapat berupa kolom apa pun di tabel yang dikonfigurasi.
`minimum`	Jumlah minimum nilai berbeda untuk yang terkait `aggregate Column` yang harus dimiliki baris keluaran (misalnya , COUNT DISTINCT) agar dapat dikembalikan dalam hasil kueri.	Minimal `minimum` harus bernilai 2.

Struktur aturan analisis agregasi

Contoh berikut menunjukkan struktur yang telah ditetapkan untuk aturan analisis agregasi.

Dalam contoh berikut, *`MyTable`*mengacu pada tabel data Anda. Anda dapat mengganti setiap *`placeholder input pengguna dengan informasi`* Anda sendiri.

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

Aturan analisis agregasi - contoh

Contoh berikut menunjukkan bagaimana dua perusahaan dapat berkolaborasi dalam AWS Clean Rooms menggunakan analisis agregasi.

Perusahaan A memiliki data pelanggan dan penjualan. Perusahaan A tertarik untuk memahami aktivitas pengembalian produk. Perusahaan B adalah salah satu pengecer Perusahaan A dan memiliki data pengembalian. Perusahaan B juga memiliki atribut segmen pada pelanggan yang berguna bagi Perusahaan A (misalnya, membeli produk terkait, menggunakan layanan pelanggan dari pengecer). Perusahaan B tidak ingin memberikan data pengembalian pelanggan tingkat baris dan informasi atribut. Perusahaan B hanya ingin mengaktifkan serangkaian kueri untuk Perusahaan A untuk mendapatkan statistik agregat tentang pelanggan yang tumpang tindih pada ambang agregasi minimum.

Perusahaan A dan Perusahaan B memutuskan untuk berkolaborasi sehingga Perusahaan A dapat memahami aktivitas pengembalian produk dan memberikan produk yang lebih baik di Perusahaan B dan saluran lainnya.

Untuk membuat kolaborasi dan menjalankan analisis agregasi, perusahaan melakukan hal berikut:

1. Perusahaan A menciptakan kolaborasi dan menciptakan keanggotaan. Kolaborasi ini menjadikan Perusahaan B sebagai anggota lain dalam kolaborasi tersebut. Perusahaan A memungkinkan pencatatan kueri dalam kolaborasi, dan memungkinkan pencatatan kueri di akun mereka.
2. Perusahaan B menciptakan keanggotaan dalam kolaborasi. Ini memungkinkan pencatatan kueri di akunnya.
3. Perusahaan A membuat tabel penjualan yang dikonfigurasi.
4. Perusahaan A menambahkan aturan analisis agregasi berikut ke tabel yang dikonfigurasi penjualan.

```
{
  "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`Perusahaan A ingin menghitung jumlah pelanggan unik dalam tumpang tindih antara data penjualan dan data pengembalian. Perusahaan A juga ingin menjumlahkan jumlah yang `purchases` dibuat untuk dibandingkan dengan jumlah`returns`.

`joinColumns`— Perusahaan A ingin menggunakan `identifier` untuk mencocokkan pelanggan dari data penjualan ke pelanggan dari data pengembalian. Ini akan membantu perusahaan A match kembali ke pembelian yang tepat. Ini juga membantu segmen Perusahaan A tumpang tindih pelanggan.

`dimensionColumns`— Perusahaan A menggunakan `dimensionColumns` untuk memfilter berdasarkan produk tertentu, membandingkan pembelian dan pengembalian selama periode waktu tertentu, memastikan tanggal pengembalian setelah tanggal produk, dan membantu segmen pelanggan yang tumpang tindih.

`scalarFunctions`— Perusahaan A memilih fungsi `CAST` skalar untuk membantu memperbarui format tipe data jika diperlukan berdasarkan tabel yang dikonfigurasi Perusahaan A terkait dengan kolaborasi. Ini juga menambahkan fungsi skalar untuk membantu memformat kolom jika diperlukan.

`outputConstraints`— Perusahaan A menetapkan batasan output minimum. Tidak perlu membatasi hasil karena analis diizinkan untuk melihat data tingkat baris dari tabel penjualan mereka

> **Note**
>
> Perusahaan A tidak termasuk `joinRequired` dalam aturan analisis. Ini memberikan fleksibilitas bagi analis mereka untuk menanyakan tabel penjualan saja.

5. Perusahaan B membuat tabel yang dikonfigurasi pengembalian.
6. Perusahaan B menambahkan aturan analisis agregasi berikut ke tabel pengembalian yang dikonfigurasi.

```
{
  "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`— Perusahaan B memungkinkan Perusahaan A untuk menjumlahkan `returns` untuk dibandingkan dengan jumlah pembelian. Mereka memiliki setidaknya satu kolom agregat karena mereka mengaktifkan kueri agregat.

`joinColumns`— Perusahaan B memungkinkan Perusahaan A untuk bergabung `identifier` untuk mencocokkan pelanggan dari data pengembalian ke pelanggan dari data penjualan.

`identifier`data sangat sensitif dan memilikinya sebagai `joinColumn` memastikan bahwa data tidak akan pernah dikeluarkan dalam kueri.

`joinRequired`— Perusahaan B mengharuskan kueri pada data pengembalian agar tumpang tindih dengan data penjualan. Mereka tidak ingin mengaktifkan Perusahaan A untuk menanyakan semua individu dalam kumpulan data mereka. Mereka juga menyetujui pembatasan itu dalam perjanjian kolaborasi mereka.

`dimensionColumns`— Perusahaan B memungkinkan Perusahaan A untuk memfilter dan mengelompokkan berdasarkan `statepopularpurchases`,, dan `customerserviceuser` yang merupakan atribut unik yang dapat membantu membuat analisis untuk Perusahaan A. Perusahaan B memungkinkan Perusahaan A untuk menggunakan `returndate` untuk menyaring output pada `returndate` yang terjadi setelahnya`purchasedate`. Dengan penyaringan ini, output lebih akurat untuk mengevaluasi dampak perubahan produk.

`scalarFunctions`— Perusahaan B memungkinkan hal-hal berikut:

- TRUNC untuk tanggal
- LOWER dan UPPER jika `producttype` dimasukkan dalam format yang berbeda dalam data mereka
- CASTjika Perusahaan A perlu mengonversi tipe data dalam penjualan agar sama dengan tipe data dalam pengembalian

Perusahaan A tidak mengaktifkan fungsi skalar lainnya karena mereka tidak percaya bahwa mereka diperlukan untuk kueri.

`outputConstraints`Perusahaan B menetapkan batasan output minimum `hashedemail` untuk membantu mengurangi kemampuan untuk mengidentifikasi kembali pelanggan. Ini juga menambahkan kendala keluaran minimum `producttype` untuk mengurangi kemampuan mengidentifikasi kembali produk tertentu yang dikembalikan. Jenis produk tertentu bisa lebih dominan berdasarkan dimensi output (misalnya,`state`). Kendala output mereka akan selalu diberlakukan terlepas dari kendala output yang ditambahkan oleh Perusahaan A ke data mereka.

7. Perusahaan A menciptakan asosiasi tabel penjualan untuk kolaborasi.
8. Perusahaan B menciptakan asosiasi tabel pengembalian untuk kolaborasi.
9. Perusahaan A menjalankan kueri, seperti contoh berikut, untuk lebih memahami jumlah pengembalian di Perusahaan B dibandingkan dengan total pembelian berdasarkan lokasi pada tahun 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. Perusahaan A dan Perusahaan B meninjau log kueri. Perusahaan B memverifikasi bahwa kueri sejalan dengan apa yang disepakati dalam perjanjian kolaborasi.

Memecahkan masalah aturan analisis agregasi

Gunakan informasi di sini untuk membantu Anda mendiagnosis dan memperbaiki masalah umum saat Anda bekerja dengan aturan analisis agregasi.

Masalah

- Kueri saya tidak mengembalikan hasil apa pun

Kueri saya tidak mengembalikan hasil apa pun

Hal ini dapat terjadi ketika tidak ada hasil yang cocok atau ketika hasil yang cocok tidak memenuhi satu atau lebih ambang agregasi minimum.

Untuk informasi selengkapnya tentang ambang agregasi minimum, lihat. Aturan analisis agregasi - contoh

Aturan analisis daftar

DalamAWS Clean Rooms, aturan analisis daftar menampilkan daftar tingkat baris tumpang tindih antara tabel yang dikonfigurasi yang ditambahkan dan tabel yang dikonfigurasi dari anggota yang dapat melakukan kueri. Anggota yang dapat melakukan kueri menjalankan kueri yang menyertakan aturan analisis daftar.

Jenis aturan analisis daftar mendukung penggunaan kasus seperti pengayaan dan pembangunan audiens.

Untuk informasi selengkapnya tentang struktur kueri dan sintaks yang telah ditentukan untuk aturan analisis ini, lihat. Daftar aturan analisis struktur yang telah ditentukan

Parameter aturan analisis daftar, yang didefinisikan dalamAturan analisis daftar - kontrol kueri, memiliki kontrol kueri. Kontrol kuerinya mencakup kemampuan untuk memilih kolom yang dapat dicantumkan dalam output. Kueri diperlukan untuk memiliki setidaknya satu gabungan dengan tabel yang dikonfigurasi dari anggota yang dapat melakukan kueri, baik secara langsung maupun transitif.

Tidak ada kontrol hasil kueri seperti yang ada untuk aturan analisis Agregasi.

Kueri daftar hanya dapat menggunakan operator matematika. Mereka tidak dapat menggunakan fungsi lain (seperti agregasi atau skalar).

Topik

- Daftar struktur kueri dan sintaks
- Aturan analisis daftar - kontrol kueri
- Daftar aturan analisis struktur yang telah ditentukan
- Aturan analisis daftar - contoh

Daftar struktur kueri dan sintaks

Kueri pada tabel yang memiliki aturan analisis daftar harus mematuhi sintaks berikut.

```
--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]
```

Tabel berikut menjelaskan setiap ekspresi yang tercantum dalam sintaks sebelumnya.

Ekspresi	Definisi	Contoh-contoh
select_list_expression	Daftar dipisahkan koma yang berisi setidaknya satu nama kolom tabel. Diperlukan `DISTINCT` parameter. **Note** Kolom alias `select_list_expression` kaleng dengan atau tanpa `AS` parameter. Ini juga mendukung `TOP` parameter. Untuk informasi selengkapnya, lihat Referensi AWS Clean Rooms SQL.	`SELECT DISTINCT segment`
table_expression	Sebuah tabel, atau gabungan tabel, dengan `join_condition` untuk menghubungkannya`join_condition` . `join_condition` mengembalikan Boolean. `table_expression` Dukungan:	`FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2`

Ekspresi	Definisi	Contoh-contoh
	• Jenis JOIN tertentu (INNERJOIN) • Kondisi perbandingan kesetaraan dalam a `join_condition` () = • Operator logis (AND,OR).	

where_expression	Ekspresi kondisional yang mengembalikan Boolean. Ini dapat terdiri dari yang berikut:
	• Nama kolom tabel.
	• Operator matematika
	• String literal
	• Literal numerik
	
	Kondisi perbandingan yang didukung adalah (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Operator logika yang didukung adalah (`AND, OR`).
	
	`where_expression` Itu opsional.
		`WHERE state + '_' + city = 'NY_NYC'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

limit_expression	Ekspresi ini harus mengambil bilangan bulat positif. Itu juga dapat dipertukarkan dengan parameter TOP. `limit_expression` Itu opsional.	`LIMIT 100`

Untuk struktur kueri daftar dan sintaks, perhatikan hal berikut:

- Perintah SQL selain SELECT tidak didukung.
- Subkueri dan ekspresi tabel umum (misalnya,WITH) tidak didukung
- BYKlausul HAVING GROUPBY,, dan ORDER tidak didukung
- Parameter OFFSET tidak didukung

Aturan analisis daftar - kontrol kueri

Dengan kontrol kueri daftar, Anda dapat mengontrol bagaimana kolom dalam tabel Anda digunakan untuk menanyakan tabel. Misalnya, Anda dapat mengontrol kolom mana yang digunakan untuk bergabung, atau kolom mana yang dapat digunakan dalam pernyataan dan WHERE klausa SELECT.

Bagian berikut menjelaskan setiap kontrol.

Topik

Bergabunglah dengan kontrol

Dengan kontrol Gabung, Anda dapat mengontrol bagaimana tabel Anda dapat digabungkan ke tabel lain di table_expression. AWS Clean Roomshanya mendukung INNER JOIN. Dalam aturan analisis daftar, setidaknya satu INNER JOIN diperlukan dan anggota yang dapat melakukan kueri diminta untuk menyertakan tabel yang mereka miliki di INNER JOIN. Ini berarti mereka harus menggabungkan meja Anda dengan meja mereka, baik secara langsung maupun transitif.

Berikut ini adalah contoh transitivitas.

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

INNERPernyataan JOIN hanya dapat menggunakan kolom yang secara eksplisit dikategorikan sebagai aturan analisis `joinColumn` Anda.

INNERJOIN harus beroperasi pada `joinColumn` dari tabel yang dikonfigurasi dan `joinColumn` dari tabel lain yang dikonfigurasi dalam kolaborasi. Anda memutuskan kolom mana dari tabel Anda dapat digunakan sebagai`joinColumn`.

Setiap kondisi kecocokan dalam ON klausa diperlukan untuk menggunakan kondisi perbandingan kesetaraan (=) antara dua kolom.

Beberapa kondisi pertandingan dalam suatu ON klausa dapat berupa:

- Dikombinasikan menggunakan operator AND logis
- Dipisahkan menggunakan operator OR logis

> **Note**
>
> Semua kondisi JOIN pertandingan harus cocok dengan satu baris dari setiap sisiJOIN. Semua kondisional yang dihubungkan oleh OR atau operator AND logis harus mematuhi persyaratan ini juga.

Berikut ini adalah contoh dari query dengan operator AND logis.

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

Berikut ini adalah contoh dari query dengan operator OR logis.

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

Pengendalian	Definisi	Penggunaan
`joinColumns`	Kolom yang ingin Anda izinkan anggota yang dapat	Kolom yang sama tidak dapat dikategorikan sebagai a `joinColumn` dan

Pengendalian	Definisi	Penggunaan
	kueri untuk digunakan dalam pernyataan INNER JOIN.	`listColumn` (lihatKontrol daftar). `joinColumn` tidak dapat digunakan di bagian lain dari kueri selain INNER JOIN.

Kontrol daftar

Kontrol daftar mengontrol kolom yang dapat dicantumkan dalam output kueri (yaitu, digunakan dalam pernyataan SELECT) atau digunakan untuk memfilter hasil (yaitu, digunakan dalam WHERE pernyataan).

Pengendalian	Definisi	Penggunaan
`listColumns`	Kolom yang Anda izinkan anggota yang dapat kueri untuk digunakan dalam SELECT dan WHERE	A `listColumn` dapat digunakan di SELECT danWHERE. Kolom yang sama tidak dapat digunakan sebagai a `listColumn` dan`joinColumn` .

Daftar aturan analisis struktur yang telah ditentukan

Contoh berikut mencakup struktur yang telah ditentukan yang menunjukkan bagaimana Anda menyelesaikan aturan analisis daftar.

Dalam contoh berikut, *`MyTable`*mengacu pada tabel data Anda. Anda dapat mengganti setiap *`placeholder input pengguna dengan informasi`* Anda sendiri.

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

```
}
```

Aturan analisis daftar - contoh

Contoh berikut menunjukkan bagaimana dua perusahaan dapat berkolaborasi dalam AWS Clean Rooms menggunakan analisis daftar.

Perusahaan A memiliki data manajemen hubungan pelanggan (CRM). Perusahaan A ingin mendapatkan data segmen tambahan pada pelanggannya untuk mempelajari lebih lanjut tentang pelanggan mereka dan berpotensi menggunakan atribut sebagai masukan ke dalam analisis lain. Perusahaan B memiliki data segmen yang terdiri dari atribut segmen unik yang mereka buat berdasarkan data pihak pertama mereka. Perusahaan B ingin memberikan atribut segmen unik kepada Perusahaan A hanya pada pelanggan yang tumpang tindih antara data mereka dan data Perusahaan A.

Perusahaan memutuskan untuk berkolaborasi sehingga Perusahaan A dapat memperkaya data yang tumpang tindih. Perusahaan A adalah anggota yang dapat menanyakan, dan Perusahaan B adalah kontributor.

Untuk membuat kolaborasi dan menjalankan analisis daftar secara kolaborasi, perusahaan melakukan hal berikut:

1. Perusahaan A menciptakan kolaborasi dan menciptakan keanggotaan. Kolaborasi ini memiliki Perusahaan B sebagai anggota lain dalam kolaborasi tersebut. Perusahaan A memungkinkan pencatatan kueri dalam kolaborasi, dan memungkinkan pencatatan kueri di akunnya.
2. Perusahaan B menciptakan keanggotaan dalam kolaborasi. Ini memungkinkan pencatatan kueri di akunnya.
3. Perusahaan A membuat tabel yang dikonfigurasi CRM
4. Perusahaan A menambahkan aturan analisis ke tabel yang dikonfigurasi pelanggan, seperti yang ditunjukkan pada contoh berikut.

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

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

`joinColumns`Perusahaan A ingin menggunakan `hashedemail` dan/atau `thirdpartyid` (diperoleh dari vendor identitas) untuk mencocokkan pelanggan dari data CRM ke pelanggan dari data segmen. Ini akan membantu memastikan Perusahaan A mencocokkan data yang diperkaya untuk pelanggan yang tepat. Mereka memiliki dua JoinColumns untuk berpotensi meningkatkan tingkat kecocokan analisis.

`listColumns`— Perusahaan A menggunakan `listColumns` untuk mendapatkan kolom yang diperkaya di samping yang `internalid` mereka gunakan dalam sistem mereka sendiri. Mereka menambahkan`segment1`,`segment2`, dan `customercategory` berpotensi membatasi pengayaan ke segmen tertentu dengan menggunakannya dalam filter.

5. Perusahaan B membuat tabel yang dikonfigurasi segmen.
6. Perusahaan B menambahkan aturan analisis ke tabel yang dikonfigurasi segmen.

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

`joinColumns`— Perusahaan B memungkinkan Perusahaan A untuk bergabung `identifier2` untuk mencocokkan pelanggan dari data segmen ke data CRM. Perusahaan A dan Perusahaan B bekerja dengan vendor identitas untuk mendapatkan `identifier2` mana yang cocok untuk kolaborasi ini. Mereka tidak menambahkan yang lain `joinColumns` karena mereka percaya `identifier2` memberikan tingkat kecocokan tertinggi dan paling akurat dan pengidentifikasi lain tidak diperlukan untuk kueri.

`listColumns`Perusahaan B memungkinkan Perusahaan A untuk memperkaya data mereka dengan `segment3` dan `segment4` atribut yang merupakan atribut unik yang telah mereka buat, kumpulkan, dan selaraskan (dengan pelanggan A) untuk menjadi bagian dari pengayaan data.

Mereka ingin Perusahaan A mendapatkan segmen ini untuk tumpang tindih pada tingkat baris karena ini adalah kolaborasi pengayaan data.

7. Perusahaan A menciptakan asosiasi tabel CRM untuk kolaborasi.
8. Perusahaan B menciptakan asosiasi tabel segmen untuk kolaborasi.
9. Perusahaan A menjalankan kueri, seperti yang berikut untuk memperkaya data pelanggan yang tumpang tindih.

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

10. Perusahaan A dan Perusahaan B meninjau log kueri. Perusahaan B memverifikasi bahwa kueri sejalan dengan apa yang disepakati dalam perjanjian kolaborasi.

Aturan analisis kustom di AWS Clean Rooms

Dalam AWS Clean Rooms, aturan analisis kustom adalah jenis aturan analisis baru yang memungkinkan kueri kustom dijalankan pada tabel yang dikonfigurasi. Kueri SQL khusus masih dibatasi untuk hanya memiliki SELECT perintah tetapi dapat menggunakan lebih banyak konstruksi SQL daripada agregasi dan kueri daftar (misalnya, fungsi jendela, OUTER JOIN, CTE, atau subquery; lihat Referensi SQL untuk daftar lengkap).AWS Clean Rooms Kueri SQL kustom tidak harus mengikuti struktur kueri seperti agregasi dan kueri daftar.

Aturan analisis kustom mendukung kasus penggunaan yang lebih maju daripada yang dapat didukung oleh aturan agregasi dan analisis daftar seperti analisis atribusi khusus, pembandingan, analisis inkrementalitas, dan penemuan audiens. Ini merupakan tambahan dari superset kasus penggunaan yang didukung oleh agregasi dan aturan analisis daftar.

Aturan analisis kustom juga mendukung privasi diferensial. Privasi diferensial adalah kerangka kerja yang ketat secara matematis untuk perlindungan privasi data. Untuk informasi selengkapnya, lihat AWS Clean Rooms Privasi Diferensial. Saat Anda membuat templat analisis, Privasi AWS Clean Rooms Diferensial memeriksa templat untuk menentukan apakah templat tersebut kompatibel dengan struktur kueri tujuan umum untuk AWS Clean Rooms Privasi Diferensial. Validasi ini memastikan bahwa Anda tidak membuat templat analisis yang tidak diizinkan dengan tabel yang dilindungi privasi diferensial.

Untuk mengonfigurasi aturan analisis kustom, pemilik data dapat memilih untuk mengizinkan kueri khusus tertentu, yang disimpan dalam templat analisis, untuk dijalankan pada tabel yang dikonfigurasi. Pemilik data meninjau templat analisis sebelum menambahkannya ke kontrol analisis yang diizinkan dalam aturan analisis khusus. Template analisis tersedia dan hanya terlihat dalam kolaborasi di mana mereka dibuat (bahkan jika tabel dikaitkan dengan kolaborasi lain) dan hanya dapat dijalankan oleh anggota yang dapat melakukan kueri dalam kolaborasi itu.

Atau, anggota dapat memilih untuk mengizinkan anggota lain (penyedia kueri) untuk membuat kueri tanpa ulasan. Anggota menambahkan akun penyedia kueri yang dikendalikan oleh penyedia kueri yang diizinkan dalam aturan analisis kustom. Jika penyedia kueri adalah anggota yang dapat melakukan kueri, mereka dapat menjalankan kueri apa pun secara langsung pada tabel yang dikonfigurasi. Penyedia kueri juga dapat membuat kueri dengan membuat templat analisis. Setiap kueri yang telah dibuat oleh penyedia kueri secara otomatis diizinkan untuk berjalan di atas meja di semua kolaborasi di mana Akun AWS ada dan tabel terkait.

Pemilik data hanya dapat mengizinkan templat analisis atau akun untuk membuat kueri, bukan keduanya. Jika pemilik data membiarkannya kosong, anggota yang dapat melakukan kueri tidak dapat menjalankan kueri pada tabel yang dikonfigurasi.

Topik

Aturan analisis kustom struktur yang telah ditentukan

Contoh berikut mencakup struktur yang telah ditentukan yang menunjukkan kepada Anda cara menyelesaikan aturan analisis kustom dengan privasi diferensial diaktifkan. `userIdentifier`Nilai adalah kolom yang secara unik mengidentifikasi pengguna Anda, seperti user_id. Bila Anda memiliki dua atau lebih tabel dengan privasi diferensial diaktifkan dalam kolaborasi, AWS Clean Rooms Anda harus mengonfigurasi kolom yang sama dengan kolom pengenal pengguna di kedua aturan analisis untuk mempertahankan definisi pengguna yang konsisten di seluruh tabel.

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

```
    "columns": [
      {
        "name": "userIdentifier"
      }
    ]
  }
}
```

Anda dapat:

- Tambahkan ARN templat analisis ke kontrol analisis yang diizinkan. Dalam hal ini, `allowedAnalysisProviders` kontrol tidak termasuk.

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

- Tambahkan Akun AWS ID anggota ke `allowedAnalysisProviders` kontrol. Dalam hal ini, Anda `ANY_QUERY` menambah `allowedAnalyses` kontrol.

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

Contoh aturan analisis kustom

Contoh berikut menunjukkan bagaimana dua perusahaan dapat berkolaborasi dalam AWS Clean Rooms menggunakan aturan analisis kustom.

Perusahaan A memiliki data pelanggan dan penjualan. Perusahaan A tertarik untuk memahami peningkatan penjualan kampanye iklan di situs Perusahaan B. Perusahaan B memiliki data pemirsa dan atribut segmen yang berguna bagi Perusahaan (misalnya, perangkat yang mereka gunakan saat melihat iklan).

Perusahaan A memiliki kueri inkrementalitas tertentu yang ingin mereka jalankan dalam kolaborasi.

Untuk membuat kolaborasi dan menjalankan analisis kustom dalam kolaborasi, perusahaan melakukan hal berikut:

1. Perusahaan A menciptakan kolaborasi dan menciptakan keanggotaan. Kolaborasi ini memiliki Perusahaan B sebagai anggota lain dalam kolaborasi tersebut. Perusahaan A memungkinkan pencatatan kueri dalam kolaborasi, dan memungkinkan pencatatan kueri di akunnya.
2. Perusahaan B menciptakan keanggotaan dalam kolaborasi. Ini memungkinkan pencatatan kueri di akunnya.
3. Perusahaan A membuat tabel yang dikonfigurasi CRM
4. Perusahaan A menambahkan aturan analisis kustom kosong ke tabel penjualan yang dikonfigurasi.
5. Perusahaan A mengaitkan tabel penjualan yang dikonfigurasi untuk kolaborasi.
6. Perusahaan B membuat tabel yang dikonfigurasi pemirsa.
7. Perusahaan B menambahkan aturan analisis kustom kosong ke tabel yang dikonfigurasi pemirsa.
8. Perusahaan B mengaitkan tabel yang dikonfigurasi pemirsa dengan kolaborasi.
9. Perusahaan A melihat tabel penjualan dan tabel pemirsa yang terkait dengan kolaborasi dan membuat templat analisis, menambahkan kueri inkrementalitas dan parameter untuk bulan kampanye.

```
{
    "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 Perusahaan A menambahkan akun mereka (misalnya, 444455556666) ke kontrol penyedia analisis yang diizinkan dalam aturan analisis khusus. Mereka menggunakan kontrol penyedia analisis yang diizinkan karena mereka ingin mengizinkan kueri apa pun yang mereka buat berjalan di tabel yang dikonfigurasi penjualan mereka.

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

11 Perusahaan B melihat template analisis yang dibuat dalam kolaborasi dan meninjau isinya termasuk string kueri dan parameter.

12 Perusahaan B menentukan bahwa templat analisis mencapai kasus penggunaan inkrementalitas dan memenuhi persyaratan privasi mereka tentang bagaimana tabel yang dikonfigurasi pemirsa mereka dapat ditanyakan.

13 Perusahaan B menambahkan templat analisis ARN ke kontrol analisis yang diizinkan dalam aturan analisis khusus dari tabel pemirsa. Mereka menggunakan kontrol analisis yang diizinkan karena mereka hanya ingin mengizinkan kueri inkrementalitas berjalan pada tabel yang dikonfigurasi pemirsa mereka.

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

14 Perusahaan A menjalankan template analisis dan menggunakan nilai parameter`05-01-2023`.

Aturan analisis khusus dengan privasi diferensial

Pada tahun AWS Clean Rooms, aturan analisis kustom mendukung privasi diferensial. Privasi diferensial adalah kerangka kerja yang ketat secara matematis untuk perlindungan privasi data yang membantu Anda melindungi data Anda dari upaya identifikasi ulang.

Privasi diferensial mendukung analisis agregat seperti perencanaan kampanye iklan, post-ad-campaign pengukuran, pembandingan dalam konsorsium lembaga keuangan, dan pengujian A/B untuk penelitian kesehatan.

Struktur kueri dan sintaks yang didukung didefinisikan dalamStruktur kueri dan sintaks.

Aturan analisis kustom dengan contoh privasi diferensial

Pertimbangkan contoh aturan analisis kustom yang disajikan di bagian sebelumnya. Contoh ini menunjukkan bagaimana Anda dapat menggunakan privasi diferensial untuk melindungi data Anda dari upaya identifikasi ulang sambil memungkinkan mitra Anda mempelajari wawasan penting bisnis dari data Anda. Asumsikan bahwa Perusahaan B, yang memiliki data pemirsa, ingin melindungi data mereka menggunakan privasi diferensial. Untuk menyelesaikan pengaturan privasi diferensial, Perusahaan B menyelesaikan langkah-langkah berikut:

1. Perusahaan B mengaktifkan privasi diferensial sambil menambahkan aturan analisis kustom ke tabel yang dikonfigurasi pemirsa. Perusahaan B memilih `viewershipdata.hashedemail` sebagai kolom pengenal pengguna.
2. Perusahaan B menambahkan kebijakan privasi diferensial dalam kolaborasi untuk membuat tabel data pemirsa mereka tersedia untuk kueri. Perusahaan B memilih kebijakan default untuk menyelesaikan penyiapan dengan cepat.

Perusahaan A, yang ingin memahami peningkatan penjualan kampanye iklan di situs Perusahaan B, menjalankan templat analisis. Karena kueri kompatibel dengan struktur kueri tujuan umum Privasi AWS Clean Rooms Diferensial, kueri berjalan dengan sukses.

Struktur kueri dan sintaks

Kueri yang berisi setidaknya satu tabel yang mengaktifkan privasi diferensial harus mematuhi sintaks berikut.

```
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

Untuk struktur dan sintaks kueri privasi diferensial, perhatikan hal-hal berikut:

- Sub-kueri tidak didukung.
- Common Table Expressions (CTE) harus memancarkan kolom pengenal pengguna jika tabel atau CTE melibatkan data yang dilindungi oleh privasi diferensial. Filter, pengelompokan, dan agregasi harus dilakukan di tingkat pengguna.

- Final_select memungkinkan fungsi agregat COUNT DISTINCT, COUNT, SUM, AVG, dan STDDEV.

Untuk detail selengkapnya tentang kata kunci SQL yang didukung untuk privasi diferensial, lihat. Kemampuan SQL dari Privasi AWS Clean Rooms Diferensial

AWS Clean Rooms Privasi Diferensial

AWS Clean Rooms Privasi Diferensial membantu Anda melindungi privasi pengguna Anda dengan teknik yang didukung secara matematis yang diterapkan dengan kontrol intuitif dalam beberapa klik. Sebagai kemampuan yang dikelola sepenuhnya, tidak diperlukan pengalaman privasi diferensial sebelumnya untuk membantu Anda mencegah identifikasi ulang pengguna Anda. AWS Clean Rooms secara otomatis menambahkan jumlah noise yang dikalibrasi dengan hati-hati ke hasil kueri saat runtime untuk membantu melindungi data tingkat individu Anda.

AWS Clean Rooms Privasi Diferensial mendukung berbagai kueri analitis dan cocok untuk berbagai kasus penggunaan, di mana sejumlah kecil kesalahan dalam hasil kueri tidak akan membahayakan kegunaan analisis Anda. Dengan itu, mitra Anda dapat menghasilkan wawasan penting bisnis tentang kampanye iklan, keputusan investasi, penelitian klinis, dan banyak lagi, semuanya tanpa memerlukan pengaturan tambahan dari mitra Anda.

AWS Clean Rooms Privasi Diferensial melindungi dari overflow atau kesalahan cast tidak valid yang menggunakan fungsi skalar atau simbol operator matematika dengan cara yang berbahaya.

Untuk informasi selengkapnya tentang Privasi AWS Clean Rooms Diferensial, lihat topik berikut.

Topik

Privasi diferensial

Privasi diferensial hanya memungkinkan wawasan agregat dan mengaburkan kontribusi data individu dalam wawasan tersebut. Privasi diferensial melindungi data kolaborasi dari anggota yang dapat menerima hasil belajar tentang individu tertentu. Tanpa privasi diferensial, anggota yang dapat menerima hasil dapat mencoba menyimpulkan data pengguna individu dengan menambahkan atau menghapus catatan tentang individu dan mengamati perbedaan dalam hasil kueri.

Ketika privasi diferensial diaktifkan, jumlah noise tertentu ditambahkan ke hasil kueri untuk mengaburkan kontribusi pengguna individu. Jika anggota yang dapat menerima hasil mencoba mengamati perbedaan hasil kueri setelah menghapus catatan tentang individu dari kumpulan data mereka, variabilitas dalam hasil kueri membantu mencegah identifikasi data individu. AWS Clean Rooms Privasi Diferensial menggunakan SampCertsampler, implementasi sampler yang terbukti benar yang dikembangkan oleh. AWS

Bagaimana Privasi Diferensial bekerja AWS Clean Rooms

Alur kerja untuk mengaktifkan privasi diferensial AWS Clean Rooms memerlukan langkah-langkah tambahan berikut saat menyelesaikan alur kerja untuk: AWS Clean Rooms

1. Anda mengaktifkan privasi diferensial saat menambahkan aturan analisis kustom.
2. Anda mengonfigurasi kebijakan privasi diferensial untuk kolaborasi agar tabel data Anda dilindungi dengan privasi diferensial yang tersedia untuk kueri.

Setelah Anda menyelesaikan langkah-langkah ini, anggota yang dapat melakukan kueri dapat mulai menjalankan kueri pada data yang dilindungi privasi diferensial. AWS Clean Rooms mengembalikan hasil yang sesuai dengan kebijakan privasi diferensial. AWS Clean Rooms Privasi Diferensial melacak perkiraan jumlah kueri yang tersisa yang dapat Anda jalankan, mirip dengan pengukur gas di mobil yang menunjukkan tingkat bahan bakar mobil saat ini. Jumlah kueri yang dapat dijalankan oleh anggota yang dapat melakukan kueri dibatasi oleh anggaran Privasi dan Kebisingan yang ditambahkan per parameter kueri yang diatur dalamKebijakan privasi diferensial.

Pertimbangan

Saat menggunakan privasi diferensial di AWS Clean Rooms, pertimbangkan hal berikut:

- Anggota yang dapat menerima hasil tidak dapat menggunakan privasi diferensial. Mereka akan mengonfigurasi aturan analisis khusus dengan privasi diferensial dimatikan untuk tabel yang dikonfigurasi.
- Anggota yang dapat melakukan kueri tidak dapat menggabungkan tabel dari dua atau lebih penyedia data ketika keduanya mengaktifkan privasi diferensial.

Kebijakan privasi diferensial

Kebijakan privasi diferensial mengontrol berapa banyak fungsi agregasi yang diizinkan oleh anggota yang dapat kueri untuk dijalankan dalam suatu kolaborasi. Anggaran Privasi mendefinisikan sumber daya umum dan terbatas yang diterapkan semua tabel dalam kolaborasi. Kebisingan yang ditambahkan per kueri mengatur tingkat di mana anggaran privasi habis.

Kebijakan privasi diferensial diperlukan untuk membuat tabel yang dilindungi privasi diferensial Anda tersedia untuk pertanyaan. Ini adalah langkah satu kali dalam kolaborasi dan mencakup dua input:

- Anggaran privasi — Dikukur dalam hal epsilon, anggaran privasi mengontrol tingkat perlindungan privasi. Ini adalah sumber daya umum dan terbatas yang diterapkan untuk semua tabel Anda yang dilindungi dengan privasi diferensial dalam kolaborasi, karena tujuannya adalah untuk menjaga privasi pengguna Anda yang informasinya dapat hadir dalam beberapa tabel.

  Anggaran Privasi dikonsumsi setiap kali kueri dijalankan di tabel Anda. Ketika anggaran privasi sepenuhnya habis, anggota kolaborasi yang dapat melakukan kueri tidak dapat menjalankan kueri tambahan hingga ditingkatkan atau di-refresh. Dengan menetapkan anggaran privasi yang lebih besar, anggota yang dapat menerima hasil dapat mengurangi ketidakpastian mereka tentang individu dalam data. Pilih anggaran privasi yang menyeimbangkan persyaratan kolaborasi Anda dengan kebutuhan privasi Anda dan setelah berkonsultasi dengan pengambil keputusan bisnis.

  Anda dapat memilih Segarkan anggaran privasi setiap bulan untuk secara otomatis membuat anggaran privasi baru setiap bulan kalender, jika Anda berencana untuk secara teratur membawa data baru ke dalam kolaborasi. Memilih opsi ini memungkinkan jumlah informasi yang sewenang-wenang untuk diungkapkan tentang baris data ketika berulang kali ditanyakan di seluruh penyegaran. Hindari memilih ini jika baris yang sama akan berulang kali ditanyakan antara penyegaran anggaran privasi.
- Kebisingan yang ditambahkan per kueri diukur dalam hal jumlah pengguna yang kontribusinya ingin Anda kaburkan. Nilai ini mengatur tingkat di mana anggaran privasi habis. Nilai noise yang lebih besar mengurangi tingkat di mana anggaran privasi habis, dan karenanya memungkinkan lebih banyak kueri untuk dijalankan pada data Anda. Namun, ini harus diimbangi dengan merilis wawasan data yang kurang akurat. Pertimbangkan akurasi yang diinginkan untuk wawasan kolaborasi saat menetapkan nilai ini.

Anda dapat menggunakan kebijakan privasi diferensial default untuk menyelesaikan pengaturan dengan cepat atau menyesuaikan kebijakan privasi diferensial Anda sesuai kasus penggunaan Anda.

AWS Clean Rooms Privasi Diferensial menyediakan kontrol intuitif untuk mengonfigurasi kebijakan. AWS Clean Rooms Privasi Diferensial memungkinkan Anda melihat pratinjau utilitas dalam hal jumlah agregasi yang mungkin di semua kueri pada data Anda dan memperkirakan berapa banyak kueri yang dapat dijalankan dalam kolaborasi data.

Anda dapat menggunakan contoh interaktif untuk memahami bagaimana nilai yang berbeda dari anggaran Privasi dan Kebisingan yang ditambahkan per kueri akan memengaruhi hasil untuk berbagai jenis kueri SQL. Secara umum, Anda perlu menyeimbangkan kebutuhan privasi Anda dengan jumlah pertanyaan yang ingin Anda izinkan dan keakuratan pertanyaan tersebut. Anggaran Privasi yang lebih kecil atau Noise yang lebih besar yang ditambahkan per kueri dapat melindungi privasi pengguna dengan lebih baik, tetapi memberikan wawasan yang kurang berarti bagi mitra kolaborasi Anda.

Jika Anda meningkatkan anggaran Privasi sambil menjaga parameter Noise yang ditambahkan per kueri tetap sama, anggota yang dapat melakukan kueri dapat menjalankan lebih banyak agregasi pada tabel Anda dalam kolaborasi. Anda dapat meningkatkan anggaran Privasi kapan saja selama kolaborasi. Jika Anda mengurangi anggaran Privasi sambil menjaga parameter Noise yang ditambahkan per kueri tetap sama, anggota yang dapat melakukan kueri dapat menjalankan agregasi yang lebih sedikit. Anda tidak dapat mengurangi anggaran Privasi setelah anggota yang dapat melakukan kueri mulai menganalisis data Anda.

Jika Anda meningkatkan Noise yang ditambahkan per kueri sambil menjaga input anggaran Privasi tetap sama, anggota yang dapat melakukan kueri dapat menjalankan lebih banyak agregasi pada tabel Anda dalam kolaborasi. Jika Anda mengurangi Noise yang ditambahkan per kueri sambil menjaga input anggaran Privasi tetap sama, anggota yang dapat melakukan kueri dapat menjalankan agregasi yang lebih sedikit. Anda dapat menambah atau mengurangi Noise yang ditambahkan per kueri kapan saja selama kolaborasi.

Kebijakan privasi diferensial dikelola oleh tindakan API templat anggaran privasi.

Kemampuan SQL dari Privasi AWS Clean Rooms Diferensial

AWS Clean Rooms Privasi Diferensial menggunakan struktur kueri tujuan umum untuk mendukung kueri SQL yang kompleks. Template analisis kustom divalidasi terhadap struktur ini untuk memastikan bahwa mereka dapat berjalan pada tabel yang dilindungi oleh privasi diferensial. Tabel berikut menunjukkan fungsi mana yang didukung. Untuk informasi selengkapnya, lihat Struktur kueri dan sintaks.

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
Fungsi agregat	• Fungsi ANY_VALUE • PERKIRAAN fungsi PERCENTILE_DISC • Fungsi AVG • Fungsi COUNT dan COUNT DISTINCT • Fungsi LISTAGG • Fungsi MAX • Fungsi MEDIAN • Fungsi MIN • Fungsi PERCENTILE_CONT • Fungsi STDDEV_SAMP dan STDDEV_POP • Fungsi SUM dan SUM DISTINCT • Fungsi VAR_SAMP dan VAR_POP	Didukung dengan syarat bahwa CTE yang menggunakan tabel yang dilindungi privasi diferensial harus menghasilkan data dengan catatan tingkat pengguna. Anda harus menulis ekspresi SELECT di CTE tersebut menggunakan `SELECT userIdentifierColumn...' format.	Agregasi yang didukung: AVG, COUNT, COUNT DISTINCT, STDDEV, dan SUM.
CTE	DENGAN klausa, DENGAN klausa subquery	Didukung dengan syarat bahwa CTE yang menggunakan tabel yang dilindungi privasi diferensial harus menghasilkan data dengan catatan tingkat pengguna. Anda harus menulis	N/A

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
		ekspresi SELECT di CTE tersebut menggunak an `SELECT userIdent ifierColu mn...' format.	
Subkueri	PILIH daftar subquery, DARI klausa subquery, WHERE klausa subquery	Tidak didukung. Subkueri dalam kueri yang mereferensikan tabel dengan privasi diferensial diaktifkan tidak didukung. Tulis ulang subkueri Anda sebagai Common Table Expressions (CTE).	
Bergabung klausa	• BERGABUNG BATIN • KIRI BERGABUNG • BERGABUNG DENGAN BENAR • BERGABUNG PENUH • [BERGABUNG] ATAU operator • CROSS JOIN	Didukung dengan syarat bahwa hanya fungsi JOIN yang equi-join pada kolom pengenal pengguna yang didukung dan wajib saat menanyakan dua atau lebih tabel dengan privasi diferensial diaktifkan. Pastikan bahwa kondisi equi-join wajib sudah benar. Konfirmas ikan bahwa pemilik tabel telah mengonfig urasi kolom pengenal pengguna yang sama di semua tabel sehingga definisi pengguna tetap konsisten di seluruh tabel. Fungsi CROSS JOIN tidak didukung saat menggabungkan dua atau lebih relasi dengan privasi diferensial diaktifkan.	
Tetapkan operator	UNION, UNION ALL, INTERSECT, KECUALI | MINUS (ini adalah sinonim)	Semua didukung	Tidak didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
Fungsi jendela	Fungsi agregat • Fungsi jendela AVG • Fungsi jendela COUNT • Fungsi jendela CUME_DIST • Fungsi jendela DENSE_RANK • Fungsi jendela FIRST_VALUE • Fungsi jendela LAG • Fungsi jendela LAST_VALUE • Fungsi jendela LEAD • Fungsi jendela MAX • Fungsi jendela MEDIAN • Fungsi jendela MIN • Fungsi jendela NTH_VALUE • Fungsi jendela RATIO_TO_REPORT • Fungsi jendela STDDEV_SAMP dan STDDEV_POP (STDDEV_SAMP dan STDDEV adalah sinonim)	Semua didukung dengan kondisi bahwa kolom pengenal pengguna di klausa partisi fungsi jendela diperlukan saat Anda menanyakan relasi dengan privasi diferensial diaktifkan.	Tidak didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
	• Fungsi jendela SUM • Fungsi jendela VAR_SAMP dan VAR_POP (VAR_SAMP dan VARIANCE adalah sinonim)		
	Fungsi peringkat • Fungsi jendela DENSE_RANK • Fungsi jendela NTILE • Fungsi jendela PERCENT_RANK • Fungsi jendela RANK • Fungsi jendela ROW_NUMBER		
Ekspresi bersyarat	• Ekspresi kondisi CASE • Ekspresi COALESCE • Fungsi TERBESAR dan PALING KECIL • Fungsi NVL dan COALESCE • Fungsi NVL2 • Fungsi NULLIF	Semua didukung	Semua didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
Ketentuan	• Kondisi perbandingan • Kondisi logis • Kondisi pencocokan pola • ANTARA kondisi rentang • Kondisi nol	`EXISTS`dan `IN` tidak dapat digunakan karena mereka memerlukan subquery. Semua yang lain didukung.	Semua didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
Fungsi tanggal-waktu	• Fungsi tanggal dan waktu dalam transaksi • Operator penggabungan • Fungsi ADD_MONTHS • Fungsi CONVERT_TIMEZONE • Fungsi CURRENT_DATE • Fungsi DATEADD • Fungsi DATEDIFF • fungsi DATE_PART • Fungsi DATE_TRUNC • Fungsi EKSTRAK • fungsi GETDATE • Fungsi TIMEOFDAY • Fungsi TO_TIMESTAMP • Bagian tanggal untuk fungsi tanggal atau stempel waktu	Semua didukung	Semua didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
Fungsi string	• || Operator (penggabungan) • Fungsi BTRIM • Fungsi CHAR_LENGTH • Fungsi CHARACTER _LENGTH • Fungsi CHARINDEX • Fungsi CONCAT • Fungsi KIRI dan KANAN • Fungsi LEN • Fungsi PANJANG • Fungsi LOWER • Fungsi LPAD dan RPAD • Fungsi LTRIM • Fungsi POSISI • Fungsi REGEXP_COUNT • Fungsi REGEXP_IN STR • Fungsi REGEXP_RE PLACE • Fungsi REGEXP_SUBSTR • Fungsi REPEAT	Semua didukung	Semua didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
	• GANTI fungsi • Fungsi REPLICATE • Fungsi REVERSE • Fungsi RTRIM • Fungsi SOUNDEX • Fungsi SPLIT_PART • fungsi STRPOS • Fungsi SUBSTRING • Fungsi TEXTLEN • FUNGSI TRANSLATE • Fungsi TRIM • Fungsi UPPER		
Fungsi pemformatan tipe data	• Fungsi CAST • TO_CHAR • Fungsi TO_DATE • TO_NUMBER • String format datetime • String format numerik	Semua didukung	Semua didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
Fungsi hash	• Fungsi MD5 • Fungsi SHA • Fungsi SHA1 • Fungsi SHA2 • MURMUR3_32_HASH	Semua didukung	Semua didukung
Simbol operator matematika	+, -, *,/,%, dan @	Semua didukung	Semua didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
Fungsi matematika	• Fungsi ABS • Fungsi ACOS • Fungsi ASIN • Fungsi ATAN • Fungsi ATAN2 • Fungsi CBRT • Fungsi CEILING (atau CEIL) • Fungsi COS • Fungsi COT • Fungsi DERAJAT • Fungsi DEXP • Fungsi LTRIM • Fungsi DLOG1 • Fungsi DLOG10 • Fungsi EXP • Fungsi FLOOR • Fungsi LN • Fungsi LOG • Fungsi MOD • Fungsi PI • Fungsi POWER • Fungsi RADIANS • fungsi RANDOM • Fungsi ROUND • Fungsi SIGN • Fungsi SIN • Fungsi SQRT	Semua didukung	Semua didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
	• Fungsi TRUNC		
Fungsi informasi tipe SUPER	• Fungsi DECIMAL_PRECISION • Fungsi DECIMAL_SCALE • Fungsi IS_ARRAY • Fungsi IS_BIGINT • Fungsi IS_CHAR • Fungsi IS_DECIMAL • Fungsi IS_FLOAT • Fungsi IS_INTEGER • fungsi IS_OBJECT • Fungsi IS_SCALAR • Fungsi IS_SMALLINT • Fungsi IS_VARCHAR • Fungsi JSON_TYPEOF	Semua didukung	Semua didukung
Fungsi VARBYTE	• Fungsi FROM_HEX • Fungsi FROM_VARBYTE • Fungsi TO_HEX • Fungsi TO_VARBYTE	Semua didukung	Semua didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
JSON	• Fungsi CAN_JSON_ PARSE • Fungsi JSON_EXTR ACT_ARRAY _ELEMENT_TEXT • Fungsi JSON_EXTR ACT_PATH_TEXT • Fungsi JSON_PARSE • Fungsi JSON_SERI ALIZE • Fungsi JSON_SERA LIZE_TO_V ARBYTE	Semua didukung	Semua didukung
Fungsi array	• fungsi array • fungsi array_concat • fungsi array_flatten • fungsi get_array _length • fungsi split_to_array • fungsi subarray	Tidak didukung	Tidak didukung
GRUP Diperpanjang OLEH	SET PENGELOMP OKAN, ROLLUP, KUBUS	Tidak didukung	Tidak didukung

Nama pendek	Konstruksi SQL	Ekspresi tabel umum (CTE)	Klausul SELECT akhir
Urutkan operasi	ORDER BY	Didukung dengan syarat bahwa klausa ORDER BY hanya didukung dalam klausa partisi fungsi jendela saat menanyakan tabel dengan privasi diferensial diaktifkan.	Didukung
Batas baris	BATAS, OFFSET	Tidak didukung di CTE menggunakan tabel yang dilindungi privasi diferensial	Semua didukung
Aliasing tabel dan kolom		Didukung	Didukung
Fungsi matematika pada fungsi agregat		Didukung	Didukung
Fungsi skalar dalam fungsi agregat		Didukung	Didukung

Alternatif umum untuk konstruksi SQL yang tidak didukung

Kategori	Konstruksi SQL	Alternatif
Fungsi jendela	• LISTAGG • PERSENTILE_CONT • PERCENTILE_DISC	Anda dapat menggunakan fungsi agregat setara dengan GROUP BY.
Simbol operator matematika	• $ kolom ||/ 2 • $ kolom |/ 2	• CBRT • SQRT

Kategori	Konstruksi SQL	Alternatif
	• $ kolom ^ 2	• DAYA ($ kolom, 2)
Fungsi skalar	• SYSDATE • $ kolom: :integer • mengkonversi (jenis, $ kolom)	• CURRENT_DATE • CAST $ kolom AS integer • CAST $ kolom tipe AS
Literal	INTERVAL '1 DETIK'	INTERVAL '1' DETIK
Pembatasan baris	TOP n	BATAS n
Join	• MENGGUNAKAN • ALAMI	Klausa ON harus secara eksplisit berisi kriteria gabungan.

Kiat dan contoh kueri Privasi Diferensial

AWS Clean Rooms Privasi Diferensial menggunakan struktur kueri tujuan umum untuk mendukung berbagai macam konstruksi SQL seperti Common Table Expressions (CTE) untuk persiapan data dan fungsi agregat yang umum digunakan seperti, atau. `COUNT` `SUM` Untuk mengaburkan kontribusi pengguna yang mungkin dalam data Anda dengan menambahkan noise ke hasil kueri agregat saat run-time, Privasi AWS Clean Rooms Diferensial mengharuskan fungsi agregat di final dijalankan pada data tingkat pengguna. `SELECT statement`

Contoh berikut menggunakan dua tabel bernama `socialco_impressions` dan `socialco_users` dari penerbit media yang ingin melindungi data menggunakan privasi diferensial saat berkolaborasi dengan merek atletik dengan data. `athletic_brand_sales` Penerbit media telah mengonfigurasi `user_id` kolom sebagai kolom pengenal pengguna sambil mengaktifkan privasi diferensial. AWS Clean Rooms Pengiklan tidak memerlukan perlindungan privasi diferensial dan ingin menjalankan kueri menggunakan CTE pada data gabungan. Karena CTE mereka menggunakan tabel yang dilindungi privasi diferensial, pengiklan menyertakan kolom pengenal pengguna dari tabel yang dilindungi tersebut dalam daftar kolom CTE dan bergabung dengan tabel yang dilindungi pada kolom pengenal pengguna.

```
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
```

Demikian pula, jika Anda ingin menjalankan fungsi jendela pada tabel data yang dilindungi privasi diferensial, Anda harus menyertakan kolom pengenal pengguna dalam klausa. `PARTITION BY`

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

Batasan Privasi AWS Clean Rooms Diferensial

AWS Clean Rooms Privasi Diferensial tidak membahas situasi berikut:

1. AWS Clean Rooms Privasi Diferensial tidak mengatasi serangan waktu. Misalnya, serangan ini dimungkinkan dalam skenario di mana pengguna individu menyumbangkan sejumlah besar baris dan menambahkan atau menghapus pengguna ini secara signifikan mengubah waktu perhitungan kueri.
2. AWS Clean Rooms Differential Privacy tidak menjamin privasi diferensial ketika kueri SQL dapat mengakibatkan overflow atau kesalahan cast tidak valid pada waktu berjalan karena penggunaan

konstruksi SQL tertentu. Tabel berikut adalah daftar beberapa, tetapi tidak semua, konstruksi SQL yang dapat menghasilkan kesalahan run-time dan harus diverifikasi dalam template analisis. Sebaiknya Anda menyetujui templat analisis yang meminimalkan kemungkinan kesalahan waktu proses tersebut dan meninjau log kueri secara berkala untuk menentukan apakah kueri sesuai dengan perjanjian kolaborasi.

Konstruksi SQL berikut rentan terhadap kesalahan overflow:

- Fungsi agregat - AVG, LISTAVG, PERCENTILE_COUNT, PERCENTILE_DISC, SUM/ SUM_DISTINCT
- Fungsi pemformatan tipe data - TO_TIMESTAMP, TO_DATE
- Fungsi tanggal dan waktu - ADD_MONTHS, DATEADD, DATEDIFF
- Fungsi matematika - +, -, *,/, DAYA
- Fungsi string - ||, CONCAT, REPEAT, REPLICATE
- Fungsi jendela - AVG, LISTAGG, PERCENTILE_COUNT, PERCENTILE_DISC, RATIO_TO_REPORT, SUM

Fungsi pemformatan tipe data CAST rentan terhadap kesalahan cast yang tidak valid.

AWS Clean Rooms ML

AWS Clean Rooms ML

AWS Clean Rooms ML menyediakan metode pelestarian privasi bagi dua pihak untuk mengidentifikasi pengguna serupa dalam data mereka tanpa perlu berbagi data mereka satu sama lain. Pihak pertama membawa data pelatihan AWS Clean Rooms sehingga mereka dapat membuat dan mengonfigurasi model yang mirip dan mengaitkannya dengan kolaborasi. Pihak kedua kemudian membawa data benih mereka ke AWS Clean Rooms dan menghasilkan segmen mirip yang menyerupai data pelatihan.

Untuk penjelasan lebih rinci tentang cara kerjanya, lihatLowongan kerja lintas akun.

- Penyedia data pelatihan — Pihak yang menyumbangkan data pelatihan, membuat dan mengonfigurasi model yang mirip, dan kemudian mengaitkan model yang mirip dengan kolaborasi.
- Penyedia data benih — Pihak yang menyumbangkan data benih, menghasilkan segmen yang mirip, dan mengekspor segmen mirip mereka.
- Data pelatihan — Data penyedia data pelatihan, yang digunakan untuk menghasilkan model yang mirip. Data pelatihan digunakan untuk mengukur kesamaan dalam perilaku pengguna.

  Data pelatihan harus berisi ID pengguna, ID item, dan kolom stempel waktu. Secara opsional, data pelatihan dapat berisi interaksi lain sebagai fitur numerik atau kategoris. Contoh interaksi adalah daftar video yang ditonton, item yang dibeli, atau artikel yang dibaca.
- Data benih — Data penyedia data benih, yang digunakan untuk membuat segmen yang mirip. Output segmen mirip adalah sekumpulan pengguna dari data pelatihan yang paling mirip dengan pengguna benih.
- Model Lookalike — Model pembelajaran mesin dari data pelatihan yang digunakan untuk menemukan pengguna serupa di kumpulan data lain.

  Saat menggunakan API, istilah model audiens digunakan secara setara dengan model yang mirip. Misalnya, Anda menggunakan API CreateAudienceModel untuk membuat model yang mirip.
- Segmen mirip — Subset dari data pelatihan yang paling mirip dengan data benih.

  Saat menggunakan API, Anda membuat segmen mirip dengan API. StartAudienceGenerationJob

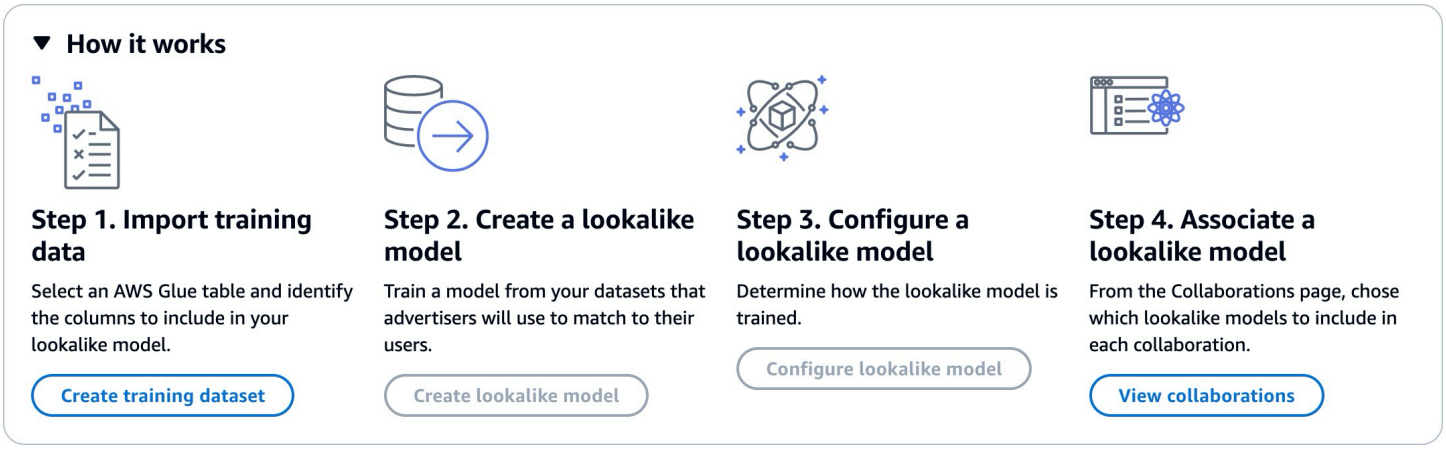
Data penyedia data pelatihan tidak pernah dibagikan dengan penyedia data benih dan data penyedia data benih tidak pernah dibagikan dengan penyedia data pelatihan. Output segmen yang mirip dibagikan dengan penyedia data pelatihan, tetapi tidak pernah penyedia data benih.

Untuk informasi selengkapnya tentang model mirip, lihat topik berikut.

Topik

- Cara kerja AWS Clean Rooms ML

Cara kerja AWS Clean Rooms ML



Clean Rooms ML mengharuskan dua pihak, penyedia data pelatihan dan penyedia data benih, bekerja secara berurutan AWS Clean Rooms untuk membawa data mereka ke dalam kolaborasi. Ini adalah alur kerja yang harus diselesaikan oleh penyedia data pelatihan terlebih dahulu:

1. Data penyedia data pelatihan harus disimpan dalam tabel katalog AWS Glue data interaksi item pengguna. Minimal, data pelatihan harus berisi kolom ID pengguna, kolom ID interaksi, dan kolom stempel waktu.
2. Penyedia data pelatihan mendaftarkan data pelatihan dengan AWS Clean Rooms.
3. Penyedia data pelatihan membuat model mirip yang dapat dibagikan dengan beberapa penyedia data benih. Model mirip adalah jaringan saraf dalam yang dapat memakan waktu hingga 24 jam untuk dilatih. Ini tidak dilatih ulang secara otomatis dan kami sarankan Anda melatih ulang model setiap minggu.
4. Penyedia data pelatihan mengonfigurasi model yang mirip, termasuk apakah akan berbagi metrik relevansi dan lokasi Amazon S3 dari segmen keluaran. Penyedia data pelatihan dapat membuat beberapa model mirip yang dikonfigurasi dari satu model mirip.

5. Penyedia data pelatihan mengaitkan model audiens yang dikonfigurasi dengan kolaborasi yang dibagikan dengan penyedia data benih.

Ini adalah alur kerja yang harus diselesaikan oleh penyedia data seed selanjutnya:

1. Data penyedia data seed harus disimpan dalam bucket Amazon S3.
2. Penyedia data benih membuka kolaborasi yang mereka bagikan dengan penyedia data pelatihan.
3. Penyedia data seed membuat segmen mirip dari tab Clean Rooms di halaman kolaborasi.
4. Penyedia data benih dapat mengevaluasi metrik relevansi, jika dibagikan, dan mengekspor segmen yang mirip untuk digunakan di luar. AWS Clean Rooms

Perlindungan privasi dari AWS Clean Rooms ML

Clean Rooms ML dirancang untuk mengurangi risiko serangan inferensi keanggotaan di mana penyedia data pelatihan dapat mempelajari siapa yang ada dalam data benih dan penyedia data benih dapat mempelajari siapa yang ada dalam data pelatihan. Beberapa langkah diambil untuk mencegah serangan ini.

Pertama, penyedia data benih tidak secara langsung mengamati output Clean Rooms MS dan penyedia data pelatihan tidak pernah dapat mengamati data benih. Penyedia data benih dapat memilih untuk memasukkan data benih di segmen output.

Selanjutnya, model mirip dibuat dari sampel acak data pelatihan. Sampel ini mencakup sejumlah besar pengguna yang tidak cocok dengan audiens benih. Proses ini membuat lebih sulit untuk menentukan apakah pengguna tidak ada dalam data, yang merupakan jalan lain untuk inferensi keanggotaan.

Selanjutnya, beberapa pelanggan benih dapat digunakan untuk setiap parameter pelatihan model mirip spesifik benih. Ini membatasi seberapa banyak model yang dapat disesuaikan, dan dengan demikian berapa banyak yang dapat disimpulkan tentang pengguna. Sebagai hasilnya, kami merekomendasikan bahwa ukuran minimum data benih adalah 500 pengguna.

Akhirnya, metrik tingkat pengguna tidak pernah diberikan kepada penyedia data pelatihan, yang menghilangkan jalan lain untuk serangan inferensi keanggotaan.

AWS Clean Rooms Metrik evaluasi model ML

Clean Rooms MLmenghitung skor recall dan relevansi untuk menentukan seberapa baik kinerja model Anda. Recall membandingkan kesamaan antara data mirip dan data pelatihan. Skor relevansi digunakan untuk memutuskan seberapa besar audiens seharusnya, bukan apakah model tersebut berkinerja baik.

Ingat adalah ukuran yang tidak bias tentang seberapa mirip segmen yang mirip dengan data pelatihan. Recall adalah persentase pengguna yang paling mirip (secara default, 20% paling mirip) dari sampel data pelatihan yang disertakan dalam audiens benih oleh pekerjaan pembuatan audiens. Nilai berkisar dari 0-1, nilai yang lebih besar menunjukkan audiens yang lebih baik. Nilai recall kira-kira sama dengan persentase bin maksimum menunjukkan bahwa model audiens setara dengan pemilihan acak.

Kami menganggap ini sebagai metrik evaluasi yang lebih baik daripada akurasi, presisi, dan skor F1 karena Clean Rooms MLtidak secara akurat memberi label pengguna negatif sejati saat membangun modelnya.

Skor relevansi tingkat segmen adalah ukuran kesamaan dengan nilai mulai dari -1 (paling tidak mirip) hingga 1 (paling mirip). Clean Rooms MLmenghitung serangkaian skor relevansi untuk berbagai ukuran segmen untuk membantu Anda menentukan ukuran segmen terbaik untuk data Anda. Skor relevansi menurun secara monoton seiring bertambahnya ukuran segmen, sehingga seiring bertambahnya ukuran segmen, hal itu bisa kurang mirip dengan data benih. Ketika skor relevansi tingkat segmen mencapai 0, model memprediksi bahwa semua pengguna di segmen mirip berasal dari distribusi yang sama dengan data benih. Meningkatkan ukuran output kemungkinan akan menyertakan pengguna di segmen mirip yang tidak berasal dari distribusi yang sama dengan data benih.

Skor relevansi dinormalisasi dalam satu kampanye dan tidak boleh digunakan untuk membandingkan di seluruh kampanye. Skor relevansi tidak boleh digunakan sebagai bukti bersumber tunggal untuk hasil bisnis apa pun karena dipengaruhi oleh beberapa faktor kompleks selain relevansi, seperti kualitas inventaris, jenis inventaris, waktu iklan, dan sebagainya.

Skor relevansi tidak boleh digunakan untuk menilai kualitas benih, melainkan jika dapat ditingkatkan atau diturunkan. Pertimbangkan contoh berikut:

- Semua skor positif — Ini menunjukkan bahwa ada lebih banyak pengguna keluaran yang diprediksi serupa daripada yang termasuk dalam segmen mirip. Ini umum untuk data benih yang merupakan bagian dari pasar besar, seperti semua orang yang telah membeli pasta gigi dalam sebulan

terakhir. Kami merekomendasikan untuk melihat data benih yang lebih kecil, seperti semua orang yang telah membeli pasta gigi lebih dari sekali dalam sebulan terakhir.

- Semua skor negatif atau negatif untuk ukuran segmen mirip yang Anda inginkan — Ini menunjukkan bahwa Clean Rooms MS memprediksi tidak ada cukup pengguna serupa dalam ukuran segmen mirip yang diinginkan. Ini bisa jadi karena data benih terlalu spesifik atau pasarnya terlalu kecil. Kami merekomendasikan untuk menerapkan lebih sedikit filter ke data benih atau memperluas pasar. Misalnya, jika data benih asli adalah pelanggan yang membeli kereta dorong dan kursi mobil, Anda dapat memperluas pasar ke pelanggan yang membeli beberapa produk bayi.

Penyedia data pelatihan menentukan apakah skor relevansi diekspos dan keranjang tempat skor relevansi dihitung.

Bekerja dengan AWS Clean Rooms ML

Model mirip adalah model data penyedia data pelatihan yang memungkinkan penyedia data benih untuk membuat segmen serupa dari data penyedia data pelatihan yang paling mirip dengan data benih mereka. Untuk membuat model mirip yang dapat digunakan dalam kolaborasi, Anda harus mengimpor data pelatihan Anda, membuat model mirip, mengonfigurasi model yang mirip, dan kemudian mengaitkannya dengan kolaborasi.

Setelah penyedia data pelatihan selesai membuat model ML, penyedia data benih dapat membuat dan mengekspor segmen benih.

Topik

Bekerja dengan model yang mirip (penyedia data pelatihan)

Impor data pelatihan

Sebelum Anda membuat model mirip, Anda harus menentukan AWS Glue tabel yang berisi data pelatihan. Clean Rooms ML tidak menyimpan salinan data ini, hanya metadata yang memungkinkannya mengakses data.

Untuk mengimpor data pelatihan di AWS Clean Rooms

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Pemodelan Pemodelan.
3. Pada tab Kumpulan data Pelatihan, pilih Buat kumpulan data pelatihan.
4. Masukkan Nama dan Deskripsi opsional.
5. Untuk Sumber data, pilih AWS Glue tabel Anda:

   a. Pilih Database yang ingin Anda konfigurasikan dari daftar dropdown.

   b. Pilih sumber data Pelatihan dengan memilih Database dan Tabel yang ingin Anda konfigurasi dari daftar dropdown.

   > **Note**
   >
   > Untuk memverifikasi bahwa ini adalah tabel yang benar, lakukan salah satu dari yang berikut:
   >
   > - Pilih Lihat di AWS Glue.
   > - Aktifkan Lihat skema untuk melihat skema.

6. Untuk detail Pelatihan, pilih kolom Pengenal pengguna, kolom pengenal item, dan kolom stempel waktu dari data Anda. Data pelatihan harus berisi tiga kolom ini. Anda juga dapat memilih kolom lain yang ingin Anda sertakan dalam data pelatihan.

   Data di kolom Timestamp harus dalam waktu epoch Unix dalam format detik.

7. Dalam akses Layanan, Anda harus menentukan peran layanan yang dapat mengakses data Anda dan memberikan kunci KMS jika data Anda dienkripsi. Pilih Buat dan gunakan peran layanan baru dan Clean Rooms akan secara otomatis membuat peran layanan dan menambahkan kebijakan izin yang diperlukan. Pilih Gunakan peran layanan yang ada dan masukkan di bidang Nama peran layanan jika Anda memiliki peran layanan tertentu yang ingin Anda gunakan.

   Jika data Anda dienkripsi, masukkan kunci KMS Anda di AWS KMS keybidang, atau klik Buat AWS KMS key untuk menghasilkan kunci KMS baru.

8. Jika Anda ingin mengaktifkan Tag untuk kumpulan data pelatihan, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.
9. Pilih Buat kumpulan data pelatihan.

Untuk tindakan API terkait, lihat CreateTrainingDataset.

Buat model yang mirip

Setelah Anda membuat kumpulan data pelatihan, Anda siap untuk membuat model yang mirip. Anda dapat membuat banyak model mirip dari satu kumpulan data pelatihan.

Anda harus membuat database default di AWS Glue Data Catalog atau menyertakan `glue:createDatabase` izin dalam peran yang disediakan.

Untuk membuat model yang mirip di AWS Clean Rooms

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Pemodelan Pemodelan.
3. Pada tab Lookalike models, pilih Create lookalike model.
4. Untuk Buat model mirip, untuk detail model Lookalike:
    a. Masukkan Nama dan Deskripsi opsional.
    b. Pilih kumpulan data Pelatihan yang ingin Anda modelkan dari daftar tarik-turun.
    c. Masukkan jendela Pelatihan opsional.
5. Jika Anda ingin mengaktifkan pengaturan enkripsi khusus untuk model yang mirip, pilih Sesuaikan pengaturan enkripsi dan kemudian masukkan kunci KMS.
6. Jika Anda ingin mengaktifkan Tag untuk model mirip, pilih Tambahkan tag baru dan kemudian masukkan pasangan Kunci dan Nilai.
7. Pilih Buat model yang mirip.

Untuk tindakan API terkait, lihat CreateAudienceModel.

Konfigurasikan model yang mirip

Setelah Anda membuat model yang mirip, Anda siap mengonfigurasinya untuk digunakan dalam kolaborasi. Anda dapat membuat beberapa model mirip yang dikonfigurasi dari satu model mirip.

Untuk mengonfigurasi model yang mirip di AWS Clean Rooms

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Pemodelan Pemodelan.
3. Pada tab Configurated lookalike models, pilih Configure lookalike model.
4. Untuk Mengonfigurasi model mirip, untuk detail model mirip yang Dikonfigurasi:
    a. Masukkan Nama dan Deskripsi opsional.
    b. Pilih model Lookalike yang ingin Anda konfigurasikan dari daftar dropdown.
    c. Pilih ukuran benih pencocokan minimum yang Anda inginkan. Ini adalah jumlah minimum pengguna dalam data penyedia data benih yang tumpang tindih dengan pengguna dalam data pelatihan. Nilai ini harus lebih besar dari 0.
5. Agar Metrik dapat dibagikan dengan anggota lain, pilih apakah Anda ingin penyedia data benih dalam kolaborasi Anda menerima metrik model, termasuk skor relevansi.
6. Untuk lokasi tujuan segmen Lookalike, masukkan bucket Amazon S3 tempat segmen mirip diekspor. Bucket ini harus terletak di wilayah yang sama dengan sumber daya Anda yang lain.
7. Untuk akses Layanan, pilih nama peran layanan yang ada yang akan digunakan untuk mengakses tabel ini.
8. Pilih Konfigurasi Model Lookalike.
9. Jika Anda ingin mengaktifkan Tag untuk sumber daya tabel yang dikonfigurasi, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.

Untuk tindakan API terkait, lihat CreateConfiguredAudienceModel.

Kaitkan model mirip yang dikonfigurasi

Setelah Anda mengonfigurasi model yang mirip, Anda dapat mengaitkannya dengan kolaborasi.

Untuk mengaitkan model mirip yang dikonfigurasi di AWS Clean Rooms

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pada tab Dengan keanggotaan aktif, pilih kolaborasi.

4. Pada tab Pemodelan ML, pilih Associate lookalike model.
5. Untuk model mirip mirip yang dikonfigurasi Associate, untuk detail model mirip Associate:

    a. Masukkan Nama untuk model audiens yang dikonfigurasi terkait.

    b. Masukkan Deskripsi tabel.

    Deskripsi membantu membedakan antara model audiens terkonfigurasi terkait lainnya dengan nama yang mirip.
6. Untuk model mirip yang dikonfigurasi, pilih model mirip yang dikonfigurasi dari daftar tarik-turun.
7. Pilih Kaitkan.

Untuk tindakan API terkait, lihat CreateConfiguredAudienceModelAsosiasi.

Perbarui model mirip yang dikonfigurasi

Setelah mengaitkan model mirip yang dikonfigurasi, Anda dapat memperbaruinya untuk mengubah informasi seperti nama, metrik yang akan dibagikan, atau menampilkan lokasi Amazon S3.

Untuk memperbarui model mirip mirip yang dikonfigurasi terkait di AWS Clean Rooms

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih pemodelan ML.
3. Pada tab Configurated lookalike models, pilih model mirip yang dikonfigurasi dan pilih Edit.
4. Untuk Mengonfigurasi model mirip, untuk detail model mirip yang Dikonfigurasi:

    a. Pilih model Lookalike yang ingin Anda konfigurasi dari daftar dropdown.

    b. Pilih ukuran benih pencocokan minimum yang Anda inginkan. Ini adalah jumlah minimum pengguna dalam data penyedia data benih yang tumpang tindih dengan pengguna dalam data pelatihan. Nilai ini harus lebih besar dari 0.
5. Agar Metrik dapat dibagikan dengan anggota lain, pilih apakah Anda ingin penyedia data benih dalam kolaborasi Anda menerima metrik model, termasuk skor relevansi.
6. Untuk lokasi tujuan segmen Lookalike, masukkan bucket Amazon S3 tempat segmen mirip diekspor. Bucket ini harus terletak di wilayah yang sama dengan sumber daya Anda yang lain.
7. Untuk akses Layanan, pilih nama peran layanan yang ada yang akan digunakan untuk mengakses tabel ini.

8. Untuk konfigurasi ukuran tempat sampah lanjutan, pilih cara Anda ingin mengonfigurasi ukuran tempat sampah audiens.
9. Pilih Simpan perubahan.

Untuk tindakan API terkait, lihat UpdateConfiguredAudienceModel.

Bekerja dengan segmen yang mirip (penyedia data benih)

Buat segmen yang mirip

Segmen mirip adalah bagian dari data pelatihan yang paling mirip dengan data benih.

Untuk membuat segmen mirip di AWS Clean Rooms

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pada tab Dengan keanggotaan aktif, pilih kolaborasi.
4. Pada tab Modeling Ml, pilih Create lookalike segment.
5. Untuk Buat segmen mirip, untuk detail segmen Lookalike masukkan Nama dan Deskripsi opsional.
6. Untuk profil Seed, pilih sumber input Amazon S3 tempat data benih Anda disimpan.
7. Untuk akses Layanan, pilih nama peran layanan yang ada yang akan digunakan untuk mengakses tabel ini.
8. Jika Anda ingin mengaktifkan Tag untuk kumpulan data pelatihan, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.
9. Pilih Buat segmen mirip.

Untuk tindakan API terkait, lihat StartAudienceGenerationJob.

Ekspor segmen yang mirip

Setelah membuat segmen yang mirip, Anda dapat mengekspor data tersebut ke bucket Amazon S3.

Untuk mengekspor segmen yang mirip di AWS Clean Rooms

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pada tab Dengan keanggotaan aktif, pilih kolaborasi.
4. Pada tab Pemodelan ML, pilih segmen yang mirip dan pilih Ekspor.
5. Untuk model mirip Ekspor, untuk detail model mirip Ekspor masukkan Nama dan Deskripsi opsional.
6. Untuk ukuran Segmen, pilih ukuran yang Anda inginkan untuk segmen yang diekspor.
7. Pilih Ekspor.

Untuk tindakan API terkait, lihat StartAudienceExportJob.

Langkah selanjutnya

Sekarang setelah Anda membuat model yang mirip dan mengekspor segmen benih, Anda siap untuk:

- Mengelola AWS Clean Rooms

Komputasi Kriptografi untuk Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) adalah kemampuan AWS Clean Rooms yang dapat digunakan selain aturan analisis. Dengan C3R, organisasi dapat menyatukan data sensitif untuk memperoleh wawasan baru dari analitik data sementara secara kriptografis membatasi apa yang dapat dipelajari oleh pihak mana pun dalam prosesnya. C3R dapat digunakan oleh dua pihak atau lebih yang ingin berkolaborasi dengan data sensitif mereka tetapi diharuskan hanya menggunakan data terenkripsi di cloud.

Klien enkripsi C3R adalah alat enkripsi sisi klien yang dapat Anda gunakan untuk mengenkripsi data Anda untuk digunakan. AWS Clean Rooms Saat Anda menggunakan klien enkripsi C3R, data tetap dilindungi secara kriptografis saat digunakan dalam kolaborasi. AWS Clean Rooms Seperti halnya AWS Clean Rooms kolaborasi reguler, data input adalah tabel database relasional, dan komputasi dinyatakan sebagai query SQL. Namun, C3R hanya mendukung subset terbatas dari kueri SQL pada data terenkripsi.

Secara khusus, C3R mendukung SQL JOIN dan SELECT pernyataan pada data yang dilindungi secara kriptografi. Setiap kolom dalam tabel input dapat digunakan tepat di salah satu jenis pernyataan SQL berikut:

- Kolom yang dilindungi secara kriptografi untuk digunakan dalam JOIN pernyataan disebut fingerprint kolom.
- Kolom yang dilindungi secara kriptografi untuk digunakan dalam SELECT pernyataan disebut sealed kolom.
- Kolom yang tidak dilindungi secara kriptografi untuk digunakan dalam JOIN atau SELECT pernyataan disebut cleartext kolom.

Dalam beberapa kasus, GROUP BY pernyataan didukung pada fingerprint kolom. Untuk informasi selengkapnya, lihat Fingerprintkolom. Saat ini, C3R tidak mendukung penggunaan konstruksi SQL lainnya pada data terenkripsi, seperti WHERE klausa atau fungsi agregat seperti SUM danAVERAGE, bahkan jika tidak diizinkan oleh aturan analisis yang relevan.

C3R dirancang untuk melindungi data dalam sel individual tabel. Menggunakan konfigurasi default untuk C3R, data dasar yang disediakan pelanggan kepada pihak ketiga melalui kolaborasi tetap dienkripsi saat konten sedang digunakan di dalamnya. AWS Clean Rooms C3R menggunakan enkripsi AES-GCM standar industri untuk semua sealed kolom dan fungsi pseudorandom standar

industri, yang dikenal sebagai Kode Otentikasi Pesan berbasis Hash (HMAC), untuk melindungi kolom. fingerprint

Meskipun C3R mengenkripsi data dalam tabel Anda, informasi berikut mungkin masih dapat disimpulkan:

- Informasi tentang tabel itu sendiri, termasuk jumlah kolom, nama kolom, dan jumlah baris dalam tabel Anda.
- Seperti kebanyakan bentuk enkripsi standar, C3R tidak mencoba menyembunyikan panjang nilai terenkripsi. C3R memang menawarkan kemampuan untuk memasukkan nilai terenkripsi untuk menyembunyikan panjang teks yang tepat. Namun, batas atas pada panjang cleartext di setiap kolom masih bisa diungkapkan ke pihak lain.
- Informasi tingkat pencatatan, seperti ketika baris tertentu ditambahkan ke tabel C3R terenkripsi.

Untuk informasi selengkapnya tentang C3R, lihat topik berikut.

Topik

Pertimbangan saat menggunakan Komputasi Kriptografi untuk Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) berupaya memaksimalkan perlindungan data. Namun, beberapa kasus penggunaan mungkin mendapat manfaat dari tingkat perlindungan data yang lebih rendah dengan imbalan fungsionalitas tambahan. Anda dapat membuat pengorbanan khusus ini dengan memodifikasi C3R dari konfigurasi yang paling aman. Sebagai pelanggan, Anda

harus menyadari pengorbanan ini dan menentukan apakah mereka sesuai untuk kasus penggunaan Anda. Pengorbanan untuk dipertimbangkan meliputi yang berikut:

Topik

- Mengizinkan data campuran cleartext dan terenkripsi dalam tabel Anda
- Mengizinkan nilai berulang dalam fingerprint kolom
- Melonggarkan pembatasan tentang bagaimana fingerprint kolom diberi nama
- Menentukan bagaimana NULL nilai direpresentasikan

Untuk informasi selengkapnya tentang cara mengatur parameter untuk skenario ini, lihatParameter komputasi kriptografi.

Mengizinkan data campuran cleartext dan terenkripsi dalam tabel Anda

Memiliki semua data dienkripsi sisi klien memberikan perlindungan data maksimum. Namun, ini membatasi jenis kueri tertentu (misalnya, fungsi SUM agregat). Risiko mengizinkan cleartext data adalah layak bahwa siapa pun yang memiliki akses ke tabel terenkripsi dapat menyimpulkan beberapa informasi tentang nilai terenkripsi. Ini dapat dilakukan dengan melakukan analisis statistik pada cleartext dan data terkait.

Misalnya, bayangkan Anda memiliki kolom `City` dan`State`. `City`Kolom adalah cleartext dan `State` kolom dienkripsi. Ketika Anda melihat nilai `Chicago` di `City` kolom, itu membantu Anda menentukan dengan probabilitas tinggi bahwa `State` itu`Illinois`. Sebaliknya, jika satu kolom `City` dan kolom lainnya`EmailAddress`, a cleartext `City` tidak mungkin mengungkapkan apa pun tentang terenkripsi`EmailAddress`.

Untuk informasi selengkapnya tentang parameter untuk skenario ini, lihatIzinkan parameter cleartext kolom.

Mengizinkan nilai berulang dalam fingerprint kolom

Untuk pendekatan yang paling aman, kami berasumsi bahwa fingerprint kolom apa pun berisi persis satu instance variabel. Tidak ada item yang dapat diulang dalam fingerprint kolom. Klien enkripsi C3R memetakan cleartext nilai-nilai ini menjadi nilai unik yang tidak dapat dibedakan dari nilai acak. Oleh karena itu, tidak mungkin untuk menyimpulkan informasi tentang cleartext dari nilai-nilai acak ini.

Risiko nilai berulang dalam fingerprint kolom adalah bahwa nilai berulang akan menghasilkan nilai yang tampak acak berulang. Dengan demikian, siapa pun yang memiliki akses ke tabel terenkripsi

dapat, secara teori, melakukan analisis statistik fingerprint kolom yang mungkin mengungkapkan informasi tentang cleartext nilai.

Sekali lagi, misalkan fingerprint kolomnya`State`, dan setiap baris tabel sesuai dengan rumah tangga AS. Dengan melakukan analisis frekuensi, seseorang dapat menyimpulkan keadaan mana `California` dan mana `Wyoming` dengan probabilitas tinggi. Kesimpulan ini dimungkinkan karena `California` memiliki lebih banyak penduduk daripada`Wyoming`. Sebaliknya, katakanlah fingerprint kolom berada pada pengidentifikasi rumah tangga dan setiap rumah tangga muncul dalam database antara 1 dan 4 kali dalam database jutaan entri. Tidak mungkin analisis frekuensi akan mengungkapkan informasi yang berguna.

Untuk informasi selengkapnya tentang parameter untuk skenario ini, lihatIzinkan parameter duplikat.

Melonggarkan pembatasan tentang bagaimana fingerprint kolom diberi nama

Secara default, kami berasumsi bahwa ketika dua tabel digabungkan menggunakan kolom terenkripsi, fingerprint kolom tersebut memiliki nama yang sama di setiap tabel. Alasan teknis untuk hasil ini adalah bahwa, secara default, kami memperoleh kunci kriptografi yang berbeda untuk mengenkripsi setiap kolom. fingerprint Kunci itu berasal dari kombinasi kunci rahasia bersama untuk kolaborasi dan nama kolom. Jika kami mencoba menggabungkan dua kolom dengan nama kolom yang berbeda, kami memperoleh kunci yang berbeda dan kami tidak dapat menghitung gabungan yang valid.

Untuk mengatasi masalah ini, Anda dapat menonaktifkan fitur yang memperoleh kunci dari setiap nama kolom. Kemudian, klien enkripsi C3R menggunakan kunci turunan tunggal untuk semua fingerprint kolom. Risikonya adalah bahwa jenis lain dari analisis frekuensi dapat dilakukan yang mungkin mengungkapkan informasi.

Mari kita gunakan `State` contoh `City` dan lagi. Jika kita memperoleh nilai acak yang sama untuk setiap fingerprint kolom (dengan tidak memasukkan nama kolom). `New York`memiliki nilai acak yang sama di `State` kolom `City` dan. New York adalah salah satu dari beberapa kota di AS di mana `City` namanya sama dengan `State` namanya. Sebaliknya, jika kumpulan data Anda memiliki nilai yang sama sekali berbeda di setiap kolom, tidak ada informasi yang bocor.

Untuk informasi selengkapnya tentang parameter untuk skenario ini, lihatIzinkan JOIN kolom dengan parameter nama yang berbeda.

Menentukan bagaimana NULL nilai direpresentasikan

Opsi yang tersedia untuk Anda adalah apakah akan memproses nilai kriptografi (enkripsi dan HMAC) seperti NULL nilai lainnya. Jika Anda tidak memproses NULL nilai seperti nilai lainnya, informasi mungkin akan terungkap.

Misalnya, anggaplah bahwa NULL di `Middle Name` kolom di cleartext menunjukkan orang tanpa nama tengah. Jika Anda tidak mengenkripsi nilai-nilai tersebut, Anda membocorkan baris mana dalam tabel terenkripsi yang digunakan untuk orang tanpa nama tengah. Informasi itu mungkin menjadi sinyal pengenal bagi beberapa orang di beberapa populasi. Tetapi jika Anda memproses NULL nilai secara kriptografi, kueri SQL tertentu bertindak berbeda. Misalnya, GROUP BY klausa tidak akan mengelompokkan fingerprint NULL nilai dalam fingerprint kolom bersama-sama.

Untuk informasi selengkapnya tentang parameter untuk skenario ini, lihatPertahankan parameter NULL nilai.

Jenis file dan data yang didukung dalam Komputasi Kriptografi untuk Clean Rooms

Klien enkripsi C3R mengenali jenis file berikut:

- Berkas CSV
- Parquetberkas

Anda dapat menggunakan `--fileFormat` bendera di klien enkripsi C3R untuk menentukan format file secara eksplisit. Ketika ditentukan secara eksplisit, format file tidak ditentukan oleh ekstensi file.

Topik

- Berkas CSV
- Parquetberkas
- Mengenkripsi nilai non-string

Berkas CSV

File dengan ekstensi.csv diasumsikan berformat CSV dan berisi teks yang dikodekan UTF-8. Klien enkripsi C3R memperlakukan semua nilai sebagai string.

Properti yang didukung dalam file.csv

Klien enkripsi C3R mensyaratkan bahwa file.csv memiliki properti berikut:

- Mungkin atau mungkin tidak berisi baris header awal yang secara unik menamai setiap kolom.
- Dibatasi koma. (Saat ini, pembatas khusus tidak didukung.)
- Teks yang dikodekan UTF-8.

Pemangkasan ruang putih dari entri .csv

Spasi putih depan dan belakang dipangkas dari entri .csv.

NULLPengkodean khusus untuk file.csv

File.csv dapat menggunakan pengkodean khususNULL.

Dengan klien enkripsi C3R, Anda dapat menentukan pengkodean kustom untuk NULL entri dalam data input dengan menggunakan bendera. `--csvInputNULLValue=<csv-input-null>` Klien enkripsi C3R dapat menggunakan pengkodean khusus dalam file keluaran yang dihasilkan untuk entri NULL dengan menggunakan bendera. `--csvOutputNULLValue=<csv-output-null>`

> **Note**
>
> NULLEntri dianggap kurang konten, khususnya dalam konteks format tabel yang lebih kaya seperti tabel SQL. Meskipun .csv tidak secara eksplisit mendukung karakterisasi ini karena alasan historis, itu adalah konvensi umum untuk mempertimbangkan entri kosong yang hanya berisi spasi putih. NULL Oleh karena itu, itulah perilaku default klien enkripsi C3R dan dapat disesuaikan sesuai kebutuhan.

Bagaimana entri .csv ditafsirkan oleh C3R

Tabel berikut memberikan contoh bagaimana entri .csv disusun (cleartextcleartextuntuk kejelasan) berdasarkan nilai (jika ada) yang disediakan untuk dan flag. `--csvInputNULLValue=<csv-input-null>` `--csvOutputNULLValue=<csv-output-null>` Memimpin dan membuntuti ruang putih di luar tanda kutip dipangkas sebelum C3R menafsirkan makna nilai apa pun.

<csv-input-null>	**<csv-output-null>**	Masukan entri	Entri keluaran
Tidak ada	Tidak ada	,AnyProduct,	,AnyProduct,
Tidak ada	Tidak ada	, AnyProduct ,	,AnyProduct,
Tidak ada	Tidak ada	,"AnyProduct",	,AnyProduct,
Tidak ada	Tidak ada	, "AnyProduct" ,	,AnyProduct,
Tidak ada	Tidak ada	,,	,,
Tidak ada	Tidak ada	, ,	,,
Tidak ada	Tidak ada	,"",	,,
Tidak ada	Tidak ada	," ",	," ",
Tidak ada	Tidak ada	, " " ,	," ",
"AnyProduct"	"NULL"	,AnyProduct,	,NULL,
"AnyProduct"	"NULL"	, AnyProduct ,	,NULL,
"AnyProduct"	"NULL"	,"AnyProduct",	,NULL,
"AnyProduct"	"NULL"	, "AnyProduct" ,	,NULL,
Tidak ada	"NULL"	,,	,NULL,
Tidak ada	"NULL"	, ,	,NULL,
Tidak ada	"NULL"	,"",	,NULL,
Tidak ada	"NULL"	," ",	," ",
Tidak ada	"NULL"	, " " ,	," ",
""	"NULL"	,,	,NULL,

<csv-input-null>	**<csv-output-null>**	Masukan entri	Entri keluaran
""	"NULL"	, ,	,NULL,
""	"NULL"	,"",	,"",
""	"NULL"	," ",	," ",
""	"NULL"	, " " ,	," ",
"\"\""	"NULL"	,,	,,
"\"\""	"NULL"	, ,	,,
"\"\""	"NULL"	,"",	,NULL,
"\"\""	"NULL"	," ",	," ",
"\"\""	"NULL"	, " " ,	," ",

File CSV tanpa header

File sumber.csv tidak perlu memiliki header di baris pertama yang secara unik memberi nama setiap kolom. Namun, file.csv tanpa baris header memerlukan skema enkripsi posisi. Skema enkripsi posisi diperlukan alih-alih skema pemetaan khas yang digunakan untuk file.csv dengan baris header dan file. Parquet

Skema enkripsi posisi menentukan kolom keluaran berdasarkan posisi, bukan dengan nama. Skema enkripsi yang dipetakan memetakan nama kolom sumber untuk menargetkan nama kolom. Untuk informasi lebih lanjut, termasuk diskusi rinci dan contoh dari kedua format skema, lihatSkema tabel yang dipetakan dan posisi.

Parquetberkas

File dengan .parquet ekstensi diasumsikan dalam Apache Parquet format.

Tipe Parquet data yang didukung

Klien enkripsi C3R dapat memproses data non-kompleks (yaitu tipe primitif) dalam Parquet file yang mewakili tipe data yang didukung oleh. AWS Clean Rooms

Namun, hanya kolom string yang dapat digunakan untuk sealed kolom.

Tipe data Parket berikut didukung:

- `Binary`tipe primitif dengan anotasi logis berikut:
  - Tidak ada jika `--parquetBinaryAsString` diatur (tipe `STRING` data)
  - `Decimal(scale, precision)`(tipe `DECIMAL` data)
  - `String`(tipe `STRING` data)
- `Boolean`tipe data primitif tanpa anotasi logis (tipe `BOOLEAN` data)
- `Double`tipe data primitif tanpa anotasi logis (tipe `DOUBLE` data)
- `Fixed_Len_Binary_Array`tipe primitif dengan anotasi `Decimal(scale, precision)` logis (tipe `DECIMAL` data)
- `Float`tipe data primitif tanpa anotasi logis (tipe `FLOAT` data)
- `Int32`tipe primitif dengan anotasi logis berikut:
  - Tidak ada (tipe `INT` data)
  - `Date`(tipe `DATE` data)
  - `Decimal(scale, precision)`(tipe `DECIMAL` data)
  - `Int(16, true)`(tipe `SMALLINT` data)
  - `Int(32, true)`(tipe `INT` data)
- `Int64`tipe data primitif dengan anotasi logis berikut:
  - Tidak ada (tipe `BIGINT` data)
  - `Decimal(scale, precision)`(tipe `DECIMAL` data)
  - `Int(64, true)`(tipe `BIGINT` data)
  - `Timestamp(isUTCAdjusted, TimeUnit.MILLIS)`(tipe `TIMESTAMP` data)
  - `Timestamp(isUTCAdjusted, TimeUnit.MICROS)`(tipe `TIMESTAMP` data)
  - `Timestamp(isUTCAdjusted, TimeUnit.NANOS)`(tipe `TIMESTAMP` data)

Mengenkripsi nilai non-string

Saat ini, hanya nilai string yang didukung untuk sealed kolom.

Untuk file.csv, klien enkripsi C3R memperlakukan semua nilai sebagai teks yang dikodekan UTF-8 dan tidak berusaha untuk menafsirkannya secara berbeda sebelum enkripsi.

Untuk kolom sidik jari, jenis dikelompokkan ke dalam kelas ekivalensi. Kelas kesetaraan adalah sekumpulan tipe data yang dapat dibandingkan secara jelas untuk kesetaraan melalui tipe data yang representatif.

Kelas kesetaraan memungkinkan sidik jari identik untuk ditetapkan ke nilai semantik yang sama terlepas dari representasi aslinya. Namun, nilai yang sama dalam dua kelas ekivalensi tidak akan menghasilkan kolom sidik jari yang sama.

Misalnya, `INTEGRAL` nilai `42` akan diberikan sidik jari yang sama terlepas dari apakah itu awalnya`SMALLINT`,`INT`, atau`BIGINT`. Juga, `INTEGRAL` nilai tidak `0` akan pernah cocok dengan `BOOLEAN` nilai `FALSE` (yang diwakili oleh nilai`0`).

Kelas kesetaraan berikut dan tipe AWS Clean Rooms data yang sesuai didukung oleh kolom sidik jari:

Kelas kesetaraan	Tipe AWS Clean Rooms data yang didukung
`BOOLEAN`	`BOOLEAN`
`DATE`	`DATE`
`INTEGRAL`	`BIGINT`, `INT`, `SMALLINT`
`STRING`	`CHAR`, `STRING`, `VARCHAR`

Nama kolom dalam Komputasi Kriptografi untuk Clean Rooms

Secara default, nama-nama kolom penting dalam Komputasi Kriptografi untukClean Rooms.

Jika nilai Izinkan JOIN kolom dengan parameter nama yang berbeda salah, nama kolom digunakan selama enkripsi fingerprint kolom. Untuk alasan ini, secara default, kolaborator harus

berkoordinasi terlebih dahulu dan menggunakan nama kolom target yang sama untuk data yang akan menggunakan JOIN pernyataan dalam kueri. Secara default, kolom yang dienkripsi JOIN dengan nama berbeda tidak berhasil JOIN pada nilai apa pun.

Jika nilai Izinkan JOIN kolom dengan parameter nama yang berbeda benar, JOIN pernyataan di seluruh kolom dienkripsi sebagai fingerprint kolom berhasil. Mengenkripsi data dengan parameter ini mungkin memungkinkan beberapa inferensi nilai. cleartext Misalnya, jika baris memiliki nilai Kode Otentikasi Pesan (HMAC) berbasis Hash yang sama di `City` kolom dan `State` kolom, nilainya mungkin. `New York`

Normalisasi nama header kolom

Nama header kolom dinormalisasi oleh klien enkripsi C3R. Setiap spasi putih depan dan belakang dihapus, dan nama kolom dibuat huruf kecil untuk output yang diubah.

Normalisasi diterapkan sebelum semua perhitungan, perhitungan, atau operasi lain yang mungkin dapat dipengaruhi oleh nama kolom. File keluaran yang dipancarkan hanya berisi nama yang dinormalisasi.

Jenis kolom dalam Komputasi Kriptografi untuk Clean Rooms

Topik ini memberikan informasi tentang jenis kolom dalam Komputasi Kriptografi untukClean Rooms.

Topik

- Fingerprintkolom
- Kolom tertutup
- Cleartextkolom

Fingerprintkolom

Fingerprintkolom adalah kolom yang dilindungi secara kriptografi untuk digunakan dalam JOIN pernyataan.

Data dari fingerprint kolom tidak dapat didekripsi. Hanya data dari kolom tertutup yang dapat didekripsi.

Fingerprintkolom hanya boleh digunakan dalam klausa dan fungsi SQL berikut:

- JOIN (INNER, OUTER, LEFT, RIGHT, or FULL)terhadap fingerprint kolom lain:
  - Jika nilai `allowJoinsOnColumnsWithDifferentNames` parameter diatur ke`false`, kedua fingerprint kolom juga JOIN harus memiliki nama yang sama.
- `SELECT COUNT()`
- `SELECT COUNT(DISTINCT )`
- `GROUP BY`(Hanya gunakan jika kolaborasi telah menetapkan nilai `preserveNulls` parameter ke`true`.)

Kueri yang melanggar batasan ini mungkin menghasilkan hasil yang salah.

Kolom tertutup

Kolom tertutup adalah kolom yang dilindungi secara kriptografis untuk digunakan dalam SELECT pernyataan.

Kolom tertutup hanya boleh digunakan dalam klausa dan fungsi SQL berikut:

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

> **Note**
>
> `SELECT COUNT(DISTINCT )` tidak didukung.

Kueri yang melanggar batasan ini mungkin menghasilkan hasil yang salah.

Padding data untuk sealed kolom sebelum enkripsi

Saat Anda menentukan bahwa kolom harus berupa sealed kolom, C3R menanyakan padding jenis apa yang harus dipilih. Padding data sebelum enkripsi adalah opsional. Tanpa padding (tipe padnone), panjang data terenkripsi menunjukkan ukuran. cleartext Dalam beberapa keadaan, ukuran cleartext dapat mengekspos plaintext. Dengan padding (tipe pad `fixed` ataumax), semua nilai pertama-tama diempuk ke ukuran umum dan kemudian dienkripsi. Dengan padding, panjang data terenkripsi tidak memberikan informasi tentang cleartext panjang aslinya, selain memberikan batas atas pada ukurannya.

Jika Anda ingin padding untuk kolom dan panjang byte maksimal data di kolom itu diketahui, gunakan `fixed` padding. Gunakan `length` nilai yang setidaknya sebesar panjang byte dari nilai terpanjang di kolom itu.

> **Note**
>
> Terjadi kesalahan dan enkripsi gagal jika nilai lebih panjang dari yang disediakan`length`.

Jika Anda ingin padding untuk kolom dan panjang byte maksimal data di kolom itu tidak diketahui, gunakan `max` padding. Mode padding ini membungkus semua data dengan panjang nilai terpanjang ditambah `length` byte tambahan.

> **Note**
>
> Anda mungkin ingin mengenkripsi data dalam batch, atau memperbarui tabel Anda dengan data baru secara berkala. Ketahuilah bahwa `max` padding akan memasukkan entri ke panjang (plus `length` byte) dari entri plaintext terpanjang dalam batch tertentu. Ini berarti bahwa panjang ciphertext dapat bervariasi dari batch ke batch. Oleh karena itu, jika Anda mengetahui panjang byte maksimum untuk kolom, maka Anda harus menggunakan `fixed` sebagai gantinya. `max`

Cleartextkolom

Cleartextkolom adalah kolom yang tidak dilindungi secara kriptografis untuk digunakan dalam JOIN atau SELECT pernyataan.

Cleartextkolom dapat digunakan di bagian manapun dari query SQL.

Parameter komputasi kriptografi

Parameter komputasi kriptografi tersedia untuk kolaborasi menggunakan Cryptographic Computing for Clean Rooms (C3R) saat membuat kolaborasi. Anda dapat membuat kolaborasi menggunakan AWS Clean Rooms konsol atau operasi `CreateCollaboration` API. Di konsol, Anda dapat mengatur nilai untuk parameter dalam parameter komputasi kriptografi setelah Anda mengaktifkan opsi komputasi kriptografi Support. Untuk informasi selengkapnya, lihat topik berikut.

Topik

Izinkan parameter cleartext kolom

Di konsol, Anda dapat mengatur parameter Izinkan cleartext kolom saat membuat kolaborasi untuk menentukan apakah cleartext data diizinkan dalam tabel dengan data terenkripsi.

Tabel berikut menjelaskan nilai-nilai untuk parameter Izinkan cleartext kolom.

Nilai parameter	Deskripsi
Tidak	Cleartextkolom tidak diizinkan dalam tabel terenkripsi. Semua data dilindungi secara kriptografi.
Ya	Cleartextkolom diperbolehkan dalam tabel terenkripsi. Cleartextkolom tidak dilindungi secara kriptografis dan disertaka n sebagai. cleartext Anda harus mencatat apa yang mungkin diungkapkan oleh cleartext data baris Anda tentang data lain dalam tabel. Untuk menjalankan SUM atau AVG pada kolom tertentu, kolom harus masukcleartext.

Menggunakan operasi `CreateCollaboration` API, untuk `dataEncryptionMetadata` parameter, Anda dapat mengatur nilai `allowCleartext` ke `true` atau`false`. Untuk informasi selengkapnya tentang operasi API, lihat Referensi AWS Clean Rooms API.

Cleartextkolom sesuai dengan kolom yang diklasifikasikan sebagai cleartext dalam skema khusus tabel. Data dalam kolom ini tidak dienkripsi dan dapat digunakan dengan cara apa pun. Cleartextkolom dapat berguna jika data tidak sensitif dan/atau jika lebih banyak fleksibilitas diperlukan daripada sealed kolom atau fingerprint kolom terenkripsi memungkinkan.

Izinkan parameter duplikat

Di konsol, Anda dapat mengatur parameter Izinkan duplikat saat membuat kolaborasi untuk menentukan apakah kolom yang dienkripsi untuk JOIN kueri dapat berisi duplikat non-nilai. NULL

> **Important**
>
> Parameter Izinkan duplikat, JOINIzinkan kolom dengan nama yang berbeda, dan Pertahankan NULL nilai memiliki efek terpisah tetapi terkait.

Tabel berikut menjelaskan nilai untuk parameter Izinkan duplikat.

Nilai parameter	Deskripsi
Tidak	Nilai berulang tidak diperbolehkan dalam fingerprint kolom. Semua nilai dalam satu fingerprint kolom harus unik.
Ya	Nilai berulang diperbolehkan dalam fingerprint kolom. Jika Anda perlu menggabungkan kolom dengan nilai berulang, atur nilai ini ke Ya. Ketika diatur ke Ya, pola frekuensi yang muncul dalam fingerprint kolom dalam tabel C3R atau hasil mungkin menyiratkan beberapa informasi tambahan tentang struktur data. cleartext

Menggunakan operasi `CreateCollaboration` API, untuk `dataEncryptionMetadata` parameter Anda dapat mengatur nilai `allowDuplicates` ke `true` atau`false`. Untuk informasi selengkapnya tentang operasi API, lihat Referensi AWS Clean Rooms API.

Secara default, jika data terenkripsi harus digunakan dalam JOIN kueri, klien enkripsi C3R mengharuskan kolom tersebut tidak memiliki nilai duplikat. Persyaratan ini merupakan upaya untuk meningkatkan perlindungan data. Perilaku ini dapat membantu memastikan bahwa pola berulang dalam data tidak dapat diamati. Namun, jika Anda ingin bekerja dengan data terenkripsi dalam JOIN kueri dan tidak peduli tentang nilai duplikat, parameter Izinkan duplikat dapat menonaktifkan pemeriksaan konservatif ini.

Izinkan JOIN kolom dengan parameter nama yang berbeda

Di konsol, Anda dapat mengatur parameter Izinkan JOIN kolom dengan nama yang berbeda saat membuat kolaborasi untuk menentukan apakah JOIN pernyataan antara kolom dengan nama berbeda didukung.

Untuk informasi selengkapnya, lihat Normalisasi nama header kolom

Tabel berikut menjelaskan nilai untuk Izinkan JOIN kolom dengan parameter nama yang berbeda.

Nilai parameter	Deskripsi
Tidak	Gabungan fingerprint kolom dengan nama berbeda tidak didukung. JOINpernyataan hanya memberikan hasil yang akurat pada kolom yang memiliki nama yang sama. **Important** Nilai No memberikan peningkatan keamanan informasi tetapi mengharuskan peserta kolaborasi untuk menyetujui sebelumnya tentang nama kolom. Jika dua kolom memiliki nama yang berbeda ketika dienkripsi sebagai fingerprint kolom dan Izinkan JOIN kolom dengan nama yang berbeda diatur ke Tidak, JOIN pernyataan pada kolom tersebut tidak menghasilkan hasil. Ini karena tidak ada nilai pasca-enkripsi yang dibagi di antara mereka.
Ya	Gabungan fingerprint kolom dengan nama berbeda didukung. Untuk fleksibilitas tambahan, pengguna dapat mengatur nilai ini ke Ya, yang memungkinkan JOIN pernyataan pada kolom terlepas dari nama kolom mereka. Jika disetel ke Ya, klien enkripsi C3R tidak mempertimbangkan nama kolom saat melindungi fingerprint kolom. Akibatnya, nilai umum di fingerprint kolom yang berbeda dapat diamati dalam tabel C3R.

Nilai parameter	Deskripsi
	Misalnya, jika baris memiliki JOIN nilai terenkripsi yang sama di `City` kolom dan `State` kolom, mungkin masuk akal untuk menyimpulkan bahwa nilainya adalah. `New York`

Menggunakan operasi `CreateCollaboration` API, untuk `dataEncryptionMetadata` parameter, Anda dapat mengatur nilai `allowJoinsOnColumnsWithDifferentNames` ke `true` atau`false`. Untuk informasi selengkapnya tentang operasi API, lihat Referensi AWS Clean Rooms API.

Secara default, enkripsi fingerprint kolom dipengaruhi oleh kolom `targetHeader` untuk itu, diaturLangkah 4: Buat skema enkripsi untuk file tabular . Oleh karena itu, cleartext nilai yang sama memiliki representasi terenkripsi yang berbeda di setiap fingerprint kolom yang berbeda yang dienkripsi untuknya.

Parameter ini dapat berguna untuk mencegah inferensi cleartext nilai dalam beberapa kasus. Misalnya, melihat nilai terenkripsi yang sama di fingerprint kolom `City` dan `State` dapat digunakan untuk menyimpulkan nilainya secara wajar. `New York` Namun, penggunaan parameter ini memerlukan koordinasi tambahan terlebih dahulu, sehingga semua kolom yang akan digabungkan dalam kueri memiliki nama bersama.

Anda dapat menggunakan Izinkan JOIN kolom dengan parameter nama yang berbeda untuk melonggarkan batasan ini. Ketika nilai parameter disetel ke`Yes`, ini memungkinkan kolom apa pun yang dienkripsi JOIN untuk digunakan bersama terlepas dari nama.

Pertahankan parameter NULL nilai

Di konsol, Anda dapat mengatur parameter Pertahankan NULL nilai saat membuat kolaborasi untuk menunjukkan bahwa tidak ada nilai yang ada untuk kolom tersebut.

Tabel berikut menjelaskan nilai untuk parameter Preserve NULL values.

Nilai parameter	Deskripsi
Tidak	NULLnilai-nilai tidak dipertahankan. NULLnilai tidak muncul seperti NULL dalam tabel terenkripsi. NULLnilai muncul sebagai nilai acak unik dalam tabel C3R.

Nilai parameter	Deskripsi
Ya	NULLnilai-nilai dipertahankan. NULLnilai muncul seperti NULL dalam tabel terenkripsi. Jika Anda memerlukan semantik SQL NULL nilai, Anda dapat mengatur nilai ini ke Ya. Akibatnya , NULL entri muncul seperti NULL pada tabel C3R, terlepas dari apakah kolom dienkripsi dan terlepas dari pengaturan parameter untuk Izinkan duplikat.

Menggunakan operasi `CreateCollaboration` API, untuk `dataEncryptionMetadata` parameter, Anda dapat mengatur nilai `preserveNulls` ke `true` atau`false`. Untuk informasi selengkapnya tentang operasi API, lihat Referensi AWS Clean Rooms API.

Saat parameter Pertahankan NULL nilai disetel ke Tidak untuk kolaborasi:

1. NULLentri dalam `cleartext` kolom tidak berubah.
2. NULLentri dalam `fingerprint` kolom terenkripsi dienkripsi sebagai nilai acak untuk menyembunyikan isinya. Bergabung di kolom terenkripsi dengan NULL entri di cleartext kolom tidak menghasilkan kecocokan apa pun untuk entri mana pun. NULL Tidak ada kecocokan yang dibuat karena mereka masing-masing menerima konten acak unik mereka sendiri.
3. NULLentri dalam `sealed` kolom terenkripsi dienkripsi.

Ketika nilai parameter Pertahankan NULL nilai disetel ke Ya untuk kolaborasi, NULL entri dari semua kolom tetap sebagai NULL terlepas dari apakah kolom dienkripsi.

Parameter Preserve NULL values berguna dalam skenario seperti pengayaan data, di mana Anda ingin berbagi kekurangan informasi yang dinyatakan sebagai. NULL Parameter Preserve NULL values juga berguna dalam format fingerprint atau HMAC jika Anda memiliki NULL nilai di kolom yang Anda inginkan JOIN atauGROUP BY.

Jika nilai parameter Izinkan duplikat dan Pertahankan NULL nilai diatur ke Tidak, memiliki lebih dari satu NULL entri dalam fingerprint kolom menghasilkan kesalahan dan menghentikan enkripsi. Jika nilai salah satu parameter disetel ke Ya, tidak ada kesalahan seperti itu terjadi.

Bendera opsional dalam Komputasi Kriptografi untuk Clean Rooms

Bagian berikut menjelaskan flag opsional yang dapat Anda atur saat Anda mengenkripsi data menggunakan klien enkripsi C3R untuk kustomisasi dan pengujian file tabular.

Topik

`--csvInputNULLValue`bendera

Anda dapat menggunakan `--csvInputNULLValue` bendera untuk menentukan pengkodean kustom untuk NULL entri dalam data input saat Anda mengenkripsi data menggunakan klien enkripsi C3R.

Tabel berikut merangkum penggunaan dan parameter flag ini.

Penggunaan	Parameter
Tidak wajib. Pengguna dapat menentukan pengkodean khusus untuk NULL entri dalam data input.	Pengkodean NULL nilai yang ditentukan pengguna dalam file CSV input

NULLEntri adalah entri yang dianggap kurang konten, khususnya dalam konteks format tabel yang lebih kaya seperti tabel SQL. Meskipun .csv tidak secara eksplisit mendukung karakterisasi ini karena alasan historis, itu adalah konvensi umum untuk mempertimbangkan entri kosong yang hanya berisi spasi putih. NULL Oleh karena itu, itulah perilaku default klien enkripsi C3R dan dapat disesuaikan sesuai kebutuhan.

`--csvOutputNULLValue`bendera

Anda dapat menggunakan `--csvOutputNULLValue` bendera untuk menentukan pengkodean kustom untuk NULL entri dalam data keluaran saat Anda mengenkripsi data menggunakan klien enkripsi C3R.

Tabel berikut merangkum penggunaan dan parameter flag ini.

Penggunaan	Parameter
Tidak wajib. Pengguna dapat menentukan pengkodean khusus dalam file keluaran yang dihasilkan untuk NULL entri.	Pengkodean NULL nilai yang ditentukan pengguna dalam file CSV keluaran

NULLEntri adalah entri yang dianggap kurang konten, khususnya dalam konteks format tabel yang lebih kaya seperti tabel SQL. Meskipun .csv tidak secara eksplisit mendukung karakterisasi ini karena alasan historis, itu adalah konvensi umum untuk mempertimbangkan entri kosong yang hanya berisi spasi putih. NULL Oleh karena itu, itulah perilaku default klien enkripsi C3R dan dapat disesuaikan sesuai kebutuhan.

`--enableStackTraces`bendera

Saat Anda mengenkripsi data menggunakan klien enkripsi C3R, gunakan `--enableStackTraces` tanda untuk memberikan informasi kontekstual tambahan untuk pelaporan kesalahan saat C3R menemukan kesalahan.

AWS tidak mengumpulkan kesalahan. Jika Anda mengalami kesalahan, gunakan jejak tumpukan untuk memecahkan masalah kesalahan sendiri atau mengirim jejak tumpukan AWS Support untuk mendapatkan bantuan.

Tabel berikut merangkum penggunaan dan parameter flag ini.

Penggunaan	Parameter
Tidak wajib. Digunakan untuk memberikan informasi kontekstual tambahan untuk pelaporan kesalahan ketika klien enkripsi C3R mengalami kesalahan.	Tidak ada

`--dryRun`bendera

Enkripsi dan dekripsi perintah klien enkripsi C3R menyertakan bendera opsional. `--dryRun` Bendera mengambil semua argumen yang disediakan pengguna dan memeriksa validitas dan konsistensi.

Anda dapat menggunakan `--dryRun` bendera untuk memeriksa apakah file skema Anda valid dan konsisten dengan file input yang sesuai.

Tabel berikut merangkum penggunaan dan parameter flag ini.

Penggunaan	Parameter
Tidak wajib. Menyebabkan klien enkripsi C3R mengurai parameter dan memeriksa file, tetapi tidak melakukan enkripsi atau dekripsi.	Tidak ada

`--tempDir`bendera

Anda mungkin ingin menggunakan direktori sementara karena file terenkripsi terkadang bisa lebih besar dari file yang tidak dienkripsi, tergantung pada pengaturannya. Kumpulan data juga harus dienkripsi per kolaborasi agar berfungsi dengan benar.

Saat Anda mengenkripsi data menggunakan C3R, gunakan `--tempDir` bendera untuk menentukan lokasi di mana file sementara dapat dibuat saat memproses input.

Tabel berikut merangkum penggunaan dan parameter flag ini.

Penggunaan	Parameter
Pengguna dapat menentukan lokasi di mana file sementara dapat dibuat saat memproses input.	Default ke direktori sementara sistem.

Kueri dengan Komputasi Kriptografi untuk Clean Rooms

Topik ini memberikan informasi tentang menulis kueri yang menggunakan tabel data yang telah dienkripsi menggunakan Cryptographic Computing untuk. Clean Rooms

Topik

Kueri yang bercabang di NULL

Untuk memiliki cabang kueri pada NULL pernyataan berarti menggunakan sintaks seperti`IF x IS NULL THEN 0 ELSE 1`.

Kueri selalu dapat bercabang pada NULL pernyataan di cleartext kolom.

Kueri dapat bercabang pada NULL pernyataan di sealed kolom dan fingerprint kolom hanya jika nilai parameter Preserve NULL values (`preserveNulls`) diatur ke. `true`

Kueri yang melanggar batasan ini mungkin menghasilkan hasil yang salah.

Memetakan satu kolom sumber ke beberapa kolom target

Satu kolom sumber dapat dipetakan ke beberapa kolom target. Misalnya, Anda mungkin ingin keduanya JOIN dan SELECT pada kolom.

Untuk informasi selengkapnya, lihat Menggunakan data yang sama untuk keduanya JOIN dan SELECT kueri.

Menggunakan data yang sama untuk keduanya JOIN dan SELECT kueri

Jika data dalam kolom tidak sensitif, itu dapat muncul di kolom cleartext target, yang memungkinkannya digunakan untuk tujuan apa pun.

Jika data dalam kolom sensitif dan harus digunakan untuk keduanya JOIN dan SELECT kueri, petakan kolom sumber itu ke dua kolom target dalam file output. Satu kolom dienkripsi dengan `type` sebagai fingerprint kolom, dan satu kolom dienkripsi dengan kolom `type` sebagai tertutup. Pembuatan skema interaktif dari klien enkripsi C3R menyarankan sufiks header dan. `_fingerprint _sealed` Sufiks header ini dapat menjadi konvensi yang berguna untuk membedakan kolom tersebut dengan cepat.

Pedoman untuk klien enkripsi C3R

Klien enkripsi C3R adalah alat yang memungkinkan organisasi untuk menyatukan data sensitif untuk mendapatkan wawasan baru dari analisis data. Alat ini secara kriptografis membatasi apa yang dapat dipelajari oleh pihak mana pun dan AWS dalam prosesnya. Meskipun ini sangat penting, proses pengamanan data secara kriptografis dapat menambah overhead yang signifikan baik dalam hal sumber daya komputasi maupun penyimpanan. Oleh karena itu, penting untuk memahami pengorbanan menggunakan setiap pengaturan dan cara mengoptimalkan pengaturan sambil tetap mempertahankan jaminan kriptografi yang diinginkan. Topik ini berfokus pada implikasi kinerja dari pengaturan yang berbeda dalam klien dan skema enkripsi C3R.

Semua pengaturan enkripsi klien enkripsi C3R memberikan jaminan kriptografi yang berbeda. Pengaturan tingkat kolaborasi paling aman secara default. Mengaktifkan fungsionalitas tambahan sambil membuat kolaborasi melemahkan jaminan privasi, memungkinkan aktivitas seperti analisis frekuensi dilakukan pada ciphertext. Untuk informasi lebih lanjut tentang bagaimana pengaturan ini digunakan dan apa implikasinya, lihatKomputasi kriptografi.

Topik

Implikasi kinerja untuk jenis kolom

C3R menggunakan tiga jenis kolom:cleartext,fingerprint, dan. sealed Masing-masing jenis kolom ini memberikan jaminan kriptografi yang berbeda dan memiliki tujuan penggunaan yang berbeda. Pada bagian berikut, implikasi kinerja dari jenis kolom dibahas dan dampak kinerja dari setiap pengaturan.

Topik

Cleartextkolom

Cleartextkolom tidak diubah dari format aslinya dan tidak diproses secara kriptografi dengan cara apa pun. Jenis kolom ini tidak dapat dikonfigurasi dan tidak memengaruhi kinerja penyimpanan atau komputasi.

Fingerprintkolom

Fingerprintkolom dimaksudkan untuk digunakan untuk menggabungkan data di beberapa tabel. Untuk tujuan ini, ukuran ciphertext yang dihasilkan harus selalu sama. Namun, kolom ini dipengaruhi oleh pengaturan tingkat kolaborasi. Fingerprintkolom mungkin memiliki berbagai tingkat dampak pada ukuran file output tergantung pada yang cleartext terkandung dalam input.

Topik

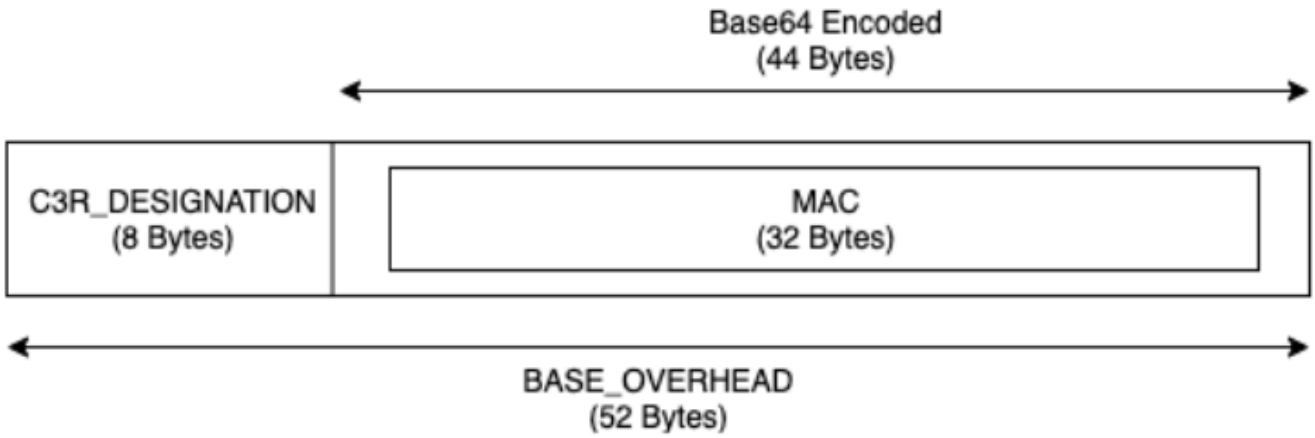
- Basis overhead untuk kolom fingerprint
- Pengaturan kolaborasi untuk fingerprint kolom
- Contoh data untuk fingerprint kolom
- Kolom pemecahan masalah fingerprint

Basis overhead untuk kolom fingerprint

Ada overhead dasar untuk fingerprint kolom. Overhead ini konstan dan menggantikan ukuran cleartext byte.

Data dalam fingerprint kolom diproses secara kriptografis melalui fungsi Kode Otentikasi Pesan berbasis Hash (HMAC), yang mengubah data menjadi kode otentikasi pesan 32 byte (MAC). Data ini kemudian diproses melalui encoder base64, menambahkan sekitar 33 persen ke ukuran byte. Ini pra-penandaan dengan penunjukan C3R 8 byte untuk menunjuk jenis kolom yang dimiliki data dan versi klien yang menghasilkannya. Hasil akhirnya adalah 52 byte. Hasil ini kemudian dikalikan dengan jumlah baris untuk mendapatkan total overhead basis (gunakan jumlah total `null` non-nilai jika `preserveNulls` disetel ke true).

Gambar berikut menunjukkan bagaimana *`BASE_OVERHEAD = C3R_DESIGNATION + (MAC * 1.33)`*



Output ciphertext dalam fingerprint kolom akan selalu 52 byte. Ini bisa menjadi penurunan penyimpanan yang signifikan jika cleartext data input rata-rata lebih dari 52 byte (misalnya, alamat jalan lengkap). Ini bisa menjadi peningkatan penyimpanan yang signifikan jika cleartext data input rata-rata kurang dari 52 byte (misalnya, usia pelanggan).

Pengaturan kolaborasi untuk fingerprint kolom

Setelan **`preserveNulls`**

Ketika pengaturan `preserveNulls` tingkat kolaborasi `false` (default), setiap `null` nilai diganti dengan 32 byte acak yang unik dan diproses seolah-olah tidak. `null` Hasilnya adalah bahwa setiap `null` nilai sekarang 52 byte. Ini dapat menambahkan persyaratan penyimpanan yang signifikan untuk tabel yang berisi data yang sangat jarang dibandingkan dengan saat pengaturan ini `true` dan `null` nilai dilewatkan sebagai`null`.

Jika Anda tidak memerlukan jaminan privasi dari pengaturan ini dan lebih memilih untuk mempertahankan `null` nilai dalam kumpulan data Anda, aktifkan `preserveNulls` pengaturan pada saat kolaborasi dibuat. `preserveNulls`Pengaturan tidak dapat diubah setelah kolaborasi dibuat.

Contoh data untuk fingerprint kolom

Berikut ini adalah contoh kumpulan data input dan output untuk fingerprint kolom dengan pengaturan untuk mereproduksi. Pengaturan tingkat kolaborasi lainnya menyukai `allowCleartext` dan `allowDuplicates` tidak memengaruhi hasil dan dapat disetel sebagai `true` atau `false` jika mencoba mereproduksi secara lokal.

Contoh rahasia bersama: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Contoh ID kolaborasi: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

allowJoinsOnColumnsWithDifferentNames: Pengaturan `True` ini tidak memengaruhi kinerja atau persyaratan penyimpanan. Namun, pengaturan ini membuat pilihan nama kolom tidak relevan saat mereproduksi nilai yang ditunjukkan dalam tabel berikut.

Contoh 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministik	`Yes`
Byte masukan	0
Byte keluaran	0

Contoh 2

Input	`null`
`preserveNulls`	`FALSE`
Output	`01:hmac:3lkFjthvV3IUu6mMvFc1a +XAHwgw/ElmOq4p3Yg25kk=`
Deterministik	No
Byte masukan	0
Byte keluaran	52

Contoh 3

Input	`empty string`
`preserveNulls`	-

Output	`01:hmac:oKTgi3Gba+eUb3JteSz 2EMgXUkF1WgM77UP0Ydw5kPQ=`
Deterministik	`Yes`
Byte masukan	0
Byte keluaran	52

Contoh 4

Input	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:hmac:kU/IqwG7FMmzzshr0B9 scomE0UJUEE7j9keTctplGww=`
Deterministik	`Yes`
Byte masukan	26
Byte keluaran	52

Contoh 5

Input	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Output	`01:hmac:ks3htnQbw2vdhCRFF6J NzW5LMndJaHG57uvE26mBtSs=`
Deterministik	`Yes`
Byte masukan	62

Byte keluaran	52

Kolom pemecahan masalah fingerprint

Mengapa ciphertext di fingerprint kolom saya beberapa kali lebih besar dari ukuran cleartext yang masuk ke dalamnya?

Ciphertext dalam fingerprint kolom selalu 52 byte panjangnya. Jika data input Anda kecil (misalnya, usia pelanggan), itu akan menunjukkan peningkatan ukuran yang signifikan. Ini juga bisa terjadi jika `preserveNulls` pengaturan diatur ke`false`.

Mengapa ciphertext di fingerprint kolom saya beberapa kali lebih kecil dari ukuran cleartext yang masuk ke dalamnya?

Ciphertext dalam fingerprint kolom selalu 52 byte panjangnya. Jika data input Anda besar (misalnya, alamat jalan lengkap pelanggan), itu akan menunjukkan penurunan ukuran yang signifikan.

Bagaimana saya tahu jika saya membutuhkan jaminan kriptografi yang disediakan oleh? **`preserveNulls`**

Sayangnya, jawabannya adalah itu tergantung. Minimal, the section called “Parameter” harus ditinjau untuk bagaimana `preserveNulls` pengaturan melindungi data Anda. Namun, kami menyarankan Anda untuk mereferensikan persyaratan penanganan data organisasi Anda dan kontrak apa pun yang berlaku untuk kolaborasi masing-masing.

Mengapa saya harus mengeluarkan biaya overhead base64?

Untuk memungkinkan kompatibilitas dengan format file tabular seperti CSV, pengkodean base64 diperlukan. Meskipun beberapa format file seperti Parquet mungkin mendukung representasi biner data, penting bahwa semua peserta dalam kolaborasi mewakili data dengan cara yang sama untuk memastikan hasil kueri yang tepat.

Sealedkolom

Sealedkolom dimaksudkan untuk digunakan untuk mentransfer data antara anggota kolaborasi. Ciphertext dalam kolom ini bersifat non-deterministik dan memiliki dampak signifikan pada kinerja dan penyimpanan berdasarkan bagaimana kolom dikonfigurasi. Kolom ini dapat dikonfigurasi secara individual dan seringkali memiliki dampak terbesar pada kinerja klien enkripsi C3R dan ukuran file keluaran yang dihasilkan.

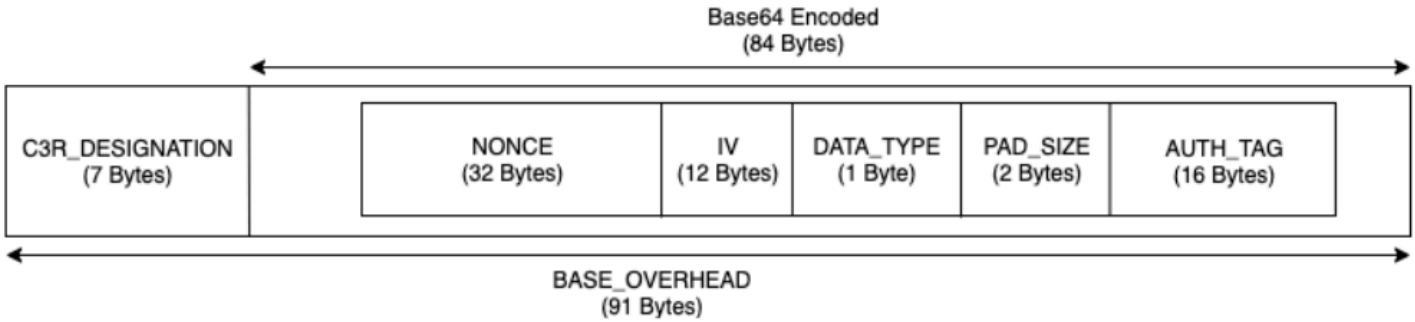
Topik

Basis overhead untuk kolom sealed

Ada overhead dasar untuk sealed kolom. Overhead ini konstan dan selain ukuran byte cleartext dan padding (jika ada).

Sebelum enkripsi apa pun, data dalam sealed kolom pra-pended dengan karakter 1 byte yang menunjuk jenis data apa yang terkandung. Jika padding dipilih, data kemudian empuk dan ditambahkan dengan 2 byte yang menyatakan ukuran pad. Setelah byte ini ditambahkan, data diproses secara kriptografi dengan menggunakan AES-GCM dan disimpan dengan IV (12 byte), (32 byte), dan nonce (16 byte). Auth Tag Data ini kemudian diproses melalui encoder base64, menambahkan sekitar 33 persen ke ukuran byte. Data pra-penandaan dengan penunjukan C3R 7 byte untuk menentukan jenis kolom apa yang dimiliki data dan versi klien yang digunakan untuk memproduksinya. Hasilnya adalah overhead basis akhir 91 byte. Hasil ini kemudian dapat dikalikan dengan jumlah baris untuk mendapatkan total overhead basis (gunakan jumlah total nilai non-null jika `preserveNulls` disetel ke true).

Gambar berikut menunjukkan bagaimana *`BASE_OVERHEAD = C3R_DESIGNATION + ((NONCE + IV + DATA_TYPE + PAD_SIZE + AUTH_TAG) * 1.33)`*



Pengaturan kolaborasi untuk sealed kolom

Setelan **preserveNulls**

Ketika pengaturan `preserveNulls` tingkat kolaborasi `false` (default), setiap `null` nilai unik, acak 32 byte dan diproses seolah-olah tidak. `null` Hasilnya adalah bahwa setiap `null` nilai sekarang 91 byte (lebih jika empuk). Ini dapat menambahkan persyaratan penyimpanan yang signifikan untuk tabel yang berisi data yang sangat jarang dibandingkan dengan saat pengaturan ini `true` dan `null` nilai dilewatkan sebagai`null`.

Jika Anda tidak memerlukan jaminan privasi dari pengaturan ini dan lebih memilih untuk mempertahankan `null` nilai dalam kumpulan data Anda, aktifkan `preserveNulls` pengaturan pada saat kolaborasi dibuat. `preserveNulls`Pengaturan tidak dapat diubah setelah kolaborasi dibuat.

sealedKolom pengaturan skema: jenis padding

Topik

- Jenis pad none
- Jenis pad fixed
- Jenis pad max

Jenis pad **none**

Memilih jenis pad `none` tidak menambahkan padding apa pun ke cleartext dan tidak menambahkan overhead tambahan ke overhead dasar yang dijelaskan sebelumnya. Tidak ada padding yang menghasilkan ukuran output yang paling hemat ruang. Namun, itu tidak memberikan jaminan privasi yang sama dengan tipe `fixed` dan `max` padding. Ini karena ukuran yang mendasarinya cleartext dapat dilihat dari ukuran ciphertext.

Jenis pad **fixed**

Memilih jenis pad `fixed` adalah ukuran pelestarian privasi untuk menyembunyikan panjang data yang terkandung dalam kolom. Hal ini dilakukan dengan padding semua cleartext ke yang disediakan `pad_length` sebelum dienkripsi. Setiap data yang melebihi ukuran itu menyebabkan klien enkripsi C3R gagal.

Mengingat bahwa padding ditambahkan ke cleartext sebelum dienkripsi, AES-GCM memiliki pemetaan 1-ke-1 untuk byte ciphertext. cleartext Pengkodean base64 akan menambah 33 persen. Overhead penyimpanan tambahan dari padding dapat dihitung dengan mengurangi panjang

rata-rata dari cleartext dari nilai `pad_length` dan mengalikannya dengan 1,33. Hasilnya adalah overhead rata-rata padding per record. Hasil ini kemudian dapat dikalikan dengan jumlah baris untuk mendapatkan overhead padding total (gunakan jumlah total `null` non-nilai jika `preserveNulls` diatur ke). `true`

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

Kami menyarankan Anda memilih minimum `pad_length` yang mencakup nilai terbesar dalam kolom. Misalnya, jika nilai terbesar adalah 50 byte, a `pad_length` dari 50 sudah cukup. Nilai yang lebih besar dari itu hanya akan menambah overhead penyimpanan tambahan.

Padding tetap tidak menambahkan overhead komputasi yang signifikan.

Jenis pad **`max`**

Memilih jenis pad `max` adalah ukuran pelestarian privasi untuk menyembunyikan panjang data yang terkandung dalam kolom. Hal ini dilakukan dengan padding semua cleartext ke nilai terbesar di kolom ditambah tambahan `pad_length` sebelum dienkripsi. Umumnya, `max` padding memberikan jaminan yang sama dengan `fixed` padding untuk satu kumpulan data sementara memungkinkan untuk tidak mengetahui nilai terbesar cleartext di kolom. Namun, `max` padding mungkin tidak memberikan jaminan privasi yang sama seperti `fixed` padding di seluruh pembaruan karena nilai terbesar dalam kumpulan data individu mungkin berbeda.

Kami menyarankan Anda memilih tambahan `pad_length` 0 saat menggunakan `max` padding. Panjang ini bantalan semua nilai menjadi ukuran yang sama dengan nilai terbesar di kolom. Nilai yang lebih besar dari itu hanya akan menambah overhead penyimpanan tambahan.

Jika cleartext nilai terbesar diketahui untuk kolom tertentu, kami sarankan Anda menggunakan jenis `fixed` pad sebagai gantinya. Menggunakan `fixed` padding menciptakan konsistensi di seluruh kumpulan data yang diperbarui. Menggunakan `max` padding menghasilkan setiap subset data yang diempuk ke nilai terbesar yang ada di subset.

Contoh data untuk sealed kolom

Berikut ini adalah contoh kumpulan data input dan output untuk sealed kolom dengan pengaturan untuk mereproduksi. Pengaturan tingkat kolaborasi lainnya seperti`allowCleartext`,`allowJoinsOnColumnsWithDifferentNames`, dan `allowDuplicates` tidak memengaruhi hasil dan dapat disetel sebagai `true` atau `false` jika mencoba mereproduksi secara lokal. Meskipun ini adalah pengaturan dasar untuk mereproduksi, sealed kolom tidak deterministik dan nilai akan berubah setiap saat. Tujuannya adalah untuk menunjukkan byte dalam dibandingkan dengan byte keluar. Contoh `pad_length` nilai dipilih dengan

sengaja. Mereka menunjukkan bahwa `fixed` padding menghasilkan nilai yang sama dengan `max` padding dengan `pad_length` pengaturan minimum yang disarankan atau ketika padding tambahan diinginkan.

Contoh rahasia bersama: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Contoh ID kolaborasi: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

Topik

Jenis pad **none**

Contoh 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministik	`Yes`
Byte masukan	0
Byte keluaran	0

Contoh 2

Input	`null`
`preserveNulls`	`FALSE`
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY`

	`Z98t5KU6aWfssGSPbNIJfG3iXmu6cbCUrizuV`
Deterministik	No
Byte masukan	0
Byte keluaran	91

Contoh 3

Input	`empty string`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSPEM6qR8DWC2PB2GMlX41YK`
Deterministik	No
Byte masukan	0
Byte keluaran	91

Contoh 4

Input	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9sGL5VLDQeHzh6DmPpyWNuI=`
Deterministik	No

Byte masukan	26
Byte keluaran	127

Contoh 5

Input	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqdP4/ QOQ3cXb/pbvPcnnohrHIGSX54ua+1/ JfcVjc=`
Deterministik	No
Byte masukan	62
Byte keluaran	175

Jenis pad **`fixed`** (Contoh 1)

Dalam contoh ini, `pad_length` adalah 62 dan masukan terbesar adalah 62 byte.

Contoh 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministik	`Yes`

Byte masukan	0
Byte keluaran	0

Contoh 2

Input	`null`
`preserveNulls`	`FALSE`
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/ hCz7oaIneVsrcoNpATs0GzbnLkor4L+/ aSuA=`
Deterministik	No
Byte masukan	0
Byte keluaran	175

Contoh 3

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

Deterministik	No
Byte masukan	0
Byte keluaran	175

Contoh 4

Input	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`
Deterministik	No
Byte masukan	26
Byte keluaran	175

Contoh 5

Input	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8t`

	`RFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Deterministik	No
Byte masukan	62
Byte keluaran	175

Jenis pad **`fixed`** (Contoh 2)

Dalam contoh ini, `pad_length` adalah 162 dan masukan terbesar adalah 62 byte.

Contoh 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministik	`Yes`
Byte masukan	0
Byte keluaran	0

Contoh 2

Input	`null`
`preserveNulls`	`FALSE`
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcnkB0xbLWD7z`

	`NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb`
Deterministik	No
Byte masukan	0
Byte keluaran	307

Contoh 3

Input	`empty string`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT`
Deterministik	No
Byte masukan	0
Byte keluaran	307

Contoh 4

Input	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf
Deterministik	No
Byte masukan	26
Byte keluaran	307

Contoh 5

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

	NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i
Deterministik	No
Byte masukan	62
Byte keluaran	307

Jenis pad **`max`** (Contoh 1)

Dalam contoh ini, `pad_length` adalah 0 dan masukan terbesar adalah 62 byte.

Contoh 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministik	`Yes`
Masukan Byte	0
Byte Keluaran	0

Contoh 2

Input	`null`
`preserveNulls`	`FALSE`

Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5`
	`MG5vbmNlMDEyMzQ1Njc4OTBqfRY`
	`Z98t5KU6aWfssGSNWfMRp7nSb7S`
	`MX2s3JKLOhK1+7r75Tk+Mx9jy48`

	`Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=`
Deterministik	No
Byte masukan	0
Byte keluaran	175

Contoh 3

Input	`empty string`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=`
Deterministik	No
Byte masukan	0
Byte keluaran	175

Contoh 4

Input	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0`

	`h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`
Deterministik	No
Byte masukan	26
Byte keluaran	175

Contoh 5

Input	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Deterministik	No
Byte masukan	62
Byte keluaran	175

Jenis pad **`max`** (Contoh 2)

Dalam contoh ini, `pad_length` adalah 100 dan masukan terbesar adalah 62 byte.

Contoh 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministik	`Yes`
Byte masukan	0
Byte keluaran	0

Contoh 2

Input	`null`
`preserveNulls`	`FALSE`
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcnkB0xbLWD7zNdAqQGR0rXoSESdW0I0vpNoGcBfv4cJbG0A3h1DvtkSSVc2B80OOGppzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn+8o4WtG/ClipNcjDXvXVtK4vfCohcCA6uwrmwv/xAySX+xcntotL703aBTBb`
Deterministik	No
Byte masukan	0
Byte keluaran	307

Contoh 3

Input	`empty string`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT`
Deterministik	No
Byte masukan	0
Byte keluaran	307

Contoh 4

Input	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp`

	pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf
Deterministik	No
Byte masukan	26
Byte keluaran	307

Contoh 5

Input	abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/QOQ3cXb/pbvPcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i
Deterministik	No
Byte masukan	62
Byte keluaran	307

Kolom pemecahan masalah sealed

Mengapa ciphertext di sealed kolom saya beberapa kali lebih besar dari ukuran cleartext yang masuk ke dalamnya?

Ini tergantung pada beberapa faktor. Untuk satu, ciphertext dalam Cleartext kolom selalu setidaknya 91 byte panjangnya. Jika data input Anda kecil (misalnya, usia pelanggan), itu akan menunjukkan peningkatan ukuran yang signifikan. Kedua, jika `preserveNulls` disetel ke `false` dan data input Anda berisi banyak `null` nilai, masing-masing `null` nilai tersebut akan berubah menjadi 91 byte ciphertext. Akhirnya, jika Anda menggunakan padding, menurut definisi byte ditambahkan ke cleartext data sebelum dienkripsi.

Sebagian besar data saya di sealed kolom sangat kecil, dan saya perlu menggunakan padding. Bisakah saya menghapus nilai besar dan memprosesnya secara terpisah untuk menghemat ruang?

Kami tidak menyarankan Anda menghapus nilai besar dan memprosesnya secara terpisah. Melakukan hal itu mengubah jaminan privasi yang disediakan oleh klien enkripsi C3R. Sebagai model ancaman, asumsikan bahwa pengamat dapat melihat kedua kumpulan data terenkripsi. Jika pengamat melihat bahwa satu subset data memiliki kolom yang dilapisi secara signifikan lebih atau kurang dari subset lain, mereka dapat membuat kesimpulan tentang ukuran data di setiap subset. Misalnya, asumsikan `fullName` kolom diempuk dengan total 40 byte dalam satu file dan diempuk hingga 800 byte di file lain. Seorang pengamat mungkin dapat berasumsi bahwa satu kumpulan data berisi nama terpanjang di dunia747 byte).

Apakah saya perlu memberikan padding tambahan saat menggunakan tipe **`max`** padding?

Tidak. Saat menggunakan `max` padding, kami merekomendasikan bahwa`pad_length`, juga dikenal sebagai padding tambahan di luar nilai terbesar di kolom, diatur ke 0.

Bisakah saya memilih yang besar **`pad_length`** saat menggunakan **`fixed`** padding untuk menghindari kekhawatiran jika nilai terbesar akan cocok?

Ya, tetapi panjang pad yang besar tidak efisien dan menggunakan lebih banyak penyimpanan dari yang diperlukan. Kami menyarankan Anda untuk memeriksa untuk melihat seberapa besar nilai terbesar dan menetapkan `pad_length` ke nilai itu.

Bagaimana saya tahu jika saya membutuhkan jaminan kriptografi yang disediakan oleh? **`preserveNulls`**

Sayangnya, jawabannya adalah itu tergantung. Minimal, Komputasi Kriptografi untuk Clean Rooms harus ditinjau untuk bagaimana `preserveNulls` pengaturan melindungi data Anda. Namun, kami

menyarankan Anda untuk mereferensikan persyaratan penanganan data organisasi Anda dan kontrak apa pun yang berlaku untuk kolaborasi masing-masing.

Mengapa saya harus mengeluarkan biaya overhead base64?

Untuk memungkinkan kompatibilitas dengan format file tabular seperti CSV, pengkodean base64 diperlukan. Meskipun beberapa format file seperti Parquet mungkin mendukung representasi biner data, penting bahwa semua peserta dalam kolaborasi mewakili data dengan cara yang sama untuk memastikan hasil kueri yang tepat.

Memecahkan masalah peningkatan ukuran ciphertext yang tidak terduga

Katakanlah Anda mengenkripsi data Anda, dan ukuran data yang dihasilkan sangat besar. Langkah-langkah berikut dapat membantu Anda mengidentifikasi di mana peningkatan ukuran terjadi dan apa, jika ada, tindakan yang dapat Anda ambil.

Mengidentifikasi di mana peningkatan ukuran terjadi

Sebelum Anda dapat memecahkan masalah mengapa data terenkripsi Anda secara signifikan lebih besar daripada cleartext data Anda, Anda harus terlebih dahulu mengidentifikasi di mana peningkatan ukurannya. Cleartextkolom dapat diabaikan dengan aman karena tidak berubah. Lihatlah yang tersisa fingerprint dan sealed kolom, dan pilih salah satu yang tampak signifikan.

Mengidentifikasi alasan peningkatan ukuran terjadi

fingerprintKolom atau sealed kolom mungkin berkontribusi pada peningkatan ukuran.

Topik

- Apakah peningkatan ukuran berasal dari fingerprint kolom?
- Apakah peningkatan ukuran berasal dari sealed kolom?

Apakah peningkatan ukuran berasal dari fingerprint kolom?

Jika kolom yang paling berkontribusi terhadap peningkatan penyimpanan adalah fingerprint kolom, ini mungkin karena cleartext datanya kecil (misalnya, usia pelanggan). Setiap fingerprint ciphertext yang dihasilkan panjangnya 52 byte. Sayangnya, tidak ada yang bisa dilakukan tentang masalah ini column-by-column atas dasar. Untuk informasi selengkapnya, lihat Basis overhead untuk kolom fingerprint detail tentang kolom ini, termasuk dampaknya terhadap persyaratan penyimpanan.

Kemungkinan penyebab lain dari peningkatan ukuran dalam fingerprint kolom adalah pengaturan kolaborasi,`preserveNulls`. Jika pengaturan kolaborasi untuk `preserveNulls` dinonaktifkan (pengaturan default), semua `null` nilai dalam fingerprint kolom akan menjadi 52 byte ciphertext. Tidak ada yang bisa dilakukan untuk ini dalam kolaborasi saat ini. `preserveNulls`Pengaturan diatur pada saat kolaborasi dibuat dan semua kolaborator harus menggunakan pengaturan yang sama untuk memastikan hasil kueri yang benar. Untuk informasi selengkapnya tentang `preserveNulls` pengaturan dan bagaimana pengaktifannya memengaruhi jaminan privasi data Anda, lihat. Komputasi kriptografi

Apakah peningkatan ukuran berasal dari sealed kolom?

Jika kolom yang paling berkontribusi terhadap peningkatan penyimpanan adalah sealed kolom, ada beberapa detail yang dapat berkontribusi pada peningkatan ukuran.

Jika cleartext data kecil (misalnya, usia pelanggan), setiap sealed ciphertext yang dihasilkan setidaknya 91 byte panjangnya. Sayangnya, tidak ada yang bisa dilakukan tentang masalah ini. Untuk informasi selengkapnya, lihat Basis overhead untuk kolom sealed detail tentang kolom ini, termasuk dampaknya terhadap persyaratan penyimpanan.

Penyebab utama kedua untuk peningkatan penyimpanan sealed kolom adalah padding. Padding menambahkan byte ekstra ke cleartext sebelum dienkripsi untuk menyembunyikan ukuran nilai individual dalam kumpulan data. Kami menyarankan Anda mengatur padding ke nilai minimum yang mungkin untuk kumpulan data Anda. Minimal, `pad_length` untuk `fixed` padding harus diatur untuk mencakup nilai terbesar yang mungkin di kolom. Pengaturan yang lebih tinggi dari itu tidak menambahkan jaminan privasi tambahan. Misalnya, jika Anda tahu nilai terbesar yang mungkin dalam kolom bisa 50 byte, kami sarankan Anda menyetel `pad_length` ke 50 byte. Namun, jika sealed kolom menggunakan `max` padding, kami sarankan Anda mengatur `pad_length` ke 0 byte. Ini karena `max` padding mengacu pada padding tambahan di luar nilai terbesar di kolom.

Kemungkinan penyebab akhir dari peningkatan ukuran dalam sealed kolom adalah pengaturan kolaborasi,`preserveNulls`. Jika pengaturan kolaborasi untuk `preserveNulls` dinonaktifkan (pengaturan default), semua `null` nilai dalam sealed kolom akan menjadi 91 byte ciphertext. Tidak ada yang bisa dilakukan untuk ini dalam kolaborasi saat ini. `preserveNulls`Pengaturan diatur pada saat kolaborasi dibuat, dan semua kolaborator harus menggunakan pengaturan yang sama untuk memastikan hasil kueri yang benar. Untuk informasi selengkapnya tentang pengaturan ini dan bagaimana cara mengaktifkannya memengaruhi jaminan privasi data Anda, lihat. Komputasi kriptografi

Kueri masuk AWS Clean Rooms

Pencatatan kueri adalah fitur di AWS Clean Rooms. Saat Anda membuat kolaborasi dan mengaktifkan pencatatan Kueri, anggota dapat menyimpan log kueri yang relevan dengannya di CloudWatch Log Amazon.

Dengan log kueri, anggota dapat menentukan apakah kueri mematuhi aturan analisis dan menyelaraskan dengan perjanjian kolaborasi. Selain itu, log kueri membantu mendukung audit.

Saat opsi Pencatatan kueri diaktifkan di AWS Clean Rooms konsol, log kueri menyertakan yang berikut:

- `analysisRule`— Aturan analisis untuk tabel yang dikonfigurasi.
- `analysisTemplateArn`— Template analisis yang dijalankan (muncul tergantung pada aturan analisis).
- `collaborationId`— Pengidentifikasi unik untuk kolaborasi di mana kueri dijalankan.
- `configuredTableID`— Pengidentifikasi unik untuk tabel yang dikonfigurasi direferensikan dalam kueri.
- `directQueryAnalysisRulePolicy.custom.allowedAnalysis`— Template analisis diizinkan untuk berjalan pada tabel yang dikonfigurasi (muncul tergantung pada aturan analisis).
- `directQueryAnalysisRulePolicy.v1.custom.allowedAnalysisProviders`— Penyedia kueri diizinkan untuk membuat kueri (muncul tergantung pada aturan analisis).
- `eventID`— Pengidentifikasi unik untuk menjalankan kueri. Setelah 31 Agustus 2023, pengidentifikasi unik sama dengan. `protectedQueryID`
- `eventTimestamp`— Query run time.
- `parameters.parametervalue`— Nilai parameter (muncul tergantung pada teks kueri).
- `queryText`— Definisi SQL dari query run. Jika ada parameter, mereka diberi label sebagai. `:parametervalue`
- `queryValidationErrors`— Kesalahan kueri pada validasi kueri.
- `schemaName`— Nama asosiasi tabel yang dikonfigurasi direferensikan dalam kueri.

Menerima log kueri

Anda tidak perlu melakukan tindakan apa pun di luar AWS Clean Rooms untuk menyiapkan log kueri. AWS Clean Rooms membuat grup log untuk kolaborasi setelah setiap anggota kolaborasi membuat keanggotaan.

Anggota yang dapat melakukan kueri, anggota yang dapat menerima hasil, dan anggota yang tabel konfigurasinya direferensikan dalam kueri akan menerima log kueri.

Anggota yang dapat melakukan kueri dan anggota yang dapat menerima hasil akan menerima log kueri untuk setiap tabel yang dikonfigurasi yang direferensikan dalam kueri. Jika mereka tidak memiliki tabel yang dikonfigurasi, mereka tidak akan dapat melihat ID tabel yang dikonfigurasi (`configuredTableID`).

Jika anggota memiliki beberapa asosiasi tabel dikonfigurasi yang direferensikan dalam kueri, mereka akan menerima log kueri untuk setiap tabel yang dikonfigurasi.

Log dibuat untuk kueri yang berisi SQL yang tidak didukung dan didukung di. AWS Clean Rooms Untuk detail selengkapnya, lihat Referensi AWS Clean Rooms SQL.

Log juga dibuat ketika referensi kueri dikonfigurasi tabel yang tidak terkait dengan kolaborasi.

Log tidak dibuat untuk SQL yang salah di AWS Clean Rooms.

Log kueri tidak menunjukkan bahwa kueri berhasil dan keluaran kueri dikirimkan. Mereka mengkonfirmasi bahwa kueri telah dikirimkan oleh anggota yang dapat menanyakan. Log kueri juga mengonfirmasi bahwa kueri berisi SQL yang didukung AWS Clean Rooms dan referensi tabel yang dikonfigurasi terkait dengan kolaborasi.

Example

Misalnya, log tidak dihasilkan jika kueri dibatalkan setelah AWS Clean Rooms memvalidasi kepatuhannya dengan aturan analisis dan selama pemrosesan kueri.

Jika Anda menghapus grup log, Anda harus membuat ulang grup log secara manual dengan nama grup log yang sama (ID kolaborasi kolaborasi). Atau, Anda dapat mematikan dan mengaktifkan log dalam keanggotaan Anda.

Untuk informasi selengkapnya tentang cara mengaktifkan pencatatan kueri, lihatMenciptakan kolaborasi di AWS Clean Rooms.

Untuk informasi selengkapnya tentang CloudWatch Log Amazon, lihat Panduan Pengguna CloudWatch Log Amazon.

Menggunakan log kueri

Kami menyarankan agar anggota secara berkala mengambil tindakan berikut:

- Untuk memverifikasi bahwa kueri cocok dengan kasus penggunaan atau kueri yang disepakati untuk kolaborasi, tinjau kueri yang dijalankan dalam kolaborasi.

  Untuk informasi selengkapnya tentang cara melihat kueri terbaru, lihat Melihat kueri terbaru.
- Untuk memverifikasi bahwa kolom tabel yang dikonfigurasi cocok dengan apa yang telah disepakati untuk kolaborasi, tinjau kolom tabel yang dikonfigurasi yang digunakan dalam aturan analisis anggota kolaborasi dan dalam kueri.

  Untuk informasi selengkapnya tentang cara melihat kolom yang dikonfigurasi, lihat Melihat tabel dan aturan analisis.

Menyiapkan AWS Clean Rooms

Topik berikut menjelaskan cara mengaturnya AWS Clean Rooms.

Topik

Mendaftar untuk AWS

Sebelum Anda dapat menggunakan apa pun Layanan AWS AWS Clean Rooms, termasuk, Anda harus mendaftar AWS.

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.
3. Ketika Anda mendaftar untuk Akun AWS, pengguna Akun AWS root dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik terbaik keamanan, tetapkan akses administratif ke pengguna administratif, dan hanya gunakan pengguna root untuk melakukan tugas-tugas yang memerlukan akses pengguna root.

Menyiapkan peran layanan untuk AWS Clean Rooms

Topik

Buat pengguna administrator

Untuk menggunakannya AWS Clean Rooms, Anda perlu membuat pengguna administrator untuk diri sendiri dan menambahkan pengguna administrator ke grup administrator.

Untuk membuat pengguna administrator, pilih salah satu opsi berikut.

Pilih salah satu cara untuk mengelola administrator Anda	Untuk	Oleh	Anda juga bisa
Di Pusat Identitas IAM (Direkomendasikan)	Gunakan kredensi jangka pendek untuk mengakses. AWS Ini sejalan dengan praktik terbaik keamanan. Untuk informasi tentang praktik terbaik, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.	Mengikuti petunjuk di Memulai di Panduan AWS IAM Identity Center Pengguna.	Konfigurasikan akses terprogram dengan Mengonfigurasi AWS CLI yang akan digunakan AWS IAM Identity Center dalam AWS Command Line Interface Panduan Pengguna.
Di IAM (Tidak direkomendasikan)	Gunakan kredensi jangka panjang untuk mengakses. AWS	Mengikuti petunjuk dalam Membuat pengguna admin IAM pertama Anda dan grup pengguna di Panduan Pengguna IAM.	Konfigurasikan akses terprogram dengan Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Buat peran IAM untuk anggota kolaborasi

Anggota adalah AWS pelanggan yang merupakan peserta dalam kolaborasi.

Untuk membuat peran IAM untuk anggota kolaborasi

1. Ikuti Membuat peran untuk mendelegasikan izin ke prosedur pengguna IAM di Panduan Pengguna.AWS Identity and Access Management
2. Untuk langkah Buat kebijakan, pilih tab JSON di editor Kebijakan, lalu tambahkan kebijakan tergantung pada kemampuan yang diberikan kepada anggota kolaborasi.

   AWS Clean Rooms menawarkan kebijakan terkelola berikut berdasarkan kasus penggunaan umum:

Jika Anda ingin...	Kemudian gunakan...
Lihat sumber daya dan metadata	AWS kebijakan terkelola: `AWSCleanRoomsReadOnlyAccess`
Kueri	AWS kebijakan terkelola: `AWSCleanRoomsFullAccess`
Kueri dan terima hasil	AWS kebijakan terkelola: `AWSCleanRoomsFullAccess`
Kelola sumber daya kolaborasi tetapi jangan kueri	AWS kebijakan terkelola: `AWSCleanRoomsFullAccessNoQuerying`

   Untuk informasi tentang berbagai kebijakan terkelola yang ditawarkan oleh AWS Clean Rooms, lihat AWS kebijakan terkelola untuk AWS Clean Rooms

Membuat peran layanan untuk membaca data

AWS Clean Rooms menggunakan peran layanan untuk membaca data.

Ada dua cara untuk membuat peran layanan ini:

Jika...	Maka
Anda memiliki izin IAM yang diperlukan untuk membuat peran layanan	Gunakan AWS Clean Rooms konsol untuk membuat peran layanan.
Anda tidak memiliki`iam:CreateRole` , `iam:CreatePolicy` dan `iam:AttachRolePolicy` izin atau Anda ingin membuat peran IAM secara manual	Lakukan salah satu hal berikut ini: • Gunakan prosedur berikut untuk membuat peran layanan. • Minta administrator Anda untuk membuat peran layanan menggunakan prosedur berikut.

Untuk membuat peran layanan untuk membaca data

> **Note**
>
> Anda atau administrator IAM Anda hanya harus mengikuti prosedur ini jika Anda tidak memiliki izin yang diperlukan untuk membuat peran layanan menggunakan konsol. AWS Clean Rooms

1. Ikuti prosedur Membuat peran menggunakan kebijakan kepercayaan kustom (konsol) di Panduan AWS Identity and Access Management Pengguna.
2. Gunakan kebijakan kepercayaan kustom berikut sesuai dengan prosedur Membuat peran menggunakan kebijakan kepercayaan kustom (konsol).

   > **Note**
   >
   > Jika Anda ingin memastikan bahwa peran tersebut hanya dapat digunakan dalam konteks keanggotaan kolaborasi tertentu, Anda dapat meringkas kebijakan kepercayaan lebih lanjut. Untuk informasi selengkapnya, lihat Pencegahan confused deputy lintas layanan.

   ```
   {
   ```

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

3. Gunakan kebijakan izin berikut sesuai dengan prosedur Membuat peran menggunakan kebijakan kepercayaan kustom (konsol).

> **Note**
>
> Kebijakan contoh berikut mendukung izin yang diperlukan untuk membaca AWS Glue metadata dan data Amazon S3 yang sesuai. Namun, Anda mungkin perlu mengubah kebijakan ini tergantung pada cara Anda mengatur data S3. Misalnya, jika Anda telah menyiapkan kunci KMS khusus untuk data S3 Anda, Anda mungkin perlu mengubah kebijakan ini dengan izin tambahan. AWS KMS
> AWS Glue Sumber daya Anda dan sumber daya Amazon S3 yang mendasarinya harus Wilayah AWS sama dengan kolaborasi. AWS Clean Rooms

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

```
            ],
            "Resource": [
                "arn:aws:glue:aws-region:accountId:database/database",
                "arn:aws:glue:aws-region:accountId:table/table",
                "arn:aws:glue:aws-region:accountId:catalog"
            ]
        },
    {
            "Effect": "Allow",
            "Action": [
                "glue:GetSchema",
                "glue:GetSchemaVersion"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "NecessaryS3BucketPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket"
            ],
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "s3BucketOwnerAccountId"
                    ]
                }
            }
        },
        {
            "Sid": "NecessaryS3ObjectPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3::bucket/prefix/*"
            ],
```

```
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "s3BucketOwnerAccountId"
                    ]
                }
            }
        }

    ]
}
```

4. Ganti setiap *placeholder* dengan informasi Anda sendiri.
5. Terus ikuti prosedur Membuat peran menggunakan kebijakan kepercayaan khusus (konsol) untuk membuat peran.

Buat peran layanan untuk menerima hasil

> **Note**
>
> Jika Anda adalah anggota yang hanya dapat menerima hasil (di konsol, kemampuan anggota Anda hanya Terima hasil), ikuti prosedur ini.
> Jika Anda adalah anggota yang dapat menanyakan dan menerima hasil (di konsol, Kemampuan anggota Anda adalah hasil Kueri dan Terima), Anda dapat melewati prosedur ini.

Untuk anggota kolaborasi yang hanya dapat menerima hasil, AWS Clean Rooms gunakan peran layanan untuk menulis hasil data kueri dalam kolaborasi ke bucket Amazon S3 yang ditentukan.

Ada dua cara untuk membuat peran layanan ini:

Jika...	Maka
Anda memiliki izin IAM yang diperlukan untuk membuat peran layanan	Gunakan AWS Clean Rooms konsol untuk membuat peran layanan.

Jika...	Maka
Anda tidak memiliki`iam:CreateRole` , `iam:CreatePolicy` dan `iam:AttachRolePolicy` izin atau Anda ingin membuat peran IAM secara manual	Lakukan salah satu hal berikut ini: • Gunakan prosedur berikut untuk membuat peran layanan. • Minta administrator Anda untuk membuat peran layanan menggunakan prosedur berikut.

Untuk membuat peran layanan untuk menerima hasil

> **Note**
>
> Anda atau administrator IAM Anda hanya harus mengikuti prosedur ini jika Anda tidak memiliki izin yang diperlukan untuk membuat peran layanan menggunakan konsol. AWS Clean Rooms

1. Ikuti prosedur Membuat peran menggunakan kebijakan kepercayaan kustom (konsol) di Panduan AWS Identity and Access Management Pengguna.
2. Gunakan kebijakan kepercayaan kustom berikut sesuai dengan prosedur Membuat peran menggunakan kebijakan kepercayaan kustom (konsol).

```
{
    "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. Gunakan kebijakan izin berikut sesuai dengan prosedur Membuat peran menggunakan kebijakan kepercayaan kustom (konsol).

> **Note**
>
> Kebijakan contoh berikut mendukung izin yang diperlukan untuk membaca AWS Glue metadata dan data Amazon S3 yang sesuai. Namun, Anda mungkin perlu mengubah kebijakan ini tergantung pada cara Anda mengatur data S3.
> AWS Glue Sumber daya Anda dan sumber daya Amazon S3 yang mendasarinya harus Wilayah AWS sama dengan kolaborasi. AWS Clean Rooms

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
```

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

4. Ganti setiap *placeholder* dengan informasi Anda sendiri:

   - *wilayah* — Nama Wilayah AWS. Misalnya, **us-east-1**.
   - *A1B2C3D4-5678-90AB-CDEF-ExampleAAAAAAA* - ID Keanggotaan anggota yang dapat melakukan query. ID Keanggotaan dapat ditemukan di tab Detail kolaborasi. Ini memastikan bahwa AWS Clean Rooms mengasumsikan peran hanya ketika anggota ini menjalankan analisis dalam kolaborasi ini.
   - *arn:aws:cleanrooms:us-east- 1:55555555555555:Keanggotaan/ A1B2C3D4-5678-90AB-CDEF-exampleAAAAAA* - ARN Keanggotaan tunggal dari anggota yang dapat meminta. ARN Keanggotaan dapat ditemukan di tab Detail kolaborasi. AWS Clean Rooms Ini memastikan mengasumsikan peran hanya ketika anggota ini menjalankan analisis dalam kolaborasi ini.

- *bucket_name* – Nama Sumber Daya Amazon (ARN) dari bucket S3. Nama Sumber Daya Amazon (ARN) dapat ditemukan di tab Properties bucket di Amazon S3.
- *AccountID* — ID Akun AWS tempat bucket S3 berada.

  bucket_name/optional_key_prefix – Nama Sumber Daya Amazon (ARN) dari tujuan hasil di S3. Nama Sumber Daya Amazon (ARN) dapat ditemukan di tab Properties bucket di Amazon S3.

5. Terus ikuti prosedur Membuat peran menggunakan kebijakan kepercayaan khusus (konsol) untuk membuat peran.

Menyiapkan peran layanan untuk AWS Clean Rooms ML

Topik

- Membuat peran layanan untuk membaca data pelatihan
- Buat peran layanan untuk menulis segmen yang mirip
- Buat peran layanan untuk membaca data benih

Membuat peran layanan untuk membaca data pelatihan

AWS Clean Rooms menggunakan peran layanan untuk membaca data pelatihan. Anda dapat membuat peran ini menggunakan konsol jika Anda memiliki izin IAM yang diperlukan. Jika Anda tidak memiliki `CreateRole` izin, minta administrator Anda untuk membuat peran layanan.

Untuk membuat peran layanan untuk melatih kumpulan data

1. Masuk ke konsol IAM (https://console.aws.amazon.com/iam/) dengan akun administrator Anda.
2. Di bagian Manajemen akses, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Di editor Kebijakan, pilih tab JSON, lalu salin dan tempel kebijakan berikut.

> **Note**
>
> Kebijakan contoh berikut mendukung izin yang diperlukan untuk membaca AWS Glue metadata dan data Amazon S3 yang sesuai. Namun, Anda mungkin perlu mengubah

kebijakan ini tergantung pada cara Anda mengatur data S3. Kebijakan ini tidak menyertakan kunci KMS untuk mendekripsi data.
AWS Glue Sumber daya Anda dan sumber daya Amazon S3 yang mendasarinya harus Wilayah AWS sama dengan kolaborasi. AWS Clean Rooms

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

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

Jika Anda perlu menggunakan kunci KMS untuk mendekripsi data, tambahkan AWS KMS pernyataan ini ke template sebelumnya:

```
{
            "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. Pilih Selanjutnya.
6. Untuk meninjau dan membuat, masukkan nama Kebijakan dan Deskripsi, dan tinjau Ringkasan.
7. Pilih Buat kebijakan.

   Anda telah membuat kebijakan untuk AWS Clean Rooms.
8. Di bawah Manajemen akses, pilih Peran.

   Dengan Peran, Anda dapat membuat kredensyal jangka pendek, yang direkomendasikan untuk meningkatkan keamanan. Anda juga dapat memilih Pengguna untuk membuat kredensi jangka panjang.
9. Pilih Buat peran.
10. Di wizard Buat peran, untuk jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus.
11. Salin dan tempel kebijakan kepercayaan khusus berikut ke 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/*"
```

```
                }
            }
        }
    ]
}
```

`SourceAccount`Itu selalu AWS akun Anda. Ini `SourceArn` dapat dibatasi pada kumpulan data pelatihan tertentu, tetapi hanya setelah kumpulan data itu dibuat. Karena Anda tidak dapat mengetahui sebelumnya kumpulan data pelatihan ARN, wildcard ditentukan di sini.

12. Pilih Berikutnya dan di bawah Tambahkan izin, masukkan nama kebijakan yang baru saja Anda buat. (Anda mungkin perlu memuat ulang halaman.)
13. Pilih kotak centang di samping nama kebijakan yang Anda buat, lalu pilih Berikutnya.
14. Untuk Nama, tinjau, dan buat, masukkan nama Peran dan Deskripsi.

> **Note**
>
> Nama Peran harus cocok dengan pola dalam `passRole` izin yang diberikan kepada anggota yang dapat melakukan kueri dan menerima hasil dan peran anggota.

    a. Tinjau Pilih entitas tepercaya, dan edit jika perlu.
    b. Tinjau izin di Tambahkan izin, dan edit jika perlu.
    c. Tinjau Tag, dan tambahkan tag jika perlu.
    d. Pilih Buat peran.

15. Peran layanan untuk AWS Clean Rooms telah dibuat.

Buat peran layanan untuk menulis segmen yang mirip

AWS Clean Rooms menggunakan peran layanan untuk menulis segmen yang mirip ke ember. Anda dapat membuat peran ini menggunakan konsol jika Anda memiliki izin IAM yang diperlukan. Jika Anda tidak memiliki `CreateRole` izin, minta administrator Anda untuk membuat peran layanan.

Untuk membuat peran layanan untuk menulis segmen mirip

1. Masuk ke konsol IAM (https://console.aws.amazon.com/iam/) dengan akun administrator Anda.
2. Di bagian Manajemen akses, pilih Kebijakan.

3. Pilih Buat kebijakan.
4. Di editor Kebijakan, pilih tab JSON, lalu salin dan tempel kebijakan berikut.

> **Note**
>
> Kebijakan contoh berikut mendukung izin yang diperlukan untuk membaca AWS Glue metadata dan data Amazon S3 yang sesuai. Namun, Anda mungkin perlu mengubah kebijakan ini tergantung pada cara Anda mengatur data S3. Kebijakan ini tidak menyertakan kunci KMS untuk mendekripsi data.
> AWS Glue Sumber daya Anda dan sumber daya Amazon S3 yang mendasarinya harus Wilayah AWS sama dengan kolaborasi. AWS Clean Rooms

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

```
            "Condition":{
                "StringEquals":{
                    "s3:ResourceAccount":[
                        "accountId"
                    ]
                }
            }
        }
  ]
}
```

Jika Anda perlu menggunakan kunci KMS untuk mengenkripsi data, tambahkan AWS KMS pernyataan ini ke template:

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

Jika Anda perlu menggunakan kunci KMS untuk mendekripsi data, tambahkan AWS KMS pernyataan ini ke template:

```
{
            "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. Pilih Selanjutnya.
6. Untuk meninjau dan membuat, masukkan nama Kebijakan dan Deskripsi, dan tinjau Ringkasan.
7. Pilih Buat kebijakan.

   Anda telah membuat kebijakan untuk AWS Clean Rooms.
8. Di bawah Manajemen akses, pilih Peran.

   Dengan Peran, Anda dapat membuat kredensyal jangka pendek, yang direkomendasikan untuk meningkatkan keamanan. Anda juga dapat memilih Pengguna untuk membuat kredensi jangka panjang.
9. Pilih Buat peran.
10. Di wizard Buat peran, untuk jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus.
11. Salin dan tempel kebijakan kepercayaan khusus berikut ke 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/*"
                }
            }
        }
    ]
}
```

`SourceAccount`Itu selalu AWS akun Anda. Ini `SourceArn` dapat dibatasi pada kumpulan data pelatihan tertentu, tetapi hanya setelah kumpulan data itu dibuat. Karena Anda tidak dapat mengetahui sebelumnya kumpulan data pelatihan ARN, wildcard ditentukan di sini.

12. Pilih Selanjutnya.
13. Pilih kotak centang di samping nama kebijakan yang Anda buat, lalu pilih Berikutnya.
14. Untuk Nama, tinjau, dan buat, masukkan nama Peran dan Deskripsi.

> **Note**
>
> Nama Peran harus cocok dengan pola dalam `passRole` izin yang diberikan kepada anggota yang dapat melakukan kueri dan menerima hasil dan peran anggota.

    a. Tinjau Pilih entitas tepercaya, dan edit jika perlu.
    b. Tinjau izin di Tambahkan izin, dan edit jika perlu.
    c. Tinjau Tag, dan tambahkan tag jika perlu.
    d. Pilih Buat peran.
15. Peran layanan untuk AWS Clean Rooms telah dibuat.

Buat peran layanan untuk membaca data benih

AWS Clean Rooms menggunakan peran layanan untuk membaca data benih. Anda dapat membuat peran ini menggunakan konsol jika Anda memiliki izin IAM yang diperlukan. Jika Anda tidak memiliki `CreateRole` izin, minta administrator Anda untuk membuat peran layanan.

Untuk membuat peran layanan untuk membaca data benih

1. Masuk ke konsol IAM (https://console.aws.amazon.com/iam/) dengan akun administrator Anda.
2. Di bagian Manajemen akses, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Di editor Kebijakan, pilih tab JSON, lalu salin dan tempel kebijakan berikut.

> **Note**
>
> Kebijakan contoh berikut mendukung izin yang diperlukan untuk membaca AWS Glue metadata dan data Amazon S3 yang sesuai. Namun, Anda mungkin perlu mengubah kebijakan ini tergantung pada cara Anda mengatur data S3. Kebijakan ini tidak menyertakan kunci KMS untuk mendekripsi data.
> AWS Glue Sumber daya Anda dan sumber daya Amazon S3 yang mendasarinya harus Wilayah AWS sama dengan kolaborasi. AWS Clean Rooms

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

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

Jika Anda perlu menggunakan kunci KMS untuk mendekripsi data, tambahkan AWS KMS pernyataan ini ke template:

```
{
            "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. Pilih Selanjutnya.
6. Untuk meninjau dan membuat, masukkan nama Kebijakan dan Deskripsi, dan tinjau Ringkasan.
7. Pilih Buat kebijakan.

   Anda telah membuat kebijakan untuk AWS Clean Rooms.

8. Di bawah Manajemen akses, pilih Peran.

   Dengan Peran, Anda dapat membuat kredensyal jangka pendek, yang direkomendasikan untuk meningkatkan keamanan. Anda juga dapat memilih Pengguna untuk membuat kredensi jangka panjang.

9. Pilih Buat peran.

10. Di wizard Buat peran, untuk jenis entitas Tepercaya, pilih Kebijakan kepercayaan khusus.

11. Salin dan tempel kebijakan kepercayaan khusus berikut ke 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/*"
                }
            }
        }
    ]
}
```

   `SourceAccount`Itu selalu AWS akun Anda. Ini `SourceArn` dapat dibatasi pada kumpulan data pelatihan tertentu, tetapi hanya setelah kumpulan data itu dibuat. Karena Anda tidak dapat mengetahui sebelumnya kumpulan data pelatihan ARN, wildcard ditentukan di sini.

12. Pilih Selanjutnya.

13. Pilih kotak centang di samping nama kebijakan yang Anda buat, lalu pilih Berikutnya.

14. Untuk Nama, tinjau, dan buat, masukkan nama Peran dan Deskripsi.

> **Note**
>
> Nama Peran harus cocok dengan pola dalam `passRole` izin yang diberikan kepada anggota yang dapat melakukan kueri dan menerima hasil dan peran anggota.

a. Tinjau Pilih entitas tepercaya, dan edit jika perlu.
b. Tinjau izin di Tambahkan izin, dan edit jika perlu.
c. Tinjau Tag, dan tambahkan tag jika perlu.
d. Pilih Buat peran.

15. Peran layanan untuk AWS Clean Rooms telah dibuat.

Menciptakan kolaborasi di AWS Clean Rooms

Kolaborasi adalah batas logis yang aman AWS Clean Rooms di mana anggota dapat melakukan kueri SQL pada tabel yang dikonfigurasi.

Setiap anggota AWS Clean Rooms dapat membuat kolaborasi.

Pembuat kolaborasi dapat menunjuk satu anggota untuk melakukan kueri dan menerima hasil. Namun, pembuat kolaborasi mungkin ingin mencegah anggota yang dapat melakukan kueri agar tidak memiliki akses ke hasil kueri. Dalam hal ini, pembuat kolaborasi dapat menunjuk satu anggota untuk siapa yang dapat meminta dan anggota lain yang dapat menerima hasil.

Dalam kebanyakan kasus, anggota yang dapat menanyakan juga anggota yang membayar biaya komputasi kueri. Namun, pembuat kolaborasi dapat mengonfigurasi anggota yang berbeda agar bertanggung jawab membayar biaya komputasi kueri.

Untuk informasi tentang cara membuat kolaborasi menggunakan AWS SDK, lihat Referensi AWS Clean Rooms API.

Topik

Buat kolaborasi

Sebelum Anda mulai, pastikan Anda telah menyelesaikan prasyarat berikut:

- Anda memiliki nama dan Akun AWS ID untuk setiap anggota yang ingin Anda undang ke kolaborasi.
- Anda memiliki izin untuk membagikan nama dan Akun AWS ID untuk setiap anggota dengan semua anggota kolaborasi.

> **Note**
>
> Anda tidak dapat menambahkan lebih banyak anggota setelah kolaborasi dibuat.

Untuk membuat kolaborasi menggunakan AWS Clean Rooms konsol

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Akun AWS yang akan berfungsi sebagai pembuat kolaborasi.
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Di sudut kanan atas, pilih Buat kolaborasi.
4. Untuk Langkah 1: Tentukan kolaborasi, lakukan hal berikut:

    a. Untuk Detail, masukkan Nama dan Deskripsi kolaborasi.

    Informasi ini akan terlihat oleh anggota kolaborasi yang diundang untuk berpartisipasi dalam kolaborasi. Nama dan Deskripsi membantu mereka memahami apa yang dimaksud dengan kolaborasi.

    b. Untuk Anggota:

        i. Untuk Anggota 1: Anda, masukkan nama tampilan Anggota sesuai keinginan untuk kolaborasi.

        > **Note**
        >
        > Akun AWSID Anda disertakan secara otomatis untuk Akun AWSID Anggota.

        ii. Untuk Anggota 2, masukkan nama tampilan Anggota dan Akun AWS ID Anggota untuk anggota yang ingin Anda undang ke kolaborasi.

        Nama tampilan Anggota dan Akun AWSID Anggota akan terlihat oleh semua orang yang diundang ke kolaborasi. Setelah Anda memasukkan dan menyimpan nilai untuk bidang ini, mereka tidak dapat diedit.

        > **Note**
        >
        > Anda harus memberi tahu anggota kolaborasi bahwa Akun AWSID Anggota dan nama tampilan Anggota mereka akan terlihat oleh semua kolaborator yang diundang dan aktif dalam kolaborasi.

        iii. Jika Anda ingin menambahkan anggota lain, pilih Tambahkan anggota lain. Kemudian masukkan nama tampilan Anggota dan Akun AWSID Anggota untuk setiap anggota yang dapat menyumbangkan data yang ingin Anda undang ke kolaborasi.

c. Untuk kemampuan Anggota, pilih salah satu dari berikut ini,

Jika Anda ingin...	Lalu...
Kueri data dalam kolaborasi dan terima hasilnya	1. Pilih diri Anda sebagai anggota yang dapat Menjalankan kueri. 2. Biarkan pengaturan default anggota yang dapat Menerima hasil adalah Sama seperti yang menjalankan kueri.
Kueri data dalam kolaborasi dan tetapkan anggota yang berbeda untuk menerima hasil	1. Pilih diri Anda sebagai anggota yang dapat Menjalankan kueri. 2. Pilih anggota yang dapat Menerima hasil dari daftar dropdown.
Menerima hasil kueri dalam kolaborasi dan menetapkan anggota yang berbeda untuk kueri data	1. Pilih anggota yang dapat Jalankan kueri dari daftar dropdown. 2. Pilih diri Anda sebagai anggota yang dapat Menerima hasil dari daftar dropdown.
Buat dan kelola kolaborasi, tetapkan anggota yang berbeda untuk menanyakan data, dan menetapkan anggota lain untuk menerima hasil	1. Pilih anggota yang dapat Jalankan kueri dari daftar dropdown. 2. Pilih anggota yang dapat Menerima hasil dari daftar dropdown.

d. Untuk konfigurasi Pembayaran, pilih salah satu dari berikut ini:

Jika Anda ingin...	Lalu...
Tetapkan anggota yang dapat Menjalankan kueri untuk menjadi anggota yang membayar biaya komputasi kueri	Biarkan pengaturan default anggota yang akan Membayar kueri adalah Sama seperti yang menjalankan kueri.

Jika Anda ingin...	Lalu...
Tetapkan anggota yang berbeda untuk membayar biaya komputasi kueri	Pilih anggota yang akan membayar kueri dari daftar dropdown.

e. Jika Anda ingin mengaktifkan Pencatatan kueri, pilih kotak centang Pencatatan kueri Dukungan untuk kolaborasi ini.

f. Jika Anda ingin mengaktifkan kemampuan komputasi Cryptographic, pilih kotak centang Support cryptographic computing dalam kolaborasi ini dan pilih parameter komputasi Cryptographic berikut:

- Izinkan cleartext kolom

  Pilih Tidak jika Anda tidak ingin cleartext kolom diizinkan dalam tabel terenkripsi.

  Pilih Ya jika Anda ingin cleartext kolom diizinkan dalam tabel terenkripsi.

  Untuk menjalankan SUM atau AVG pada kolom tertentu, kolom harus masukcleartext.

- Izinkan duplikat

  Pilih Tidak jika Anda tidak ingin entri duplikat diizinkan dalam kolom. fingerprint

  Pilih Ya jika Anda ingin entri duplikat diizinkan dalam kolom. fingerprint

- Izinkan JOIN kolom dengan nama yang berbeda

  Pilih Tidak jika Anda tidak ingin bergabung dengan fingerprint kolom dengan nama yang berbeda.

  Pilih Ya jika Anda ingin bergabung dengan fingerprint kolom dengan nama yang berbeda.

- Pertahankan NULL nilai

  Pilih Tidak jika Anda tidak ingin mempertahankan NULL nilai. NULLnilai tidak akan muncul seperti NULL dalam tabel terenkripsi.

  Pilih Ya jika Anda ingin mempertahankan NULL nilai. NULLnilai akan muncul seperti NULL dalam tabel terenkripsi.

Untuk informasi selengkapnya tentang parameter komputasi kriptografi, lihatParameter komputasi kriptografi.

Untuk informasi selengkapnya tentang cara mengenkripsi data Anda untuk digunakanAWS Clean Rooms, lihatMempersiapkan tabel data terenkripsi dengan Cryptographic Computing untuk Clean Rooms.

> **Note**
>
> Verifikasi konfigurasi ini dengan hati-hati sebelum menyelesaikan langkah berikutnya. Setelah membuat kolaborasi, Anda hanya dapat mengedit nama kolaborasi, deskripsi, dan apakah log kueri disimpan di Amazon CloudWatch Logs.

g. Jika Anda ingin mengaktifkan Tag untuk sumber kolaborasi, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.

h. Pilih Selanjutnya.

5. Untuk Langkah 2: Konfigurasikan keanggotaan, lakukan hal berikut:

a. Pilih satu opsi:

Jika Anda memilih...	Lalu...
Ya, bergabunglah dengan membuat keanggotaan sekarang	Kolaborasi dan keanggotaan Anda dibuat. Status Anda dalam kolaborasi aktif.
Tidak, saya akan membuat keanggotaan nanti	Hanya kolaborasi yang dibuat. Status Anda dalam kolaborasi tidak aktif.

b. Jika Anda adalah anggota yang dapat Menerima hasil, di bawah Pengaturan hasil kueri default, pilih salah satu opsi:

Jika kau...	Lalu...
Simpan kotak centang Setel pengaturan default sekarang dipilih. (Ini dipilih secara default.)	1. Untuk tujuan Hasil di Amazon S3, masukkan tujuan Amazon S3. 2. Untuk format hasil kueri, pilih CSV atau PARQUET.
Kosongkan kotak centang Setel pengaturan default sekarang	Hanya kolaborasi yang dibuat. Status Anda dalam kolaborasi tidak aktif.

c. Jika Anda memilih untuk mengaktifkan pencatatan Kueri di langkah 4.e, pilih salah satu opsi berikut untuk penyimpanan Log di Amazon CloudWatch Logs:

Jika Anda memilih...	Lalu...
Nyalakan	Log kueri yang relevan dengan Anda disimpan di CloudWatch Log Amazon. Setiap anggota hanya dapat menerima log untuk kueri yang mereka mulai atau yang berisi data mereka. Anggota yang dapat menerima hasil juga menerima log untuk semua kueri yang dijalankan dalam kolaborasi, bahkan jika data mereka tidak diakses dalam kueri.
Matikan	Log kueri yang relevan dengan Anda tidak disimpan di akun Amazon CloudWatch Logs Anda.

> **Note**
>
> Setelah Anda mengaktifkan pencatatan Kueri, penyimpanan log dapat diatur beberapa menit dan mulai menerima log di Amazon CloudWatch Logs. Selama

periode singkat ini, anggota yang dapat melakukan kueri mungkin menjalankan kueri yang sebenarnya tidak mengirim log.

d. Jika Anda ingin mengaktifkan Tag untuk sumber daya keanggotaan, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.

e. Jika Anda adalah anggota yang Membayar untuk kueri, tunjukkan penerimaan Anda dengan memilih kotak centang Saya setuju untuk membayar biaya komputasi kueri dalam kolaborasi ini.

> **Note**
>
> Anda harus memilih kotak centang ini untuk melanjutkan.
> Untuk informasi selengkapnya tentang cara penghitungan harga, lihatHarga untuk AWS Clean Rooms.

Jika Anda adalah anggota yang membayar biaya komputasi kueri tetapi bukan anggota yang dapat melakukan kueri, disarankan agar Anda menggunakan AWS Budgets untuk mengonfigurasi anggaran AWS Clean Rooms dan menerima pemberitahuan setelah anggaran maksimum tercapai. Untuk informasi selengkapnya tentang menyiapkan anggaran, lihat Mengelola biaya Anda AWS Budgets di Panduan AWS Cost Management Pengguna. Untuk informasi selengkapnya tentang mengatur notifikasi, lihat Membuat topik Amazon SNS untuk pemberitahuan anggaran di AWS Cost ManagementPanduan Pengguna. Jika anggaran maksimum telah tercapai, Anda dapat menghubungi anggota yang dapat menjalankan kueri atau meninggalkan kolaborasi. Jika Anda meninggalkan kolaborasi, tidak ada lagi kueri yang diizinkan untuk dijalankan, dan oleh karena itu Anda tidak akan lagi ditagih untuk biaya komputasi kueri.

f. Pilih Selanjutnya.

6. Untuk Langkah 3: Tinjau dan buat, lakukan hal berikut:

a. Tinjau pilihan yang Anda buat untuk langkah-langkah sebelumnya dan edit jika perlu.

b. Pilih salah satu dari berikut:

Jika Anda memilih untuk...	Kemudian pilih...
Buat keanggotaan dengan kolaborasi (Ya, bergabung dengan membuat keanggotaan sekarang)	Buat kolaborasi dan keanggotaan
Buat kolaborasi, dan bukan untuk membuat keanggotaan saat ini (Tidak, saya akan membuat keanggotaan nanti)	Buat kolaborasi

Setelah kolaborasi Anda berhasil dibuat, Anda dapat melihat halaman detail kolaborasi di bawah Kolaborasi.

Langkah selanjutnya

Anda sekarang siap untuk:

- Siapkan tabel data Anda untuk ditanyakan. AWS Clean Rooms (Opsional jika Anda ingin menanyakan data Anda sendiri.)
- Kaitkan tabel yang dikonfigurasi dengan kolaborasi Anda. (Opsional jika Anda ingin menanyakan data Anda sendiri.)
- Konfigurasikan aturan analisis untuk tabel yang dikonfigurasi. (Opsional jika Anda ingin menanyakan data Anda sendiri.)
- Buat keanggotaan dan bergabunglah dengan kolaborasi.
- Kelola kolaborasi Anda.

Membuat keanggotaan dan bergabung dengan kolaborasi

Keanggotaan adalah sumber daya yang dibuat ketika anggota bergabung dengan kolaborasi. AWS Clean Rooms

Anda dapat bergabung dengan kolaborasi sebagai anggota yang dapat melakukan kueri data, anggota yang dapat menerima hasil kueri, atau keduanya. Anda juga dapat bergabung dengan kolaborasi sebagai anggota yang membayar biaya komputasi kueri. Semua anggota dapat menyumbangkan data.

Untuk informasi tentang cara membuat keanggotaan dan bergabung dengan kolaborasi menggunakan AWS SDK, lihat Referensi AWS Clean Rooms API.

Topik

Buat keanggotaan dan bergabunglah dengan kolaborasi

Untuk membuat keanggotaan dan bergabung dengan kolaborasi

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan anggota Anda Akun AWS.
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pada tab Tersedia untuk bergabung, untuk Kolaborasi yang tersedia untuk bergabung, pilih Nama kolaborasi.
4. Pada halaman detail kolaborasi, lihat detail kolaborasi, termasuk detail anggota Anda dan daftar anggota lainnya.

   Verifikasi bahwa Akun AWS ID untuk setiap anggota kolaborasi adalah yang ingin Anda masuki dalam kolaborasi.
5. Pilih Buat keanggotaan.
6. Pada halaman Buat keanggotaan, di Ringkasan, lihat nama Kolaborasi, Deskripsi Kolaborasi, Akun AWS ID pembuat Kolaborasi, Kemampuan anggota Anda, dan Akun AWS ID anggota yang akan Membayar kueri.

7. Jika pembuat kolaborasi telah memilih untuk mengaktifkan pencatatan Kueri, pilih salah satu opsi berikut untuk penyimpanan Log di Amazon CloudWatch Logs:

Jika Anda memilih...	Lalu...
Nyalakan	Log kueri yang relevan dengan Anda disimpan di CloudWatch Log Amazon. Setiap anggota hanya dapat menerima log untuk kueri yang mereka mulai atau yang berisi data mereka. Anggota yang dapat menerima hasil juga menerima log untuk semua kueri yang dijalankan dalam kolaborasi, meskipun data mereka tidak diakses dalam kueri.
Matikan	Log kueri yang relevan dengan Anda tidak disimpan di akun Amazon CloudWatch Logs Anda.

> **Note**
>
> Setelah Anda mengaktifkan pencatatan Kueri, penyimpanan log dapat diatur beberapa menit dan mulai menerima log di Amazon CloudWatch Logs. Selama periode singkat ini, anggota yang dapat melakukan kueri mungkin menjalankan kueri yang sebenarnya tidak mengirim log.

8. Jika kemampuan anggota Anda termasuk Menerima hasil:

   a. Untuk pengaturan hasil Kueri,

      i. Tentukan tujuan Hasil di Amazon S3 dengan memasukkan tujuan S3 atau pilih Jelajahi S3 untuk memilih dari daftar bucket S3 yang tersedia.

         Example

         Misalnya: **`s3://bucket/prefix`**

ii. Pilih format Hasil (CSV atau PARQUET).

b. Untuk akses Layanan, pilih Membuat dan menggunakan peran layanan baru atau Gunakan peran layanan yang ada.

> **Note**
>
> Anda harus memilih peran layanan yang ada atau memiliki izin untuk membuat yang baru. Untuk informasi selengkapnya, lihat Buat peran layanan untuk menerima hasil.

9. Jika Anda ingin mengaktifkan Tag untuk sumber daya keanggotaan, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.

10. Jika pembuat kolaborasi telah menunjuk Anda sebagai anggota yang akan membayar kueri, tunjukkan penerimaan Anda dengan memilih kotak centang Saya setuju untuk membayar biaya komputasi kueri dalam kolaborasi ini.

> **Note**
>
> Anda harus memilih kotak centang ini untuk melanjutkan.
> Untuk informasi selengkapnya tentang cara penghitungan harga, lihatHarga untuk AWS Clean Rooms.

Jika Anda adalah anggota yang membayar biaya komputasi kueri tetapi bukan anggota yang dapat melakukan kueri, disarankan agar Anda menggunakan AWS Budgets untuk mengonfigurasi anggaran AWS Clean Rooms dan menerima pemberitahuan setelah anggaran maksimum tercapai. Untuk informasi selengkapnya tentang menyiapkan anggaran, lihat Mengelola biaya Anda AWS Budgets di Panduan AWS Cost Management Pengguna. Untuk informasi selengkapnya tentang mengatur notifikasi, lihat Membuat topik Amazon SNS untuk pemberitahuan anggaran di AWS Cost Management Panduan Pengguna. Jika anggaran maksimum telah tercapai, Anda dapat menghubungi anggota yang dapat menjalankan kueri atau meninggalkan kolaborasi. Jika Anda meninggalkan kolaborasi, tidak ada lagi kueri yang diizinkan untuk dijalankan, dan oleh karena itu Anda tidak akan lagi ditagih untuk biaya komputasi kueri.

11. Jika Anda yakin ingin membuat keanggotaan dan bergabung dengan kolaborasi, pilih Buat keanggotaan.

Anda diberi akses baca ke metadata kolaborasi. Ini termasuk informasi seperti nama tampilan dan deskripsi kolaborasi, selain semua nama dan Akun AWS ID anggota lain.

Untuk informasi tentang cara meninggalkan kolaborasi, lihatMeninggalkan Kolaborasi.

Langkah selanjutnya

Anda sekarang siap untuk:

- Siapkan tabel data Anda untuk ditanyakan. AWS Clean Rooms(Opsional jika Anda ingin menanyakan data Anda sendiri.)
- Kaitkan tabel yang dikonfigurasi dengan kolaborasi Anda.
- Konfigurasikan aturan analisis untuk tabel yang dikonfigurasi.

Mempersiapkan tabel data untuk kueri di AWS Clean Rooms

> **Note**
>
> Mempersiapkan tabel data dapat dilakukan sebelum atau setelah Anda bergabung dengan kolaborasi. Setelah tabel disiapkan, Anda dapat menggunakannya kembali di beberapa kolaborasi selama kebutuhan privasi Anda untuk tabel itu sama.

Sebagai anggota dalam kolaborasi, Anda harus menyiapkan tabel data Anda sebelum mereka dapat ditanyakan AWS Clean Rooms oleh anggota kolaborasi yang dapat melakukan kueri.

Jika kasus penggunaan Anda tidak mengharuskan Anda untuk membawa data Anda sendiri, Anda dapat melewati prosedur ini.

Jika tabel data Anda sudah dikatalogkan AWS Glue, lewati ke. Membuat tabel yang dikonfigurasi di AWS Clean Rooms

Mempersiapkan tabel data Anda melibatkan langkah-langkah berikut:

- Langkah 1: Selesaikan prasyarat
- Langkah 2: (Opsional) Siapkan data Anda untuk komputasi kriptografi
- Langkah 3: Unggah tabel data Anda ke Amazon S3
- Langkah 4: Buat AWS Glue tabel
- Langkah selanjutnya

Untuk informasi selengkapnya tentang format data yang dapat Anda gunakan untuk kueri, lihatFormat data untuk AWS Clean Rooms.

Langkah 1: Selesaikan prasyarat

Untuk menyiapkan tabel data Anda untuk digunakan AWS Clean Rooms, Anda harus menyelesaikan prasyarat berikut:

- Kumpulan data Anda harus disimpan sebagai salah satu format data yang didukung untuk. AWS Clean Rooms

- Tabel data Anda harus dikatalogkan AWS Glue dan menggunakan tipe data yang didukung untuk. AWS Clean Rooms
- Semua tabel data Anda harus disimpan di Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) Wilayah AWS sama dengan saat kolaborasi dibuat.
- AWS Glue Data Catalog Harus berada di Wilayah yang sama di mana kolaborasi dibuat.
- AWS Glue Data Catalog Harus sama Akun AWS dengan keanggotaan.
- Bucket Amazon S3 tidak dapat didaftarkan. AWS Lake Formation
- Pembuat kolaborasi telah membuat kolaborasi di AWS Clean Rooms. Untuk informasi selengkapnya, lihat Menciptakan kolaborasi di AWS Clean Rooms.
- Pembuat kolaborasi telah mengirimkan ID kolaborasi kepada Anda sebagai peserta dalam kolaborasi.

Langkah 2: (Opsional) Siapkan data Anda untuk komputasi kriptografi

(Opsional) Jika Anda menggunakan komputasi kriptografi dan tabel data Anda berisi informasi sensitif yang ingin Anda enkripsi, Anda harus mengenkripsi tabel data menggunakan klien enkripsi C3R.

Untuk mempersiapkan data Anda untuk komputasi kriptografi, ikuti prosedur diMempersiapkan tabel data terenkripsi dengan Cryptographic Computing untuk Clean Rooms.

Langkah 3: Unggah tabel data Anda ke Amazon S3

> **Note**
>
> Jika Anda bermaksud menggunakan tabel data terenkripsi dalam kolaborasi, Anda harus terlebih dahulu mengenkripsi data untuk komputasi kriptografi sebelum mengunggah tabel data Anda ke Amazon S3. Untuk informasi selengkapnya, lihat Mempersiapkan tabel data terenkripsi dengan Cryptographic Computing untuk Clean Rooms.

Untuk mengunggah tabel data Anda ke Amazon S3

1. Masuk ke AWS Management Console dan buka konsol Amazon S3 di https://console.aws.amazon.com/s3/.

2. Pilih Bucket, lalu pilih bucket tempat Anda ingin menyimpan tabel data Anda.
3. Pilih Unggah, lalu ikuti petunjuknya.
4. Pilih tab Objek untuk melihat awalan tempat data Anda disimpan. Catat nama folder.

   Anda dapat memilih folder untuk melihat data.

Langkah 4: Buat AWS Glue tabel

Jika Anda sudah memiliki tabel AWS Glue data, Anda dapat melewati langkah ini.

Pada langkah ini, Anda menyiapkan crawler yang meng-crawl semua file di bucket S3 dan membuat tabel. AWS Glue AWS Glue Untuk informasi selengkapnya, lihat Mendefinisikan crawler AWS Glue di AWS Glue Panduan Pengguna.

Untuk informasi selengkapnya tentang tipe AWS Glue Data Catalog data yang didukung, lihatJenis data yang didukung.

> **Note**
>
> AWS Clean Rooms saat ini tidak mendukung bucket S3 yang terdaftar. AWS Lake Formation

Prosedur berikut menjelaskan cara membuat AWS Glue tabel. Jika Anda ingin menggunakan AWS Glue Data Catalog objek terenkripsi dengan kunci AWS Key Management Service (AWS KMS), Anda perlu mengonfigurasi kebijakan izin kunci KMS untuk mengizinkan akses ke tabel terenkripsi tersebut. Untuk informasi selengkapnya, lihat Menyiapkan enkripsi di AWS Glue di Panduan AWS Glue Pengembang.

Untuk membuat AWS Glue tabel

1. Ikuti Bekerja dengan crawler pada prosedur AWS Glue konsol di Panduan AWS Glue Pengguna.
2. Buat catatan nama AWS Glue database dan nama AWS Glue tabel.

Langkah selanjutnya

Sekarang setelah Anda menyiapkan tabel data Anda, Anda siap untuk:

- Buat tabel yang dikonfigurasi

- Buat model ML

Format data untuk AWS Clean Rooms

Kumpulan data yang Anda gunakan untuk kueri biasanya AWS Clean Rooms adalah jenis kumpulan data yang sama yang Anda gunakan untuk aplikasi lain. Misalnya, jenis kumpulan data yang sama digunakan dengan Amazon Athena, Amazon EMR, Amazon Redshift Spectrum, dan Amazon. QuickSight Anda dapat menanyakan data dalam format aslinya langsung dari Amazon Simple Storage Service (Amazon S3).

Untuk kueri data, kumpulan data harus dalam format yang AWS Clean Rooms mendukung. Bucket Amazon S3 dengan kumpulan data dan AWS Clean Rooms cluster harus sama. Wilayah AWS

Format data yang didukung

AWS Clean Rooms mendukung format terstruktur berikut:

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

> **Note**
>
> `timestamp`Nilai dalam file teks harus dalam format`yyyy-MM-dd HH:mm:ss.SSSSSS`. Misalnya:`2017-05-01 11:30:59.000000`.

Sebaiknya gunakan format file penyimpanan kolumnar, seperti. Apache Parquet Dengan format file penyimpanan kolumnar, Anda dapat meminimalkan transfer data dari Amazon S3 dengan memilih

hanya kolom yang Anda butuhkan. Untuk kinerja optimal, objek besar harus dibagi menjadi objek 100mb—1gb.

Jenis data yang didukung

Untuk pengalaman yang optimal AWS Clean Rooms, semua data Anda harus dikatalogkan. AWS Glue Untuk informasi selengkapnya, lihat bagian berjudul Memulai dengan AWS Glue Data Catalog di Panduan AWS Glue Pengembang.

AWS Clean Rooms mendukung tipe AWS Glue Data Catalog data berikut:

- bigint
- boolean
- char
- date
- decimal
- double
- float
- int
- Tipe data bersarang seperti:
  - array
  - map
  - struct
- smallint
- string
- timestamp
- varchar

AWS Clean Rooms tidak mendukung:

- biner
- interval

Jenis kompresi file untuk AWS Clean Rooms

Untuk mengurangi ruang penyimpanan, meningkatkan kinerja, dan meminimalkan biaya, kami sangat menyarankan Anda untuk mengompres kumpulan data Anda.

AWS Clean Rooms mengenali jenis kompresi file berdasarkan ekstensi file dan mendukung jenis kompresi dan ekstensi yang ditunjukkan pada tabel berikut.

Algoritma kompresi	Ekstensi file
GZIP	.gz
Bzip2	.bz2
Snappy	.snappy

Anda dapat menerapkan kompresi pada level yang berbeda. Paling umum, Anda mengompres seluruh file atau mengompres blok individual dalam file. Mengompresi format kolumnar pada tingkat file tidak menghasilkan manfaat kinerja.

Enkripsi sisi server untuk AWS Clean Rooms

> **Note**
>
> Enkripsi sisi server tidak menggantikan komputasi kriptografi untuk kasus penggunaan yang memerlukannya.

AWS Clean Rooms secara transparan mendekripsi kumpulan data yang dienkripsi menggunakan opsi enkripsi berikut:

- SSE-S3 - Enkripsi sisi server menggunakan kunci enkripsi AES-256 yang dikelola oleh Amazon S3
- SSE-KMS - Enkripsi sisi server dengan kunci yang dikelola oleh AWS Key Management Service

Untuk menggunakan SSE-S3, peran AWS Clean Rooms layanan yang digunakan untuk mengaitkan tabel yang dikonfigurasi ke kolaborasi harus memiliki izin dekripsi KMS. Untuk menggunakan SSE-KMS, kebijakan kunci KMS juga harus mengizinkan peran AWS Clean Rooms layanan untuk mendekripsi.

AWS Clean Rooms tidak mendukung enkripsi sisi klien Amazon S3. Untuk informasi selengkapnya tentang enkripsi sisi server, lihat Melindungi data menggunakan enkripsi sisi server di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Menggunakan Apache Iceberg tabel di AWS Clean Rooms

Apache Icebergadalah format tabel sumber terbuka untuk danau data. AWS Clean Rooms dapat menggunakan statistik yang disimpan dalam Apache Iceberg metadata untuk mengoptimalkan rencana kueri dan mengurangi pemindaian file selama pemrosesan kueri ruang bersih. Untuk informasi lebih lanjut, lihat dokumentasi Apache Iceberg.

Pertimbangkan hal berikut saat menggunakan AWS Clean Rooms dengan tabel Iceberg:

- Tabel dalam AWS Glue Data Catalog satu-satunya — Apache Iceberg tabel harus didefinisikan AWS Glue Data Catalog berdasarkan implementasi katalog lem open source.
- Format file parket - AWS Clean Rooms hanya mendukung tabel Iceberg dalam format file data Parket.
- Kompresi GZIP dan Snappy — AWS Clean Rooms mendukung Parket dengan GZIP dan kompresi. Snappy
- Versi Iceberg - AWS Clean Rooms mendukung menjalankan kueri terhadap versi 1 dan versi 2 tabel Iceberg.
- Partisi — Anda tidak perlu menambahkan partisi secara manual untuk Apache Iceberg tabel Anda. AWS Glue AWS Clean Rooms mendeteksi partisi baru dalam Apache Iceberg tabel secara otomatis dan tidak diperlukan operasi manual untuk memperbarui partisi dalam definisi tabel. Partisi gunung es muncul sebagai kolom reguler dalam skema AWS Clean Rooms tabel dan tidak secara terpisah sebagai kunci partisi dalam skema tabel yang dikonfigurasi.
- Batasan
  - Hanya tabel Iceberg baru

    Apache Icebergtabel yang dikonversi dari Apache Parquet tabel tidak didukung.
  - Pertanyaan perjalanan waktu

    AWS Clean Rooms tidak mendukung kueri perjalanan waktu dengan Apache Iceberg tabel.
  - Mesin Athena versi 2

    Icebergtabel yang dibuat dengan mesin Athena versi 2 tidak didukung.
  - Format berkas

Avrodan format file Optimized Row Columnar (ORC) tidak didukung.

- Kompresi

  Zstandard(Zstd) kompresi untuk tidak Parquet didukung.

Tipe data yang didukung untuk tabel Iceberg

AWS Clean Rooms dapat menanyakan Iceberg tabel yang berisi tipe data berikut:

- boolean
- date
- decimal
- double
- float
- int
- list
- long
- map
- string
- struct
- timestamp without time zone

Untuk informasi selengkapnya tentang tipe data Gunung Es, lihat Skema untuk Gunung Es di dokumentasi Apache Iceberg.

Mempersiapkan tabel data terenkripsi dengan Cryptographic Computing untuk Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) adalah kemampuan dalam. AWS Clean Rooms Anda dapat menggunakan C3R untuk membatasi secara kriptografi apa yang dapat dipelajari oleh pihak mana pun dan AWS dalam kolaborasi. AWS Clean Rooms

Anda dapat mengenkripsi tabel data menggunakan klien enkripsi C3R, alat enkripsi sisi klien, sebelum mengunggah tabel data ke Amazon Simple Storage Service (Amazon S3).

Untuk informasi selengkapnya, lihat Komputasi Kriptografi untuk Clean Rooms.

Mempersiapkan tabel data terenkripsi dengan C3R melibatkan langkah-langkah berikut:

Langkah-langkah

- Langkah 1: Selesaikan prasyarat
- Langkah 2: Unduh klien enkripsi C3R
- (Opsional) Langkah 3: Lihat perintah yang tersedia di klien enkripsi C3R
- Langkah 4: Buat skema enkripsi untuk file tabular
- Langkah 5: Buat kunci rahasia bersama
- Langkah 6: Simpan kunci rahasia bersama dalam variabel lingkungan
- Langkah 7: Enkripsi data
- Langkah 8: Verifikasi enkripsi data
- (Opsional) Buat skema (pengguna tingkat lanjut)

Langkah 1: Selesaikan prasyarat

Untuk menyiapkan tabel data Anda untuk digunakan dengan C3R, Anda harus menyelesaikan prasyarat berikut:

- Anda dapat mengakses Komputasi Kriptografi untuk Clean Rooms repositori di: GitHub

  https://github.com/aws/c3r
- Anda telah menyiapkan AWS kredensil untuk menggunakan klien enkripsi C3R. Kredensil ini digunakan oleh klien enkripsi C3R untuk panggilan API hanya-baca untuk mengambil metadata

kolaborasi. AWS Clean Rooms Untuk informasi selengkapnya, lihat AWS CLI Mengonfigurasi Panduan AWS Command Line Interface Pengguna untuk Versi 2.

- Anda memiliki Java Runtime Environment (JRE) 11 atau lebih baru diinstal pada mesin Anda.
  - Yang direkomendasikanJava Runtime Environment, Amazon Corretto 11 atau lebih tinggi, dapat diunduh dari https://aws.amazon.com/corretto.
  - The Java Development Kit (JDK) termasuk yang sesuai JRE dari versi yang sama. Namun, kemampuan tambahan tidak JDK diperlukan untuk menjalankan klien enkripsi Cryptographic Computing for Clean Rooms (C3R).
- File data tabular Anda (.csv) atau Parquet file (. parquet) disimpan secara lokal.
- Anda atau anggota lain dalam kolaborasi memiliki kemampuan untuk membuat kunci rahasia bersama. Untuk informasi selengkapnya, lihat Langkah 5: Buat kunci rahasia bersama.
- Pencipta kolaborasi telah menciptakan kolaborasi AWS Clean Rooms dengan komputasi Cryptographic yang diaktifkan untuk kolaborasi. Untuk informasi selengkapnya, lihat Menciptakan kolaborasi di AWS Clean Rooms.
- Pembuat kolaborasi telah mengirimkan ID kolaborasi kepada Anda sebagai peserta dalam kolaborasi. Kolaborasi Amazon Resource Name (ARN) disertakan dalam undangan yang dikirim, yang berisi ID kolaborasi.

Langkah 2: Unduh klien enkripsi C3R

Untuk mengunduh klien enkripsi C3R dari GitHub

1. Buka Komputasi Kriptografi untuk Clean RoomsAWSGitHub repositori: https://github.com/aws/c3r
2. Pilih dan unduh file.

   Kode sumber, lisensi, dan materi terkait dapat dikloning atau diunduh sebagai file. zipfile dari halaman arahan GitHub repositori. (Lihat tombol Kode di kanan atas daftar konten repositori).

   Klien enkripsi C3R terbaru yang ditandatangani Java Executable File (yaitu, aplikasi antarmuka baris perintah) ada di halaman Rilis repositori. GitHub

   Paket klien enkripsi C3R untuk Apache Spark (`c3r-cli-spark`) adalah versi c3r-cli yang harus dikirimkan sebagai pekerjaan ke server Apache Spark yang sedang berjalan. Untuk informasi selengkapnya, lihat Menjalankan C3R di Apache Spark.

(Opsional) Langkah 3: Lihat perintah yang tersedia di klien enkripsi C3R

Gunakan prosedur ini untuk membiasakan diri dengan perintah yang tersedia di klien enkripsi C3R.

Untuk melihat semua perintah yang tersedia di klien enkripsi C3R

1. Dari antarmuka baris perintah (CLI), navigasikan ke folder yang berisi file yang diunduhc3r-cli.jar.
2. Jalankan perintah berikut: `java -jar c3r-cli.jar`
3. Lihat daftar perintah dan opsi yang tersedia.

Langkah 4: Buat skema enkripsi untuk file tabular

Untuk mengenkripsi data, diperlukan skema enkripsi yang menjelaskan bagaimana data akan digunakan. Bagian ini menjelaskan bagaimana klien enkripsi C3R membantu dalam menghasilkan skema enkripsi untuk file CSV dengan baris header atau file. Parquet

Anda hanya perlu melakukan ini sekali per file. Setelah skema ada, dapat digunakan kembali untuk mengenkripsi file yang sama (atau file apa pun dengan nama kolom yang identik). Jika nama kolom atau skema enkripsi yang diinginkan berubah, Anda harus memperbarui file skema. Untuk informasi selengkapnya, lihat (Opsional) Buat skema (pengguna tingkat lanjut).

> **Important**
>
> Sangat penting bahwa semua pihak yang berkolaborasi menggunakan kunci rahasia bersama yang sama. Pihak yang berkolaborasi juga harus mengoordinasikan nama kolom agar sesuai jika mereka akan JOIN di-ed atau dibandingkan untuk kesetaraan dalam kueri. Jika tidak, kueri SQL mungkin menghasilkan hasil yang tidak terduga atau salah. Namun, ini tidak diperlukan jika pembuat kolaborasi mengaktifkan pengaturan `allowJoinsOnColumnsWithDifferentNames` enkripsi selama pembuatan kolaborasi. Untuk informasi selengkapnya tentang setelan terkait enkripsi, lihat. Parameter komputasi kriptografi

Ketika dijalankan dalam mode skema, klien enkripsi C3R melewati kolom file input demi kolom, meminta Anda apakah dan bagaimana kolom itu harus diperlakukan. Jika file berisi banyak kolom

yang tidak diinginkan untuk output terenkripsi, pembuatan skema interaktif mungkin menjadi membosankan karena Anda harus melewati setiap kolom yang tidak diinginkan. Untuk menghindari hal ini, Anda dapat menulis skema secara manual, atau membuat versi sederhana dari file input yang hanya menampilkan kolom yang diinginkan. Kemudian, generator skema interaktif dapat dijalankan pada file yang dikurangi itu. Klien enkripsi C3R mengeluarkan informasi tentang file skema dan menanyakan bagaimana kolom sumber harus disertakan atau dienkripsi (jika ada) dalam output target.

Untuk setiap kolom sumber dalam file input, Anda diminta untuk:

1. Berapa banyak kolom target yang harus dihasilkan
2. Bagaimana setiap kolom target harus dienkripsi (jika ada)
3. Nama setiap kolom target
4. Bagaimana data harus diempuk sebelum enkripsi jika kolom dienkripsi sebagai kolom sealed

> **Note**
>
> Saat Anda mengenkripsi data untuk kolom yang telah dienkripsi sebagai sealed kolom, Anda harus menentukan data mana yang membutuhkan padding. Klien enkripsi C3R menyarankan padding default selama pembuatan skema yang membungkus semua entri dalam kolom dengan panjang yang sama.
> Saat menentukan panjangnya`fixed`, perhatikan bahwa padding dalam byte, bukan bit.

Berikut ini adalah tabel keputusan untuk membuat skema.

Tabel keputusan skema

Keputusan	Jumlah kolom target dari kolom sumber <' name-of-column '>?	Jenis kolom target: [c]cleartext, [f]fingerprint, atau [s]sealed?	Nama judul kolom target <default 'name-of-column'>	Tambahkan akhiran <suffix>ke header untuk menunjukkan bagaimana itu dienkripsi, [y] ya atau [n] tidak <default 'yes'>	<' name-of-column _disegel'> tipe bantalan: [n] satu, [f] tetap, atau [m] maks <default 'max'>
Biarkan kolom tidak terenkripsi.	1	c	Tidak berlaku	Tidak berlaku	Tidak berlaku
Enkripsi kolom sebagai fingerprint kolom.	1	f	Pilih default atau masukkan nama header baru.	Masukkan y untuk memilih default (`_fingerprint`) atau entern.	Tidak berlaku
Enkripsi kolom sebagai sealed kolom.	1	s	Pilih default atau masukkan nama header baru.	Masukkan y untuk memilih default (`_sealed`) atau entern.	Pilih jenis padding. Untuk informasi selengkapnya, lihat (Opsional) Buat skema (pengguna tingkat lanjut).

Keputusan	Jumlah kolom target dari kolom sumber <' name-of-column '>?	Jenis kolom target: [c]cleartext, [f]fingerprint, atau [s]sealed?	Nama judul kolom target <default 'name-of-column'>	Tambahkan akhiran <suffix>ke header untuk menunjukkan bagaimana itu dienkripsi, [y] ya atau [n] tidak <default 'yes'>	<' name-of-column _disegel'> tipe bantalan: [n] satu, [f] tetap, atau [m] maks <default 'max'>
Enkripsi kolom sebagai keduanya fingerprint dansealed.	2	Masukkan kolom target pertama: f. Masukkan kolom target kedua: s.	Pilih header target untuk setiap kolom target.	Masuk y untuk memilih default atau masuk n.	Pilih jenis padding (hanya untuk sealed kolom). Untuk informasi selengkapnya, lihat (Opsional) Buat skema (pengguna tingkat lanjut).

Berikut ini adalah dua contoh cara membuat skema enkripsi. Konten yang tepat dari interaksi Anda tergantung pada file input dan tanggapan yang Anda berikan.

Contoh

- Contoh: Menghasilkan skema enkripsi untuk fingerprint kolom dan kolom cleartext
- Contoh: Menghasilkan skema enkripsi dengansealed,fingerprint, dan kolom cleartext

Contoh: Menghasilkan skema enkripsi untuk fingerprint kolom dan kolom cleartext

Dalam contoh ini, untukads.csv, hanya ada dua kolom: username danad_variant. Untuk kolom ini, kami menginginkan yang berikut:

- Untuk username kolom yang akan dienkripsi sebagai kolom fingerprint
- Untuk ad_variant kolom menjadi cleartext kolom

Untuk menghasilkan skema enkripsi untuk fingerprint kolom dan kolom cleartext

1. (Opsional) Untuk memastikan c3r-cli.jar file dan file yang akan dienkripsi hadir:

   a. Arahkan ke direktori yang diinginkan dan jalankan ls (jika menggunakan Mac atauUnix/Linux) atau dir jika menggunakanWindows).

   b. Lihat daftar file data tabular (misalnya, .csv) dan pilih file untuk dienkripsi.

      Dalam contoh ini, ads.csv adalah file yang ingin kita enkripsi.

2. Dari CLI, jalankan perintah berikut untuk membuat skema secara interaktif.

```
java -jar c3r-cli.jar schema ads.csv --interactive --output=ads.json
```

> **Note**
>
> - Kau bisa larijava --jar PATH/TO/c3r-cli.jar. Atau, jika Anda telah menambahkan PATH/TO/c3r-cli.jar ke variabel lingkungan CLASSPATH Anda, Anda juga dapat menjalankan nama kelas. Klien enkripsi C3R akan mencari di CLASSPATH untuk menemukannya (misalnya,). java com.amazon.psion.cli.Main
> - --interactiveBendera memilih mode interaktif untuk mengembangkan skema. Ini memandu pengguna melalui wizard untuk membuat skema. Pengguna dengan keterampilan tingkat lanjut dapat membuat skema JSON mereka sendiri tanpa menggunakan wizard. Untuk informasi selengkapnya, lihat (Opsional) Buat skema (pengguna tingkat lanjut).

- `--output`Bendera menetapkan nama output. Jika Anda tidak menyertakan `--output` bendera, klien enkripsi C3R mencoba memilih nama keluaran default (seperti `<input>.out.csv` atau untuk skema,). `<input>.json`

3. Untuk`Number of target columns from source column 'username'?`, enter **1** dan kemudian tekan Enter.
4. Untuk`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, enter **f** dan kemudian tekan Enter.
5. Untuk`Target column headername <default 'username'>`, tekan Enter.

   Nama default '`username`' digunakan.
6. Untuk`Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, enter **y** dan kemudian tekan Enter.

> **Note**
>
> Mode interaktif menyarankan sufiks untuk ditambahkan ke header kolom terenkripsi (`_fingerprint`untuk kolom dan untuk fingerprint kolom). `_sealed` sealed Sufiks mungkin berguna saat Anda melakukan tugas seperti mengunggah data ke Layanan AWS atau membuat kolaborasi. AWS Clean Rooms Sufiks ini dapat membantu menunjukkan apa yang dapat dilakukan dengan data terenkripsi di setiap kolom. Misalnya, hal-hal tidak akan berfungsi jika Anda mengenkripsi kolom sebagai sealed kolom (`_sealed`) dan mencoba JOIN melakukannya atau mencoba sebaliknya.

7. Untuk`Number of target columns from source column 'ad_variant'?`, enter **1** dan kemudian tekan Enter.
8. Untuk`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, enter **c** dan kemudian tekan Enter.
9. Untuk`Target column headername <default 'username'>`, tekan Enter.

   Nama default '`ad_variant`' digunakan.

   Skema ditulis ke file baru bernama`ads.json`.

> **Note**
>
> Anda dapat melihat skema dengan membukanya di editor teks apa pun, seperti Notepad on Windows atau TextEdit onmacOS.

10. Anda sekarang siap untuk mengenkripsi data.

Contoh: Menghasilkan skema enkripsi dengansealed,fingerprint, dan kolom cleartext

Dalam contoh ini, untuk`sales.csv`, ada tiga kolom:`username`,`purchased`, dan`product`. Untuk kolom ini, kami menginginkan yang berikut:

- Untuk `product` kolom menjadi `sealed` kolom
- Untuk `username` kolom yang akan dienkripsi sebagai kolom `fingerprint`
- Untuk `purchased` kolom menjadi `cleartext` kolom

Untuk menghasilkan skema enkripsi dengansealed,fingerprint, dan kolom cleartext

1. (Opsional) Untuk memastikan c3r-cli.jar file dan file yang akan dienkripsi hadir:

   a. Arahkan ke direktori yang diinginkan dan jalankan `ls` (jika menggunakan Mac atauUnix/Linux) atau `dir` jika menggunakanWindows).

   b. Lihat daftar file data tabular (.csv) dan pilih file untuk dienkripsi.

      Dalam contoh ini, `sales.csv` adalah file yang ingin kita enkripsi.

2. Dari CLI, jalankan perintah berikut untuk membuat skema secara interaktif.

```
java -jar c3r-cli.jar schema sales.csv --interactive --
output=sales.json
```

> **Note**
>
> - `--interactive`Bendera memilih mode interaktif untuk mengembangkan skema. Ini memandu pengguna melalui alur kerja terpandu untuk membuat skema.

- Jika Anda adalah pengguna tingkat lanjut, Anda dapat membuat skema JSON Anda sendiri tanpa menggunakan alur kerja yang dipandu. Untuk informasi selengkapnya, lihat (Opsional) Buat skema (pengguna tingkat lanjut).
- Untuk file.csv tanpa header kolom, lihat `--noHeaders` tanda untuk perintah skema yang tersedia di CLI.
- `--output`Bendera menetapkan nama output. Jika Anda tidak menyertakan `--output` bendera, klien enkripsi C3R mencoba memilih nama keluaran default (seperti `<input>.out` atau untuk skema,). `<input>.json`

3. Untuk`Number of target columns from source column ‘username’?`, enter **1** dan kemudian tekan Enter.
4. Untuk`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, enter **f** dan kemudian tekan Enter.
5. Untuk`Target column headername <default 'username'>`, tekan Enter.

   Nama default '`username`' digunakan.
6. Untuk`Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, enter **y** dan kemudian tekan Enter.
7. Untuk`Number of target columns from source column ‘purchased’?`, enter **1** dan kemudian tekan Enter.
8. Untuk`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, enter **c** dan kemudian tekan Enter.
9. Untuk`Target column headername <default 'purchased'>`, tekan Enter.

   Nama default '`purchased`' digunakan.
10. Untuk`Number of target columns from source column ‘product’?`, enter **1** dan kemudian tekan Enter.
11. Untuk`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, enter **s** dan kemudian tekan Enter.
12. Untuk`Target column headername <default 'product'>`, tekan Enter.

    Nama default '`product`' digunakan.
13. Untuk`‘product_sealed’ padding type: [n]one, [f]ixed, or [m]ax <default ’max’?>`, tekan Enter untuk memilih default.

14. Untuk `Byte-length beyond max length to pad cleartext to in 'product_sealed' <default '0'>?` tekan Enter untuk memilih default.

    Skema ditulis ke file baru bernama`sales.json`.

15. Anda sekarang siap untuk mengenkripsi data.

Langkah 5: Buat kunci rahasia bersama

Untuk mengenkripsi tabel data, peserta kolaborasi harus menyetujui dan berbagi kunci rahasia bersama dengan aman.

Kunci rahasia bersama harus setidaknya 256-bit (32 byte). Anda dapat menentukan kunci yang lebih besar, tetapi itu tidak akan memberi Anda keamanan tambahan.

> **Important**
>
> Ingat, ID kunci dan kolaborasi yang digunakan untuk enkripsi dan dekripsi harus identik untuk semua peserta kolaborasi.

Bagian berikut memberikan contoh perintah konsol untuk menghasilkan kunci rahasia bersama yang disimpan seperti `secret.key` di direktori kerja terminal masing-masing saat ini.

Topik

- Contoh: Pembuatan kunci menggunakan OpenSSL
- Contoh: Pembuatan kunci saat Windows menggunakan PowerShell

Contoh: Pembuatan kunci menggunakan OpenSSL

Untuk pustaka kriptografi tujuan umum umum, jalankan perintah berikut untuk membuat kunci rahasia bersama.

```
openssl rand 32 > secret.key
```

Jika Anda menggunakan Windows dan belum OpenSSL menginstal, Anda dapat membuat kunci menggunakan contoh yang dijelaskan dalam Contoh: Pembuatan kunci saat Windows menggunakan PowerShell.

Contoh: Pembuatan kunci saat Windows menggunakan PowerShell

UntukPowerShell, aplikasi terminal tersediaWindows, jalankan perintah berikut untuk membuat kunci rahasia bersama.

```
$bs = New-Object Byte[](32);
[Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($bs); Set-
Content 'secret.key' -Encoding Byte -Value $bs
```

Langkah 6: Simpan kunci rahasia bersama dalam variabel lingkungan

Variabel lingkungan adalah cara yang nyaman dan dapat diperluas bagi pengguna untuk menyediakan kunci rahasia dari berbagai toko utama seperti AWS Secrets Manager dan meneruskannya ke klien enkripsi C3R.

Klien enkripsi C3R dapat menggunakan kunci yang disimpan Layanan AWS jika Anda menggunakan AWS CLI untuk menyimpan kunci tersebut dalam variabel lingkungan yang relevan. Misalnya, klien enkripsi C3R dapat menggunakan kunci dari. AWS Secrets Manager Untuk informasi selengkapnya, lihat Membuat dan mengelola rahasia AWS Secrets Manager di Panduan AWS Secrets Manager Pengguna.

> **Note**
>
> Namun, sebelum Anda menggunakan Layanan AWS seperti AWS Secrets Manager untuk menahan kunci C3R Anda, verifikasi bahwa kasus penggunaan Anda mengizinkannya. Kasus penggunaan tertentu mungkin mengharuskan kunci ditahan. AWS Ini untuk memastikan bahwa data terenkripsi dan kunci tidak pernah dipegang oleh pihak ketiga yang sama.

Satu-satunya persyaratan untuk kunci rahasia bersama adalah bahwa kunci rahasia bersama base64 dikodekan dan disimpan dalam variabel lingkungan. `C3R_SHARED_SECRET`

Bagian berikut menjelaskan perintah konsol untuk mengonversi `secret.key` file ke base64 dan menyimpannya sebagai variabel lingkungan. `secret.key`File dapat dihasilkan dari salah satu perintah yang tercantum di Langkah 5: Buat kunci rahasia bersama dan hanya merupakan sumber contoh.

Simpan kunci dalam variabel lingkungan saat Windows menggunakan PowerShell

Untuk mengonversi ke base64 dan mengatur variabel lingkungan saat Windows menggunakanPowerShell, jalankan perintah berikut.

```
$Bytes=[IO.File]::ReadAllBytes((Get-Location).ToString()+'\secret.key');
 $env:C3R_SHARED_SECRET=[Convert]::ToBase64String($Bytes)
```

Simpan kunci dalam variabel lingkungan pada Linux atau macOS

Untuk mengkonversi ke base64 dan mengatur variabel lingkungan pada Linux ataumacOS, jalankan perintah berikut.

```
export C3R_SHARED_SECRET="$(cat secret.key | base64)"
```

Langkah 7: Enkripsi data

Untuk melakukan langkah ini, Anda harus memperoleh ID AWS Clean Rooms kolaborasi dan kunci rahasia bersama. Untuk informasi lebih lanjut, lihat Prasyarat.

Dalam contoh berikut, kita menjalankan enkripsi padaads.csv, menggunakan skema yang kita buat disebutads.json.

Untuk mengenkripsi data

1. Simpan kunci rahasia bersama untuk kolaborasi diLangkah 6: Simpan kunci rahasia bersama dalam variabel lingkungan.
2. Dari baris perintah, masukkan perintah berikut.

   ```
   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. Untuk<name of input .csv file>, masukkan nama file input .csv.
4. Untukschema=, masukkan nama file skema enkripsi .json.
5. Untukid=, masukkan ID kolaborasi.
6. Untukoutput=, masukkan nama file output (misalnya,ads-output.csv).

7. Sertakan salah satu bendera baris perintah yang dijelaskan dalam Parameter komputasi kriptografi danBendera opsional dalam Komputasi Kriptografi untuk Clean Rooms.
8. Jalankan perintah .

Dalam contoh untuk`ads.csv`, kita menjalankan perintah berikut.

java -jar c3r-cli.jar encrypt ***ads.csv*** --schema=***ads.json*** --id=***123e4567-e89b-42d3-a456-556642440000*** --output=***ads-output.csv***

Dalam contoh untuksales.csv, kita menjalankan perintah berikut.

java -jar c3r-cli.jar encrypt ***sales.csv*** --schema=***sales.json*** --id=***123e4567-e89b-42d3-a456-556642440000***

> **Note**
>
> Dalam contoh ini, kita tidak menentukan nama file output (`--output=`*`sales-output.csv`*). Akibatnya, nama file output default `name-of-file.out.csv` dihasilkan.

Anda sekarang siap untuk memverifikasi data terenkripsi.

Langkah 8: Verifikasi enkripsi data

Untuk memverifikasi bahwa data dienkripsi

1. Lihat file data terenkripsi (misalnya,`sales-output.csv`).
2. Verifikasi kolom berikut:
   a. Kolom 1 - Terenkripsi (misalnya,`username_fingerprint`).

      Untuk fingerprint kolom (HMAC), setelah awalan versi dan tipe (misalnya,`01:hmac:`), ada 44 karakter data yang disandikan base64.
   b. Kolom 2 - Tidak dienkripsi (misalnya,`purchased`).
   c. Kolom 3 - Terenkripsi (misalnya,`product_sealed`).

      Untuk kolom enkripsi (SELECT), panjang padding cleartext plus apa pun setelah awalan versi dan tipe (misalnya,`01:enc:`) berbanding lurus dengan panjang yang dienkripsi.

cleartext Artinya, panjang adalah ukuran input ditambah sekitar 33 persen overhead karena pengkodean.

Anda sekarang siap untuk:

1. Unggah data terenkripsi ke S3.
2. Buat AWS Glue tabel.
3. Buat tabel yang dikonfigurasi di AWS Clean Rooms.

Klien enkripsi C3R akan membuat file sementara yang tidak berisi data yang tidak terenkripsi (kecuali data itu juga tidak dienkripsi dalam output akhir). Namun, beberapa nilai terenkripsi mungkin tidak diempuk dengan benar. Kolom sidik jari mungkin berisi nilai duplikat, meskipun setelan `allowRepeatedFingerprintValue` kolaborasinya. `false` Masalah ini terjadi karena file sementara ditulis sebelum panjang padding yang tepat dan properti penghapusan duplikat diperiksa.

Jika klien enkripsi C3R gagal atau terputus selama enkripsi, mungkin berhenti setelah menulis file sementara tetapi sebelum memeriksa properti ini dan menghapus file sementara. Oleh karena itu, file-file sementara ini mungkin masih ada di disk. Jika ini masalahnya, konten dalam file-file ini tidak melindungi data plaintext ke tingkat yang sama dengan output. Secara khusus, file-file sementara ini mungkin mengungkapkan data teks biasa ke analisis statistik yang tidak akan bekerja melawan output akhir. Pengguna harus menghapus file-file ini (terutama SQLite database) untuk mencegah file-file ini jatuh ke tangan yang tidak sah.

(Opsional) Buat skema (pengguna tingkat lanjut)

Membuat skema secara manual adalah untuk pengguna tingkat lanjut.

Berikut ini adalah deskripsi format file skema JSON untuk file input dengan atau tanpa header kolom. Pengguna tingkat lanjut dapat langsung menulis atau memodifikasi skema jika diinginkan.

> **Note**
>
> Klien enkripsi C3R dapat membantu Anda dalam membuat skema melalui proses interaktif yang dijelaskan dalam Contoh: Menghasilkan skema enkripsi dengansealed,fingerprint, dan kolom cleartext atau melalui pembuatan templat rintisan.

Skema tabel yang dipetakan dan posisi

Bagian berikut menjelaskan dua jenis skema tabel:

- Skema tabel yang dipetakan - Skema ini digunakan untuk mengenkripsi file.csv dengan baris header dan file. Apache Parquet
- Skema tabel posisi - Skema ini digunakan untuk mengenkripsi file.csv tanpa baris header.

Klien enkripsi C3R dapat mengenkripsi file tabular untuk kolaborasi. Untuk melakukan ini, ia harus memiliki file skema yang sesuai yang menentukan bagaimana output terenkripsi harus diturunkan dari input.

Klien enkripsi C3R dapat membantu menghasilkan skema untuk `INPUT` file dengan menjalankan perintah skema klien enkripsi C3R di baris perintah. Contoh dari sebuah perintah adalah`java -jar c3r-cli.jar schema --interactive INPUT`.

Skema menentukan informasi berikut:

1. Kolom sumber mana yang memetakan kolom yang mengubah kolom dalam file output melalui nama tajuknya (skema yang dipetakan) atau posisi (skema posisi)
2. Kolom target mana yang akan tetap cleartext
3. Kolom target mana yang akan dienkripsi untuk kueri SELECT
4. Kolom target mana yang akan dienkripsi untuk kueri JOIN

Informasi ini dikodekan dalam file skema JSON khusus tabel, yang terdiri dari satu objek yang bidangnya `headerRow` adalah nilai Boolean. Nilai harus `true` untuk Parquet file dan file.csv dengan baris header, dan `false` sebaliknya.

Skema tabel yang dipetakan

Skema yang dipetakan memiliki bentuk sebagai berikut.

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": STRING,
      "targetHeader": STRING,
```

```
      "type": TYPE,
      "pad": PAD
    },
    ...
  ]
}
```

Jika `headerRow` yatrue, bidang berikutnya dalam objek adalah`columns`, yang berisi larik skema kolom yang memetakan header sumber ke header target (yaitu, objek JSON yang menjelaskan apa yang harus berisi kolom keluaran).

- `sourceHeader`— Nama `STRING` header dari kolom sumber tempat datanya berasal.

  > **Note**
  >
  > Kolom sumber yang sama dapat digunakan untuk beberapa kolom target.
  > Kolom dari file input yang tidak terdaftar sebagai di `sourceHeader` mana saja dalam skema tidak muncul di file output.

- `targetHeader`— Nama `STRING` header dari kolom yang sesuai dalam file output.

  > **Note**
  >
  > Bidang ini opsional untuk skema yang dipetakan. Jika bidang ini dihilangkan, `sourceHeader` digunakan kembali untuk nama header dalam output. Entah `_fingerprint` atau `_sealed` ditambahkan jika kolom output masing-masing adalah fingerprint kolom atau sealed kolom.

- `type`— Kolom target dalam file output. `TYPE` Yaitu, salah satu `cleartext`sealed, atau `fingerprint` tergantung pada bagaimana kolom akan digunakan dalam kolaborasi.
- `pad`- Bidang objek skema kolom yang hanya ada saat ada. `TYPE` `sealed` Nilai yang sesuai dari `PAD` adalah objek yang menggambarkan bagaimana data harus empuk sebelum dienkripsi.

  ```
  {
    "type": PAD_TYPE,
    "length": INT
  }
  ```

  Untuk menentukan padding pra-enkripsi, `type` dan `length` digunakan sebagai berikut:

- PAD_TYPEas none — Tidak ada padding yang akan diterapkan pada data kolom dan `length` bidang tidak berlaku (yaitu, dihilangkan).
- PAD_TYPEas `fixed` — Data kolom diempuk dengan byte `length` yang ditentukan.
- PAD_TYPEas `max` — Data kolom diempuk dengan ukuran panjang byte nilai terpanjang ditambah `length` byte tambahan.

Berikut ini adalah contoh skema yang dipetakan, dengan kolom masing-masing jenis.

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

Sebagai contoh yang lebih kompleks, berikut ini adalah contoh file.csv dengan header.

```
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
```

Dalam contoh skema dipetakan berikut, kolom `FirstName` dan `LastName` kolom. `cleartext` `State`Kolom dienkripsi sebagai `fingerprint` kolom dan sebagai `sealed` kolom dengan padding. `none` Kolom yang tersisa dihilangkan.

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

```
}
```

Berikut ini adalah file.csv yang dihasilkan dari skema yang dipetakan.

```
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=
```

Skema tabel posisi

Skema posisi memiliki bentuk sebagai berikut.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      },
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      }
    ],
    [],
    ...
  ]
```

```
}
```

Jika `headerRow` yafalse, bidang berikutnya dalam objek adalah`columns`, yang berisi array entri. Setiap entri itu sendiri merupakan larik skema kolom posisi nol atau lebih (tanpa `sourceHeader` bidang), yang merupakan objek JSON yang menjelaskan apa yang harus dikandung output.

- `sourceHeader`— Nama `STRING` header dari kolom sumber tempat datanya berasal.

  > **Note**
  >
  > Bidang ini harus dihilangkan dalam skema posisi. Dalam skema posisi, kolom sumber disimpulkan oleh indeks kolom yang sesuai dalam file skema.

- `targetHeader`— Nama `STRING` header dari kolom yang sesuai dalam file output.

  > **Note**
  >
  > Bidang ini diperlukan untuk skema posisi.

- `type`— Kolom target dalam file output. `TYPE` Yaitu, salah satu `cleartextsealed`, atau `fingerprint` tergantung pada bagaimana kolom akan digunakan dalam kolaborasi.
- `pad`- Bidang objek skema kolom yang hanya ada saat ada. `TYPE` `sealed` Nilai yang sesuai dari `PAD` adalah objek yang menggambarkan bagaimana data harus empuk sebelum dienkripsi.

  ```
  {
    "type": PAD_TYPE,
    "length": INT
  }
  ```

  Untuk menentukan padding pra-enkripsi, `type` dan `length` digunakan sebagai berikut:

  - `PAD_TYPE`as `none` — Tidak ada padding yang akan diterapkan pada data kolom dan `length` bidang tidak berlaku (yaitu, dihilangkan).
  - `PAD_TYPE`as `fixed` — Data kolom diempuk dengan byte `length` yang ditentukan.
  - `PAD_TYPE`as `max` — Data kolom diempuk dengan ukuran panjang byte nilai terpanjang ditambah `length` byte tambahan.

> **Note**
>
> `fixed`berguna jika Anda tahu sebelumnya batas atas pada ukuran byte data kolom. Kesalahan muncul jika ada data di kolom itu lebih panjang dari yang ditentukan`length`. `max`nyaman ketika ukuran yang tepat dari data input tidak diketahui karena berfungsi terlepas dari ukuran data. Namun, `max` membutuhkan waktu pemrosesan tambahan karena mengenkripsi data dua kali. `max`mengenkripsi data sekali saat dibaca ke file sementara dan sekali setelah entri data terpanjang di kolom diketahui.
> Juga, panjang nilai terpanjang tidak disimpan di antara pemanggilan klien. Jika Anda berencana untuk mengenkripsi data Anda dalam batch, atau mengenkripsi data baru secara berkala, ketahuilah bahwa panjang ciphertext yang dihasilkan dapat bervariasi antar batch.

Berikut ini adalah contoh skema posisi.

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

Sebagai contoh kompleks, berikut ini adalah contoh file.csv jika tidak memiliki baris pertama dengan header.

```
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
```

Skema posisi memiliki bentuk berikut.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": "GivenName",
        "type": "cleartext"
      }
    ],
    [
      {
        "targetHeader": "Surname",
        "type": "cleartext"
      }
    ],
    [],
    [],
```

```
    [
      {
        "targetHeader": "State_Join",
        "type": "fingerprint"
      },
      {
        "targetHeader": "State",
        "type": "sealed",
        "pad": {
          "type": "none"
        }
      }
    ],
    [],
    [],
    [],
    []
  ]
}
```

Skema sebelumnya menghasilkan file output berikut dengan baris header yang berisi header target yang ditentukan.

```
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=
```

Membuat tabel yang dikonfigurasi di AWS Clean Rooms

Tabel yang dikonfigurasi adalah referensi ke tabel yang ada di AWS Glue Data Catalog. Ini berisi aturan analisis yang menentukan bagaimana data dapat ditanyakan. AWS Clean Rooms Tabel yang dikonfigurasi dapat dikaitkan dengan satu atau lebih kolaborasi. Untuk informasi selengkapnya AWS Glue, lihat Panduan Pengembang AWS Glue.

Gunakan generasi statistik yang disediakan oleh AWS Glue untuk menghitung statistik tingkat kolom untuk tabel. AWS Glue Data Catalog Setelah AWS Glue menghasilkan statistik untuk tabel di Katalog Data, Amazon Redshift Spectrum secara otomatis menggunakan statistik tersebut untuk mengoptimalkan paket kueri. Untuk informasi selengkapnya tentang menggunakan statistik tingkat kolom komputasi AWS Glue, lihat Panduan Bekerja dengan statistik kolom.

Buat tabel yang dikonfigurasi

Pada langkah ini, Anda membuat tabel yang dikonfigurasi AWS Clean Rooms untuk digunakan dalam kolaborasi.

Untuk membuat tabel yang dikonfigurasi di AWS Clean Rooms

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.
3. Di sudut kanan atas, pilih Konfigurasi tabel baru.
4. Untuk Konfigurasi tabel baru, untuk Pilih AWS Glue tabel:
    a. Pilih Database yang ingin Anda konfigurasi dari daftar dropdown.
    b. Pilih Tabel yang ingin Anda konfigurasi dari daftar dropdown.

> **Note**
>
> Untuk memverifikasi bahwa ini adalah tabel yang benar, lakukan salah satu dari yang berikut:
>
> - Pilih Lihat di AWS Glue.
> - Aktifkan Lihat skema untuk melihat skema.

5. Untuk Kolom yang diizinkan dalam kolaborasi, pilih Semua kolom atau Daftar kustom.

Jika Anda memilih...	Lalu...
Semua kolom	Semua kolom diizinkan untuk digunakan di AWS Clean Rooms (tunduk pada aturan analisis).
Daftar kustom	Pilih satu atau beberapa kolom yang ingin Anda izinkan dari daftar tarik-turun Tentukan kolom yang diizinkan.

6. Untuk detail tabel yang Dikonfigurasi,

   a. Masukkan Nama untuk tabel yang dikonfigurasi.

      Anda dapat menggunakan nama default atau mengganti nama tabel ini.

   b. Masukkan Deskripsi tabel.

      Deskripsi membantu membedakan antara tabel lain yang dikonfigurasi dengan nama yang mirip.

   c. Jika Anda ingin mengaktifkan Tag untuk sumber daya tabel yang dikonfigurasi, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.

7. Pilih Konfigurasikan tabel baru.

Langkah selanjutnya

Sekarang setelah Anda membuat tabel yang dikonfigurasi, Anda siap untuk:

- Konfigurasikan aturan analisis ke tabel yang dikonfigurasi
- Kaitkan tabel yang dikonfigurasi ke kolaborasi

Mengonfigurasi aturan analisis ke tabel yang dikonfigurasi

Bagian berikut menjelaskan cara mengonfigurasi aturan analisis ke tabel yang dikonfigurasi. Dengan menentukan aturan analisis, Anda dapat mengotorisasi anggota yang dapat melakukan kueri untuk menjalankan kueri yang cocok dengan aturan analisis tertentu yang didukung oleh. AWS Clean Rooms

AWS Clean Roomsmendukung jenis aturan analisis berikut: agregasi, daftar, dan kustom.

Hanya ada satu aturan analisis per tabel yang dikonfigurasi.

> **Important**
>
> Jika Anda menggunakan Komputasi Kriptografi untuk Clean Rooms dan memiliki tabel data terenkripsi dalam kolaborasi, aturan analisis yang Anda tambahkan ke tabel terkonfigurasi terenkripsi harus konsisten dengan cara data dienkripsi. Misalnya, jika Anda mengenkripsi data untuk SELECT (aturan analisis agregasi), Anda tidak boleh menambahkan aturan analisis untuk JOIN (aturan analisis daftar).

Untuk mendapatkan pemahaman tentang jenis aturan analisis yang tersediaAWS Clean Rooms, lihatAturan analisis di AWS Clean Rooms.

Untuk informasi selengkapnya tentang aturan analisis agregasi, lihatAturan analisis agregasi.

Untuk informasi selengkapnya tentang aturan analisis daftar, lihatAturan analisis daftar.

Untuk informasi selengkapnya tentang aturan analisis kustom, lihatAturan analisis kustom di AWS Clean Rooms.

Setelah Anda meninjau dan memahami bagian ini, Anda dapat melakukan prosedur berikut:

Topik

Mengkonfigurasi aturan analisis agregasi ke tabel (aliran terpandu)

Aturan analisis agregasi memungkinkan kueri yang mengumpulkan statistik tanpa mengungkapkan informasi tingkat baris menggunakanCOUNT,SUM, dan berfungsi sepanjang dimensi opsional. AVG

Prosedur ini menjelaskan proses penambahan aturan analisis agregasi ke tabel yang dikonfigurasi dengan menggunakan opsi Aliran terpandu di AWS Clean Rooms konsol.

Untuk menambahkan aturan analisis agregasi ke tabel (aliran terpandu)

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.
3. Pilih tabel yang dikonfigurasi.
4. Pada halaman detail tabel yang dikonfigurasi, pilih Konfigurasi aturan analisis.
5. Di bawah Langkah 1: Pilih jenis, di bawah Jenis, biarkan opsi Agregasi dipilih secara default.
6. Di bawah Metode pembuatan, pilih Alur terpandu, lalu pilih Berikutnya.
7. Di bawah Langkah 2: Tentukan kontrol kueri, untuk fungsi Agregat:

    a. Pilih fungsi Agregat dari dropdown:

        - MENGHITUNG
        - HITUNG BERBEDA
        - SUM
        - JUMLAH BERBEDA
        - AVG

    b. Pilih kolom mana yang dapat digunakan dalam fungsi Agregat dari dropdown Kolom.

    c. (Opsional) Pilih Tambahkan fungsi lain untuk menambahkan fungsi agregat lain dan mengaitkan satu atau beberapa kolom ke fungsi itu.

    > **Note**
    >
    > Setidaknya diperlukan satu fungsi agregat.

    d. (Opsional) Pilih Hapus untuk menghapus fungsi agregat.
8. Untuk kontrol Gabung,

a. Pilih satu opsi untuk Izinkan tabel yang akan ditanyakan dengan sendirinya:

Jika Anda memilih...	Lalu...
Tidak, hanya tumpang tindih yang dapat ditanyakan	Tabel dapat ditanyakan hanya ketika bergabung ke tabel yang dimiliki oleh anggota yang dapat melakukan kueri.
Ya	Tabel dapat ditanyakan dengan sendirinya atau ketika bergabung ke tabel lain.

b. Di bawah Tentukan kolom gabungan, pilih kolom yang ingin Anda izinkan untuk digunakan dalam INNER JOIN pernyataan.

   Ini opsional jika Anda telah memilih Ya di langkah sebelumnya.

c. Di bawah Tentukan operator yang diizinkan untuk pencocokan, pilih operator mana, jika ada, yang dapat digunakan untuk pencocokan pada beberapa kolom gabungan. Jika Anda memilih dua atau lebih JOIN kolom, salah satu operator ini diperlukan.

Jika Anda memilih...	Lalu...
DAN	Anda dapat memasukkan `AND` dalam kondisi `INNER JOIN` pertandingan untuk menggabungkan satu kolom ke kolom lain di antara tabel.
ATAU	Anda dapat memasukkan `OR` dalam kondisi `INNER JOIN` kecocokan untuk menggabungkan beberapa kecocokan kolom antar tabel. Operator logis ini berguna untuk mendapatkan tingkat kecocokan yang lebih tinggi.

9. (Opsional) Untuk kontrol Dimensi, dalam menu tarik-turun Tentukan kolom dimensi, pilih kolom mana yang ingin Anda izinkan untuk digunakan dalam pernyataan SELECT, danWHERE, GROUPBY, dan ORDER BY bagian dari kueri.

> **Note**
>
> Fungsi agregat atau kolom gabungan tidak dapat digunakan sebagai kolom Dimensi.

10. Untuk fungsi Skalar, pilih satu opsi untuk Fungsi skalar mana yang ingin Anda izinkan?

Jika Anda memilih...	Lalu...
Semua saat ini didukung oleh AWS Clean Rooms	Anda mengizinkan semua fungsi skalar yang saat ini didukung olehAWS Clean Rooms. • Anda dapat memilih Lihat daftar untuk melihat seluruh daftar fungsi Skalar yang didukung. AWS Clean Rooms
Daftar kustom	Anda dapat menyesuaikan fungsi skalar mana yang akan diizinkan. • Pilih satu atau beberapa opsi dari menu tarik-turun Tentukan fungsi skalar yang diizinkan.
Tidak ada	Anda tidak ingin mengizinkan fungsi skalar apa pun.

Untuk informasi selengkapnya, lihat Fungsi skalar.

11. Pilih Berikutnya.
12. Di bawah Langkah 3: Tentukan kontrol hasil kueri, untuk kendala Agregasi:
    a. Pilih daftar dropdown untuk setiap nama Kolom.
    b. Pilih daftar dropdown untuk setiap Jumlah minimum nilai berbeda yang harus dipenuhi untuk setiap baris output yang akan dikembalikan, setelah COUNT DISTINCT fungsi diterapkan padanya.
    c. Pilih Tambahkan kendala untuk menambahkan lebih banyak batasan agregasi.
    d. (Opsional) Pilih Hapus untuk menghapus kendala agregasi.
13. Pilih Selanjutnya.

14. Di bawah Langkah 4: Tinjau dan konfigurasikan, tinjau pilihan yang telah Anda buat untuk langkah sebelumnya, edit jika perlu, lalu pilih Konfigurasi aturan analisis.

Anda melihat pesan konfirmasi bahwa Anda telah berhasil mengonfigurasi aturan analisis agregasi ke tabel.

Mengonfigurasi aturan analisis daftar ke tabel (alur terpandu)

Aturan analisis daftar memungkinkan kueri yang menampilkan daftar tingkat baris tumpang tindih antara tabel terkait dan tabel anggota yang dapat melakukan kueri.

Prosedur ini menjelaskan proses menambahkan aturan analisis daftar ke tabel yang dikonfigurasi menggunakan opsi Aliran terpandu di AWS Clean Rooms konsol.

Untuk menambahkan aturan analisis daftar ke tabel (alur terpandu)

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.
3. Pilih tabel yang dikonfigurasi.
4. Pada halaman detail tabel yang dikonfigurasi, pilih Konfigurasi aturan analisis.
5. Di bawah Langkah 1: Pilih jenis, di bawah Jenis, pilih Daftar pilihan.
6. Di bawah Metode pembuatan, pilih Alur terpandu, lalu pilih Berikutnya.
7. Di bawah Langkah 2: Tentukan kontrol kueri, untuk kontrol Gabung:

    a. Di bawah Tentukan kolom gabungan, pilih kolom yang ingin Anda izinkan untuk digunakan dalam INNER JOIN pernyataan.

    b. Di bawah Tentukan operator yang diizinkan untuk pencocokan, pilih operator mana, jika ada, yang dapat digunakan untuk pencocokan pada beberapa kolom gabungan. Jika Anda memilih dua atau lebih JOIN kolom, salah satu operator ini diperlukan.

Jika Anda memilih...	Lalu...
DAN	Anda dapat memasukkan `AND` dalam kondisi `INNER JOIN` pertandingan untuk

Jika Anda memilih...	Lalu...
	menggabungkan satu kolom ke kolom lain di antara tabel.
ATAU	Anda dapat memasukkan `OR` dalam kondisi `INNER JOIN` kecocokan untuk menggabungkan beberapa kecocokan kolom antar tabel. Operator logis ini berguna untuk mendapatkan tingkat kecocokan yang lebih tinggi.

8. (Opsional) Untuk kontrol Daftar, dalam menu tarik-turun Tentukan kolom daftar, pilih kolom mana yang ingin Anda izinkan untuk digunakan dalam output kueri (yaitu, digunakan dalam SELECT pernyataan), atau digunakan untuk memfilter hasil (yaitu, WHERE pernyataan).
9. Pilih Selanjutnya.
10. Di bawah Langkah 3: Tinjau dan konfigurasikan, tinjau pilihan yang telah Anda buat untuk langkah sebelumnya, edit jika perlu, lalu pilih Konfigurasi aturan analisis.

Anda melihat pesan konfirmasi bahwa Anda telah berhasil mengonfigurasi aturan analisis daftar untuk tabel.

Mengonfigurasi aturan analisis kustom ke tabel (alur terpandu)

Aturan analisis kustom memungkinkan kueri SQL kustom pada tabel yang dikonfigurasi. Aturan analisis khusus diperlukan jika menggunakan templat analisis atau privasi diferensial.

Prosedur ini menjelaskan proses penambahan aturan analisis kustom ke tabel yang dikonfigurasi menggunakan opsi Aliran terpandu di AWS Clean Rooms konsol.

Untuk menambahkan aturan analisis kustom ke tabel (alur terpandu)

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.
3. Pilih tabel yang dikonfigurasi.
4. Pada halaman detail tabel yang dikonfigurasi, pilih Konfigurasi aturan analisis.

5. Di bawah Langkah 1: Pilih jenis, di bawah Jenis, pilih Kustom pilihan.
6. Di bawah Metode pembuatan, pilih Alur terpandu, lalu pilih Berikutnya.
7. Di bawah Langkah 2: Tetapkan privasi diferensial, tentukan apakah Anda ingin privasi diferensial diaktifkan atau dimatikan. Privasi diferensial adalah teknik yang terbukti secara matematis untuk melindungi data Anda dari serangan identifikasi ulang.

   a. Untuk privasi Diferensial:

Jika kau...	Kemudian pilih...
Memiliki data tingkat pengguna dan Anda menginginkan perlindungan terhadap upaya identifikasi ulang	Nyalakan
Tidak memiliki data tingkat pengguna atau tidak memerlukan perlindungan terhadap upaya identifikasi ulang	Matikan

   b. Jika Anda memilih untuk Aktifkan privasi diferensial, pilih kolom Pengenal pengguna yang berisi pengenal unik pengguna Anda, seperti `user_id` kolom, yang privasinya ingin Anda lindungi. Jika Anda ingin mengaktifkan privasi diferensial untuk dua tabel atau lebih dalam kolaborasi, Anda harus mengonfigurasi kolom yang sama dengan kolom pengenal Pengguna di kedua aturan analisis untuk mempertahankan definisi pengguna yang konsisten di seluruh tabel. Jika terjadi kesalahan konfigurasi, anggota yang dapat melakukan kueri menerima pesan kesalahan bahwa ada dua kolom yang dapat dipilih untuk menghitung jumlah kontribusi pengguna (misalnya, jumlah tayangan iklan yang dibuat oleh pengguna) saat menjalankan kueri.
   c. Pilih Selanjutnya.
8. Di bawah Langkah 3: Tentukan kontrol kueri,

   a. Untuk tipe Kontrol:

Jika Anda ingin...	Kemudian pilih...
Tinjau setiap templat analisis baru sebelum dijalankan pada tabel yang dikonfigurasi	Tinjau setiap analisis baru sebelum diizinkan untuk dijalankan di tabel ini

Jika Anda ingin...	Kemudian pilih...
Biarkan template analisis atau kueri langsung dilakukan pada tabel yang dikonfigurasi	Izinkan kueri apa pun yang dibuat oleh kolaborator tertentu berjalan tanpa peninjauan pada tabel ini

b. Pilih salah satu dari berikut:

Jika Anda memilih...	Lalu...
Tinjau setiap analisis baru sebelum diizinkan untuk dijalankan di tabel ini	Di bawah Template analisis yang diizinkan untuk dijalankan, pilih Tambahkan templat analisis, lalu pilih Kolaborasi dan templat Analisis yang sesuai dari daftar tarik-turun.
Izinkan kueri apa pun yang dibuat oleh kolaborator tertentu berjalan tanpa peninjauan pada tabel ini	Di bawah Akun AWSdiizinkan untuk membuat kueri apa punAkun AWS, pilih Tambah, lalu pilih Akun AWSID yang sesuai.

9. Pilih Selanjutnya.
10. Di bawah Langkah 4: Tinjau dan konfigurasikan, tinjau pilihan yang telah Anda buat untuk langkah sebelumnya, edit jika perlu, lalu pilih Konfigurasi aturan analisis.

Anda melihat pesan konfirmasi bahwa Anda telah berhasil mengonfigurasi aturan analisis kustom untuk tabel.

Mengkonfigurasi aturan analisis ke tabel (editor JSON)

Prosedur berikut menunjukkan cara menambahkan aturan analisis ke tabel menggunakan opsi editor JSON di AWS Clean Rooms konsol.

Untuk mengonfigurasi agregasi, daftar, atau aturan analisis kustom ke tabel (editor JSON)

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.

3. Pilih tabel yang dikonfigurasi.
4. Pada halaman detail tabel yang dikonfigurasi, pilih Konfigurasi aturan analisis.
5. Di bawah Langkah 1: Pilih jenis, di bawah Jenis, pilih opsi Agregasi, Daftar, atau Kustom.
6. Di bawah Metode pembuatan, pilih editor JSON, lalu pilih Berikutnya.
7. Di bawah Langkah 2: Tentukan kontrol, Anda dapat memilih untuk menyisipkan struktur kueri (Sisipkan template) atau menyisipkan file (Impor dari file).

Jika Anda memilih...	Lalu...
Sisipkan templat	1. Tentukan parameter untuk aturan analisis yang dipilih dalam Definisi aturan analisis. 2. Anda dapat menekan Ctrl+Spacebar untuk mengaktifkan pelengkapan otomatis. Untuk informasi selengkapnya tentang parameter aturan analisis agregasi, lihatAturan analisis agregasi - kontrol kueri. Untuk informasi selengkapnya tentang parameter aturan analisis daftar, lihatAturan analisis daftar - kontrol kueri.
Impor dari file	1. Pilih file JSON Anda dari drive lokal Anda. 2. Pilih Buka . Definisi aturan Analisis menampilkan aturan analisis dari file yang diunggah.

8. Pilih Selanjutnya.
9. Di bawah Langkah 3: Tinjau dan konfigurasikan, tinjau pilihan yang telah Anda buat untuk langkah sebelumnya, edit jika perlu, lalu pilih Konfigurasi aturan analisis.

Anda menerima pesan konfirmasi bahwa Anda telah berhasil mengonfigurasi aturan analisis untuk tabel.

Langkah selanjutnya

Sekarang setelah Anda mengonfigurasi aturan analisis ke tabel yang dikonfigurasi, Anda siap untuk:

- Kaitkan tabel yang dikonfigurasi ke kolaborasi
- Kueri tabel data (sebagai anggota yang dapat melakukan kueri)

Mengaitkan tabel yang dikonfigurasi ke kolaborasi

Setelah Anda membuat tabel yang dikonfigurasi dan menambahkan aturan analisis ke dalamnya, Anda dapat mengaitkannya dengan kolaborasi.

Important

Sebelum Anda mengaitkan AWS Glue tabel yang dikonfigurasi ke kolaborasi, lokasi AWS Glue tabel harus mengarah ke folder Amazon Simple Storage Service (Amazon S3) dan bukan ke satu file. Anda dapat memverifikasi lokasi ini dengan melihat tabel di AWS Glue konsol di https://console.aws.amazon.com/glue/.

Note

Jika Anda telah mengonfigurasi enkripsi AWS Glue dan membuat peran layanan, Anda harus memberikan akses peran tersebut untuk digunakan AWS KMS keys untuk mendekripsi tabel AWS Glue .
Jika Anda mengaitkan tabel yang dikonfigurasi yang didukung oleh kumpulan data Amazon AWS KMS S3 yang dienkripsi, Anda harus memberikan akses peran untuk menggunakan kunci KMS untuk mendekripsi data Amazon S3.
Untuk informasi selengkapnya, lihat Menyiapkan enkripsi AWS Glue di Panduan AWS Glue Pengembang.

Topik berikut menjelaskan cara mengaitkan tabel yang dikonfigurasi ke kolaborasi menggunakan AWS Clean Rooms konsol:

Topik

Untuk informasi tentang cara mengaitkan tabel yang dikonfigurasi dengan kolaborasi menggunakan AWS SDK, lihat Referensi AWS Clean Rooms API.

Kaitkan tabel yang dikonfigurasi dari halaman detail tabel yang dikonfigurasi

Untuk mengaitkan AWS Glue tabel ke kolaborasi dari halaman detail tabel yang dikonfigurasi

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.
3. Pilih tabel yang dikonfigurasi.
4. Pada halaman detail tabel yang dikonfigurasi, pilih Kaitkan dengan kolaborasi.
5. Untuk kotak dialog Tabel asosiasi ke kolaborasi, pilih Kolaborasi dari daftar dropdown.
6. Pilih Pilih kolaborasi.

   Pada halaman tabel Associate, nama tabel yang dikonfigurasi yang Anda pilih muncul di bawah bagian Pilih tabel yang dikonfigurasi.
7. Untuk Pilih tabel yang dikonfigurasi, lakukan hal berikut:

Jika Anda ingin...	Lalu...
Konfigurasikan tabel baru	Pilih Konfigurasi tabel dan ikuti petunjuk pada halaman Konfigurasi tabel.
Lihat skema dan aturan analisis untuk tabel yang dikonfigurasi	Aktifkan Lihat skema dan aturan analisis.

8. Tentukan izin akses Layanan dengan memilih Buat dan gunakan peran layanan baru atau Gunakan peran layanan yang ada.

Jika Anda memilih...	Lalu...
Membuat dan menggunakan peran layanan baru	• AWS Clean Rooms membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah `cleanrooms-<timestamp>`

Jika Anda memilih...	Lalu...
	• Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, Anda dapat memilih Data ini dienkripsi dengan kunci KMS dan kemudian masukkan AWS KMS key yang akan digunakan untuk mendekripsi input data Anda.

Jika Anda memilih...	Lalu...
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun. Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk membuat daftar peran, Anda dapat memasukkan Nama Sumber Daya Amazon (ARN) peran yang ingin Anda gunakan. 2. Lihat peran layanan dengan memilih tautan eksternal Lihat di IAM. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. Secara default, AWS Clean Rooms tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan. 3. (Opsional) Pilih kotak centang Tambahkan kebijakan yang telah dikonfigurasi sebelumnya dengan izin yang diperlukan untuk peran ini untuk menambahkan izin lampiran yang diperlukan ke peran. Anda harus memiliki izin untuk mengubah peran dan membuat kebijakan.

> **Note**
>
> - AWS Clean Rooms memerlukan izin untuk melakukan kueri sesuai dengan aturan analisis. Untuk informasi selengkapnya tentang izin AWS Clean Rooms, lihatAWS kebijakan terkelola untuk AWS Clean Rooms.
> - Jika peran tidak memiliki izin yang memadai AWS Clean Rooms, Anda akan menerima pesan galat yang menyatakan bahwa peran tersebut tidak memiliki izin yang memadai untuk peran tersebut. AWS Clean Rooms Kebijakan peran harus ditambahkan sebelum melanjutkan.
> - Jika Anda tidak dapat mengubah kebijakan peran, Anda akan menerima pesan galat yang menyatakan bahwa tidak AWS Clean Rooms dapat menemukan kebijakan untuk peran layanan.

9. Jika Anda ingin mengaktifkan Tag untuk sumber daya asosiasi tabel yang dikonfigurasi, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.
10. Pilih tabel Associate.

Kaitkan tabel yang dikonfigurasi dari halaman detail kolaborasi

Untuk mengaitkan AWS Glue tabel ke kolaborasi dari halaman detail kolaborasi

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pada tab Tabel, pilih Tabel asosiasi.
5. Untuk Pilih tabel yang dikonfigurasi, lakukan hal berikut:

Jika Anda ingin...	Lalu...
Pilih tabel yang sudah dikonfigurasi	Pilih nama tabel Konfigurasi yang ingin Anda kaitkan dengan kolaborasi dari daftar dropdown.

Jika Anda ingin...	Lalu...
Konfigurasikan tabel baru	Pilih Konfigurasi tabel dan ikuti petunjuk pada halaman Konfigurasi tabel.
Lihat skema dan aturan analisis untuk tabel yang dikonfigurasi	Aktifkan Lihat skema dan aturan analisis.

6. Untuk detail asosiasi Tabel,

   a. Masukkan Nama untuk tabel terkait.

      Anda dapat menggunakan nama default atau mengganti nama tabel ini.

   b. (Opsional) Masukkan Deskripsi tabel.

      Deskripsi membantu menulis kueri.

7. Tentukan izin akses Layanan dengan memilih Buat dan gunakan peran layanan baru atau Gunakan peran layanan yang ada.

Jika Anda memilih...	Lalu...
Membuat dan menggunakan peran layanan baru	• AWS Clean Rooms membuat peran layanan dengan kebijakan yang diperlukan untuk tabel ini. • Nama peran Layanan default adalah`cleanrooms-<timestamp>` . • Anda harus memiliki izin untuk membuat peran dan melampirkan kebijakan. • Jika data input Anda dienkripsi, Anda dapat memilih Data ini dienkripsi dengan kunci KMS dan kemudian masukkan AWS KMS key yang akan digunakan untuk mendekripsi input data Anda.
Gunakan peran layanan yang ada	1. Pilih nama peran layanan yang ada dari daftar tarik-turun.

Jika Anda memilih...	Lalu...
	Daftar peran ditampilkan jika Anda memiliki izin untuk membuat daftar peran. Jika Anda tidak memiliki izin untuk membuat daftar peran, Anda dapat memasukkan Nama Sumber Daya Amazon (ARN) peran yang ingin Anda gunakan. 2. Lihat peran layanan dengan memilih tautan eksternal Lihat di IAM. Jika tidak ada peran layanan yang ada, opsi untuk Menggunakan peran layanan yang ada tidak tersedia. Secara default, AWS Clean Rooms tidak mencoba memperbarui kebijakan peran yang ada untuk menambahkan izin yang diperlukan. 3. (Opsional) Pilih kotak centang Tambahkan kebijakan yang telah dikonfigurasi sebelumnya dengan izin yang diperlukan untuk peran ini untuk menambahkan izin lampiran yang diperlukan ke peran. Anda harus memiliki izin untuk mengubah peran dan membuat kebijakan.

Note

- AWS Clean Rooms memerlukan izin untuk melakukan kueri sesuai dengan aturan analisis. Untuk informasi selengkapnya tentang izin AWS Clean Rooms, lihatAWS kebijakan terkelola untuk AWS Clean Rooms.

- Jika peran tidak memiliki izin yang memadai AWS Clean Rooms, Anda akan menerima pesan galat yang menyatakan bahwa peran tersebut tidak memiliki izin yang memadai untuk peran tersebut. AWS Clean Rooms Kebijakan peran harus ditambahkan sebelum melanjutkan.
- Jika Anda tidak dapat mengubah kebijakan peran, Anda akan menerima pesan galat yang menyatakan bahwa tidak AWS Clean Rooms dapat menemukan kebijakan untuk peran layanan.

8. Jika Anda ingin mengaktifkan Tag untuk sumber daya asosiasi tabel yang dikonfigurasi, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.
9. Pilih tabel Associate.

Langkah selanjutnya

Sekarang setelah Anda mengaitkan tabel data yang dikonfigurasi ke kolaborasi, Anda siap untuk:

- Edit kolaborasi, jika Anda pembuat kolaborasi
- Kueri tabel data (sebagai anggota yang dapat melakukan kueri)

Mengkonfigurasi kebijakan privasi diferensial

Prosedur ini menjelaskan proses konfigurasi kebijakan privasi diferensial dalam kolaborasi dengan menggunakan opsi Aliran terpandu di AWS Clean Rooms konsol. Ini adalah langkah satu kali untuk semua tabel dengan perlindungan privasi diferensial.

Untuk mengonfigurasi pengaturan privasi diferensial (aliran terpandu)

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pada tab Tabel di halaman kolaborasi, pilih Konfigurasi kebijakan privasi diferensial.
5. Pada halaman Konfigurasi kebijakan privasi diferensial, pilih nilai untuk properti berikut:

   - Anggaran privasi
   - Segarkan anggaran privasi setiap bulan
   - Kebisingan ditambahkan per kueri

   Anda dapat menggunakan nilai default atau memasukkan nilai khusus yang mendukung kasus penggunaan spesifik Anda. Setelah memilih nilai untuk anggaran Privasi dan Noise yang ditambahkan per kueri, Anda dapat melihat pratinjau utilitas yang dihasilkan dalam hal jumlah agregasi yang mungkin di semua kueri pada data Anda.
6. Pilih Konfigurasikan

Anda akan melihat pesan konfirmasi bahwa Anda telah berhasil mengonfigurasi kebijakan privasi diferensial untuk kolaborasi tersebut.

Langkah selanjutnya

Sekarang setelah Anda mengonfigurasi privasi diferensial, Anda siap untuk:

- Kueri tabel data (sebagai anggota yang dapat melakukan kueri)
- Kelola kolaborasi (jika Anda pembuat kolaborasi)

Bekerja dengan templat analisis

Template analisis bekerja dengan Aturan analisis kustom di AWS Clean Rooms. Dengan template analisis, Anda dapat menentukan parameter untuk membantu Anda menggunakan kembali kueri yang sama. AWS Clean Rooms mendukung subset parameterisasi dengan nilai literal.

Template analisis khusus untuk kolaborasi. Untuk setiap kolaborasi, anggota hanya dapat melihat kueri dalam kolaborasi tersebut. Jika Anda berencana untuk menggunakan privasi diferensial dalam sebuah kolaborasi, Anda harus memastikan bahwa templat analisis Anda kompatibel dengan struktur kueri tujuan umum Privasi Diferensial. AWS Clean Rooms

Topik

- Membuat template analisis
- Meninjau template analisis
- Kueri tabel yang dikonfigurasi menggunakan templat analisis

Membuat template analisis

Untuk informasi tentang cara membuat templat analisis menggunakan AWS SDK, lihat Referensi AWS Clean Rooms API.

Untuk membuat template analisis menggunakan AWS Clean Rooms konsol

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Akun AWS yang akan berfungsi sebagai pembuat kolaborasi.
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pada tab Template, buka bagian Analisis template yang dibuat oleh Anda.
5. Pilih Buat templat analisis.
6. Pada halaman template Buat analisis, untuk Detail, masukkan Nama dan Deskripsi opsional.
7. Untuk Tabel, lihat tabel yang dikonfigurasi terkait dengan kolaborasi.
8. Untuk Definisi,

    a. Masukkan definisi untuk templat analisis.

    b. Pilih Impor dari untuk mengimpor definisi.

c. (Opsional) Tentukan parameter di editor SQL dengan memasukkan titik dua (`:`) di depan nama parameter.

   Sebagai contoh:

   ```
   WHERE table1.date + :date_period > table1.date
   ```

9. Jika Anda menambahkan parameter sebelumnya, di bawah Parameter - opsional, untuk setiap nama Parameter, pilih nilai Jenis dan Default (opsional).
10. Jika Anda ingin mengaktifkan Tag untuk sumber daya tabel yang dikonfigurasikan, pilih Tambahkan tag baru lalu masukkan pasangan Kunci dan Nilai.
11. Pilih Buat.

Anda sekarang siap untuk:

- Beri tahu anggota kolaborasi Anda bahwa mereka dapat Meninjau templat analisis. (Opsional jika Anda ingin menanyakan data Anda sendiri.)

Meninjau template analisis

Setelah anggota kolaborasi membuat templat analisis, Anda dapat meninjau dan menyetujuinya. Setelah template analisis dan disetujui, itu bisa dalam kueri di AWS Clean Rooms.

Untuk meninjau template analisis menggunakan AWS Clean Rooms konsol

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Akun AWS yang akan berfungsi sebagai pembuat kolaborasi.
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pada tab Template, buka bagian Analisis template yang dibuat oleh anggota lain.
5. Pilih template analisis yang memiliki status Dapat menjalankan dari Tidak memerlukan ulasan Anda.
6. Pilih Tinjau.
7. Tinjau aturan analisis Ikhtisar, Definisi, dan Parameter (jika ada).
8. Tinjau tabel yang dikonfigurasi yang tercantum di bawah Tabel yang direferensikan dalam definisi.

Status di samping setiap tabel akan membaca Template tidak diperbolehkan.

9. Pilih meja.

Jika Anda	Kemudian pilih
Menyetujui template analisis	template di atas meja. Konfirmasikan persetujuan Anda dengan memilih.
Jangan menyetujui template analisis	Larang

Anda sekarang siap untuk menggunakan template analisis untuk query tabel data (sebagai anggota yang dapat query).

Kueri tabel yang dikonfigurasi menggunakan templat analisis

Prosedur ini menunjukkan cara menggunakan templat analisis di AWS Clean Rooms konsol untuk menanyakan tabel yang dikonfigurasi dengan aturan Analisis kustom.

Untuk menggunakan template analisis untuk menanyakan tabel yang dikonfigurasi dengan aturan Analisis kustom

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang memiliki status Kueri kemampuan anggota Anda.
4. Pada tab Kueri, di bawah Tabel, lihat tabel dan jenis aturan analisis terkait (Aturan analisis kustom).

> **Note**
>
> Jika Anda tidak melihat tabel yang Anda harapkan dalam daftar, mungkin karena alasan berikut:
>
> - Tabel belum dikaitkan.
> - Tabel tidak memiliki aturan analisis yang dikonfigurasi.

5. Di bawah bagian Analisis, pilih template analisis dari daftar dropdown.
6. Masukkan nilai parameter dari templat analisis yang ingin Anda gunakan dalam kueri. Nilai harus dalam tipe data parameter yang ditentukan. Anda dapat menggunakan nilai yang berbeda setiap kali Anda menjalankan template analisis. Kosong atau NULL nilai untuk parameter tidak didukung. Menggunakan parameter dalam LIMIT klausa juga tidak didukung.
7. Pilih Jalankan.

> **Note**
>
> Anda tidak dapat menjalankan kueri jika anggota yang dapat menerima hasil belum mengonfigurasi setelan hasil kueri.

8. Lanjutkan untuk menyesuaikan parameter dan jalankan kueri Anda lagi, atau pilih tombol + untuk memulai kueri baru di tab baru.

Kueri data dalam kolaborasi

Sebagai anggota yang dapat melakukan query, Anda dapat melakukan salah satu hal berikut:

- Buat kueri SQL secara manual menggunakan editor kode SQL.
- Gunakan UI pembuat Analisis untuk membuat kueri tanpa harus menulis kode SQL.
- Gunakan templat analisis yang disetujui.

Ketika anggota yang dapat melakukan kueri menjalankan kueri SQL pada tabel dalam kolaborasi, AWS Clean Rooms mengasumsikan peran yang relevan untuk mengakses tabel atas nama mereka. AWS Clean Rooms menerapkan aturan analisis yang diperlukan untuk kueri input dan outputnya.

AWS Clean Rooms mendukung query SQL yang dapat berbeda dari mesin query lainnya. Untuk spesifikasi, lihat Referensi AWS Clean Rooms SQL. Jika Anda ingin menjalankan kueri pada tabel data yang dilindungi dengan privasi diferensial, Anda harus memastikan bahwa kueri Anda kompatibel dengan struktur kueri tujuan umum Privasi Diferensial. AWS Clean Rooms

> **Note**
>
> Saat menggunakan Cryptographic Computing untuk Clean Rooms, tidak semua operasi SQL menghasilkan hasil yang valid. Misalnya, Anda dapat melakukan COUNT pada kolom terenkripsi tetapi melakukan nomor terenkripsi menyebabkan kesalahan. SUM Selain itu, kueri mungkin juga menghasilkan hasil yang salah. Misalnya, kueri yang SUM disegel kolom menghasilkan kesalahan. Namun, GROUP BY kueri di atas kolom yang disegel tampaknya berhasil tetapi menghasilkan grup yang berbeda dari yang dihasilkan oleh GROUP BY kueri di atas cleartext.

Topik berikut menjelaskan cara kueri data dalam kolaborasi menggunakan AWS Clean Rooms konsol.

Topik

- Melihat detail kueri

Untuk informasi tentang cara menanyakan data atau melihat kueri dengan memanggil operasi AWS Clean Rooms `StartProtectedQuery` API secara langsung atau menggunakan AWS SDK, lihat Referensi AWS Clean Rooms API.

Untuk informasi tentang pencatatan kueri, lihatKueri masuk AWS Clean Rooms.

> **Note**
>
> Jika Anda menjalankan kueri pada tabel data terenkripsi, hasil dari kolom terenkripsi dienkripsi.

Untuk informasi tentang menerima hasil kueri, lihatMenerima hasil kueri.

Menggunakan editor kode SQL

Sebagai anggota yang dapat melakukan kueri, Anda dapat membuat kueri secara manual dengan menulis kode SQL di editor kode SQL. Editor kode SQL terletak di bagian Analisis pada tab Kueri di konsol. AWS Clean Rooms

Editor kode SQL ditampilkan secara default. Jika Anda ingin menggunakan pembuat analisis untuk membuat kueri, lihatMenggunakan pembangun analisis.

> **Important**
>
> Jika Anda mulai menulis kueri SQL di editor kode dan kemudian mengaktifkan UI pembuat Analisis, kueri Anda tidak disimpan.

AWS Clean Rooms mendukung banyak perintah, fungsi, dan kondisi SQL. Untuk informasi selengkapnya, lihat Referensi AWS Clean Rooms SQL.

> **Tip**
>
> Jika pemeliharaan terjadwal terjadi saat kueri sedang berjalan, kueri dihentikan dan digulung kembali. Anda harus memulai ulang kueri.

Untuk membangun kueri secara manual menggunakan editor kode SQL

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang memiliki status Kueri kemampuan anggota Anda.
4. Pada tab Queries, buka bagian Analisis.

> **Note**
>
> Bagian Analisis hanya ditampilkan jika anggota yang dapat menerima hasil dan anggota yang bertanggung jawab untuk membayar biaya komputasi kueri telah bergabung dengan kolaborasi sebagai anggota aktif.

5. Pada tab Kueri, di bawah Tabel, lihat daftar tabel dan jenis aturan analisis terkait (Aturan analisis agregasi, Aturan analisis daftar, atau Aturan analisis kustom).

> **Note**
>
> Jika Anda tidak melihat tabel yang Anda harapkan dalam daftar, mungkin karena alasan berikut:
>
> - Tabel belum dikaitkan.
> - Tabel tidak memiliki aturan analisis yang dikonfigurasi.

6. (Opsional) Untuk melihat skema tabel dan kontrol aturan analisis, perluas tabel dengan memilih ikon tanda plus (+).
7. Bangun kueri dengan mengetikkan kueri ke editor kode SQL.

(Opsional) Jika Anda ingin menggunakan contoh kueri	(Opsional) Jika Anda ingin memasukkan nama kolom atau fungsi
1. Pilih tiga titik vertikal di sebelah tabel. 2. Di bawah Sisipkan di editor, pilih Contoh kueri.	1. Pilih tiga titik vertikal di sebelah kolom. 2. Di bawah Sisipkan di editor, pilih Nama kolom.

(Opsional) Jika Anda ingin menggunakan contoh kueri

> **Note**
>
> Memasukkan kueri Contoh menambahkan kueri yang sudah ada di editor.

Contoh kueri muncul. Semua tabel yang tercantum di bawah Tabel disertakan dalam kueri.

3. Edit nilai placeholder dalam kueri.

(Opsional) Jika Anda ingin memasukkan nama kolom atau fungsi

3. Untuk menyisipkan fungsi yang diizinkan secara manual pada kolom, pilih tiga titik vertikal di sebelah kolom, pilih Sisipkan di editor, lalu pilih nama fungsi yang diizinkan (sepertiINNER JOIN,SUM, SUMDISTINCT, atauCOUNT).
4. Tekan Ctrl+Spasi untuk melihat skema tabel di editor kode.

> **Note**
>
> Anggota yang dapat query dapat melihat dan menggunakan kolom partisi di setiap asosiasi tabel dikonfigurasi. Pastikan kolom partisi diberi label sebagai kolom partisi dalam tabel yang mendasari AWS Glue tabel yang dikonfigurasi.

5. Edit nilai placeholder dalam kueri.

8. Pilih Jalankan.

> **Note**
>
> Anda tidak dapat menjalankan kueri jika anggota yang dapat menerima hasil belum mengonfigurasi setelan hasil kueri.

9. Lanjutkan untuk menyesuaikan parameter dan jalankan kueri Anda lagi, atau pilih tombol + untuk memulai kueri baru di tab baru.

> **Note**
>
> AWS Clean Rooms bertujuan untuk memberikan pesan kesalahan yang jelas. Jika pesan kesalahan tidak memiliki detail yang cukup untuk membantu Anda memecahkan masalah, hubungi tim akun. Berikan mereka deskripsi tentang bagaimana kesalahan terjadi dan pesan kesalahan (termasuk pengidentifikasi apa pun). Untuk informasi selengkapnya, lihat Pemecahan masalah AWS Clean Rooms.

Menggunakan pembangun analisis

Anda dapat menggunakan pembuat analisis untuk membuat kueri tanpa harus menulis kode SQL. Dengan pembuat analisis, Anda dapat membuat kueri untuk kolaborasi yang memiliki:

- Tabel tunggal yang menggunakan aturan analisis agregasi tanpa diperlukan JOIN
- Dua tabel (satu dari setiap anggota) yang keduanya menggunakan aturan analisis agregasi
- Dua tabel (satu dari setiap anggota) yang keduanya menggunakan aturan analisis daftar
- Dua tabel (satu dari setiap anggota) yang keduanya menggunakan aturan analisis agregasi dan dua tabel (satu dari setiap anggota) yang keduanya menggunakan aturan analisis daftar

Jika Anda ingin menulis kueri SQL secara manual, lihat. Menggunakan editor kode SQL

Pembuat analisis muncul sebagai opsi UI pembuat Analisis di bagian Analisis pada tab Kueri di AWS Clean Rooms konsol.

> **Important**
>
> Jika Anda mengaktifkan UI pembuat Analisis, mulai membuat kueri di pembuat analisis, lalu matikan UI pembuat Analisis, kueri Anda tidak disimpan.

> **Tip**
>
> Jika pemeliharaan terjadwal terjadi saat kueri sedang berjalan, kueri dihentikan dan digulung kembali. Anda harus memulai ulang kueri.

Topik berikut menjelaskan cara menggunakan pembuat analisis.

Topik

Gunakan pembuat analisis untuk menanyakan satu tabel (agregasi)

Prosedur ini menunjukkan cara menggunakan UI pembuat Analisis di AWS Clean Rooms konsol untuk membuat kueri. Kueri adalah untuk kolaborasi yang memiliki satu tabel yang menggunakan aturan analisis agregasi tanpa JOIN diperlukan.

Untuk menggunakan pembuat analisis untuk menanyakan satu tabel

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang memiliki status Kueri kemampuan anggota Anda.
4. Pada tab Kueri, di bawah Tabel, lihat tabel dan jenis aturan analisis terkait. (Jenis aturan analisis harus menjadi aturan analisis Agregasi.)

   > **Note**
   >
   > Jika Anda tidak melihat tabel yang Anda harapkan, mungkin karena alasan berikut:

- Tabel belum dikaitkan.
- Tabel tidak memiliki aturan analisis yang dikonfigurasi.

5. Di bawah bagian Analisis, aktifkan UI pembuat Analisis.
6. Bangun kueri.

   Jika Anda ingin melihat semua metrik agregasi, lewati ke langkah 9.

   a. Untuk metrik Pilih, tinjau metrik agregat yang telah dipilih sebelumnya secara default dan hapus metrik apa pun jika diperlukan.

   b. (Opsional) Untuk Tambah segmen - opsional, pilih satu atau beberapa parameter.

   > **Note**
   >
   > Tambahkan segmen - opsional hanya ditampilkan jika dimensi ditentukan untuk tabel.

   c. (Opsional) Untuk Tambahkan filter — opsional, pilih Tambahkan filter, lalu pilih Parameter, operator, dan Nilai.

   Untuk menambahkan lebih banyak filter, pilih Tambahkan filter lain.

   Untuk menghapus filter, pilih Hapus.

   > **Note**
   >
   > ORDER BYtidak didukung untuk kueri agregasi.
   > Hanya AND operator yang didukung dalam filter.

   d. (Opsional) Untuk Tambahkan deskripsi — opsional, masukkan deskripsi untuk membantu mengidentifikasi kueri dalam daftar kueri.

7. Perluas kode SQL Pratinjau.

   a. Lihat kode SQL yang dihasilkan dari pembuat analisis.

   b. Untuk menyalin kode SQL, pilih Salin.

   c. Untuk mengedit kode SQL, pilih Edit di editor kode SQL.

8. Pilih Jalankan.

> **Note**
>
> Anda tidak dapat menjalankan kueri jika anggota yang dapat menerima hasil belum mengonfigurasi setelan hasil kueri.

9. Lanjutkan untuk menyesuaikan parameter dan jalankan kueri Anda lagi, atau pilih tombol + untuk memulai kueri baru di tab baru.

> **Note**
>
> AWS Clean Rooms bertujuan untuk memberikan pesan kesalahan yang jelas. Jika pesan kesalahan tidak memiliki detail yang cukup untuk membantu Anda memecahkan masalah, hubungi tim akun. Berikan mereka deskripsi tentang bagaimana kesalahan terjadi dan pesan kesalahan (termasuk pengidentifikasi apa pun). Untuk informasi selengkapnya, lihat Pemecahan masalah AWS Clean Rooms.

Gunakan pembuat analisis untuk menanyakan dua tabel (agregasi atau daftar)

Prosedur ini menjelaskan cara menggunakan pembuat analisis di AWS Clean Rooms konsol untuk membuat kueri untuk kolaborasi yang memiliki:

- Dua tabel (satu dari setiap anggota) yang keduanya menggunakan aturan analisis agregasi
- Dua tabel (satu dari setiap anggota) yang keduanya menggunakan aturan analisis daftar
- Dua tabel (satu dari setiap anggota) yang keduanya menggunakan aturan analisis agregasi dan dua tabel (satu dari setiap anggota) yang keduanya menggunakan aturan analisis daftar

Untuk menggunakan pembuat analisis untuk menanyakan dua tabel

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang memiliki status kemampuan anggota Anda Query..

4. Pada tab Kueri, di bawah Tabel, lihat dua tabel dan jenis aturan analisis terkait (Aturan analisis agregasi atau Aturan analisis daftar).

> **Note**
>
> Jika Anda tidak melihat tabel yang Anda harapkan dalam daftar, mungkin karena alasan berikut:
>
> - Tabel belum dikaitkan.
> - Tabel tidak memiliki aturan analisis yang dikonfigurasi.

5. Di bawah bagian Analisis, aktifkan UI pembuat Analisis.
6. Bangun kueri.

Jika kolaborasi berisi dua tabel yang menggunakan aturan analisis agregasi dan dua tabel yang menggunakan aturan analisis Daftar, pertama pilih Agregasi atau Daftar, lalu ikuti petunjuk berdasarkan aturan analisis yang dipilih.

Jika kedua tabel menggunakan aturan analisis agregasi	Jika kedua tabel menggunakan aturan analisis daftar
1. Untuk metrik Pilih, tinjau metrik agregat yang telah dipilih sebelumnya secara default dan hapus metrik apa pun jika diperlukan. 2. Untuk catatan Pertandingan, pilih satu atau beberapa catatan. **Note** Saat menggunakan pembuat analisis, Anda hanya dapat mencocokkan pada satu pasang kolom.	1. Untuk atribut Pilih, tinjau atribut daftar yang telah dipilih sebelumnya secara default dan hapus metrik apa pun jika diperlukan. 2. Untuk catatan Pertandingan, pilih satu atau beberapa catatan. **Note** Saat menggunakan pembuat analisis, Anda hanya dapat mencocokkan pada satu pasang kolom.

Jika kedua tabel menggunakan aturan analisis agregasi	Jika kedua tabel menggunakan aturan analisis daftar
3. (Opsional) Untuk Tambah segmen - opsional, pilih satu atau beberapa parameter. **Note** Tambahkan segmen - opsional hanya ditampilkan jika dimensi ditentukan untuk tabel.	3. (Opsional) Untuk Tambahkan filter — opsional, pilih Tambahkan filter, lalu pilih parameter, operator, dan nilai. Untuk menambahkan lebih banyak filter, pilih Tambahkan filter lain. Untuk menghapus filter, pilih Hapus. **Note** LIMITtidak didukung untuk kueri daftar. Hanya AND operator yang didukung dalam filter.
4. (Opsional) Untuk Tambahkan filter — opsional, pilih Tambahkan filter, lalu pilih parameter, operator, dan nilai. Untuk menambahkan lebih banyak filter, pilih Tambahkan filter lain. Untuk menghapus filter, pilih Hapus. **Note** ORDER BYtidak didukung untuk kueri agregasi. Hanya AND operator yang didukung dalam filter.	4. (Opsional) Untuk Tambahkan deskripsi — opsional, masukkan deskripsi untuk membantu mengidentifikasi kueri dalam daftar kueri terbaru.
5. (Opsional) Untuk Tambahkan deskripsi — opsional, masukkan deskripsi untuk	

Jika kedua tabel menggunakan aturan analisis agregasi	Jika kedua tabel menggunakan aturan analisis daftar
membantu mengidentifikasi kueri dalam daftar kueri terbaru.	

7. Perluas kode SQL Pratinjau.

   a. Lihat kode SQL yang dihasilkan dari pembuat analisis.

   b. Untuk menyalin kode SQL, pilih Salin.

   c. Untuk mengedit kode SQL, pilih Edit di editor kode SQL.

8. Pilih Jalankan.

> **Note**
>
> Anda tidak dapat menjalankan kueri jika anggota yang dapat menerima hasil belum mengonfigurasi setelan hasil kueri

9. Lanjutkan untuk menyesuaikan parameter dan jalankan kueri Anda lagi, atau pilih tombol + untuk memulai kueri baru di tab baru.

> **Note**
>
> AWS Clean Rooms bertujuan untuk memberikan pesan kesalahan yang jelas. Jika pesan kesalahan tidak memiliki detail yang cukup untuk membantu Anda memecahkan masalah, hubungi tim akun. Berikan mereka deskripsi tentang bagaimana kesalahan terjadi dan pesan kesalahan (termasuk pengidentifikasi apa pun). Untuk informasi selengkapnya, lihat Pemecahan masalah AWS Clean Rooms.

Meminta data dengan privasi diferensial

Secara umum, menulis dan menjalankan kueri tidak berubah ketika privasi diferensial diaktifkan. Namun, Anda tidak dapat menjalankan kueri jika tidak ada cukup anggaran privasi yang tersisa. Saat Anda menjalankan kueri dan menggunakan anggaran privasi, Anda dapat melihat kira-kira berapa banyak agregasi yang dapat Anda jalankan dan bagaimana hal itu dapat memengaruhi kueri future.

Untuk melihat dampak privasi diferensial dalam kolaborasi

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang memiliki status detail anggota Anda dari Jalankan kueri.
4. Pada tab Kueri, di bawah Tabel, lihat anggaran privasi yang tersisa. Ini ditampilkan sebagai perkiraan jumlah fungsi agregasi yang tersisa dan Utilitas yang digunakan (diberikan sebagai persentase).

   > **Note**
   >
   > Perkiraan jumlah fungsi agregat yang tersisa dan persentase Utilitas yang digunakan hanya ditampilkan untuk anggota yang dapat melakukan query.

5. Pilih Lihat dampak untuk melihat seberapa banyak noise yang disuntikkan ke hasil dan kira-kira berapa banyak fungsi agregasi yang dapat Anda jalankan.

Melihat kueri terbaru

Anda dapat melihat kueri yang berjalan dalam 90 hari terakhir di tab Kueri terbaru.

> **Note**
>
> Jika satu-satunya kemampuan anggota Anda adalah Kontribusikan data, dan Anda bukan anggota yang membayar biaya komputasi kueri, tab Kueri tidak akan muncul di konsol.

Untuk melihat pertanyaan terbaru

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pada tab Kueri, di bawah Kueri, lihat kueri yang telah dijalankan dalam 90 hari terakhir.

5. Untuk mengurutkan kueri terbaru berdasarkan Status, pilih status dari daftar tarik-turun Semua status.

   Statusnya adalah: Dikirim, Dimulai, Dibatalkan, Sukses, Gagal, dan Timed out.

Melihat detail kueri

Anda dapat melihat detail kueri sebagai anggota yang dapat menjalankan kueri atau sebagai anggota yang dapat menerima hasil.

Untuk melihat detail kueri

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pada tab Queries, lakukan salah satu hal berikut:
   - Pilih tombol opsi untuk kueri tertentu yang ingin Anda lihat, lalu pilih Lihat detail.
   - Pilih ID kueri yang dilindungi.
5. Pada halaman Query details,
   - Jika Anda adalah anggota yang dapat menjalankan kueri, lihat detail Kueri, teks SQL, dan Hasil.

     Anda melihat pesan yang mengonfirmasi bahwa hasil kueri dikirimkan ke anggota yang dapat menerima hasil.
   - Jika Anda adalah anggota yang dapat menerima hasil, lihat detail Kueri dan Hasil.

Menerima hasil kueri

Sebagaianggota yang dapat menerima hasil, Anda dapat menerima output kueri dariAWS Clean Roomske bucket Amazon S3 yang Anda tetapkan saat Anda bergabung dengan kolaborasi.

Topik berikut ini menjelaskan cara menerima hasil query menggunakanAWS Clean Roomskonsol.

Topik

- Terima hasil kueri
- Edit nilai default untuk pengaturan hasil kueri
- Menggunakan output kueri di lainLayanan AWS

Untuk informasi tentang cara menanyakan data atau melihat kueri dengan memanggilAWS Clean RoomsAPI secara langsung atau dengan menggunakanAWSSDK, lihatAWS Clean RoomsReferensi API.

Untuk informasi tentang pencatatan kueri, lihatKueri masuk AWS Clean Rooms.

> **Note**
>
> Jika Anda menjalankan kueri pada tabel data terenkripsi, hasil dari kolom terenkripsi dienkripsi.

Terima hasil kueri

Hasil dari query ini terletak diPengaturan hasil kueri secara defaultbagian danPertanyaanbagian dariPertanyaantab diAWS Clean Roomskonsol.

Untuk menerima hasil kueri

1. Masuk keAWS Management Consoledan bukaAWS Clean Roomskonsoldengan AndaAkun AWS(jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilihKolaborasi.
3. Pilih kolaborasi yang memilikiKemampuan anggota Andastatus dariMenerima hasil.

4. Untuk menerima hasil kueri langsung dariAWS Clean Rooms, padaPertanyaantab, di bawahPertanyaan, di bawahID kueri yang dilindungikolom, pilih kueri.
5. PadaDetail kuerihalaman, di bawahHasil, lakukan salah satu dari yang berikut:

Jika Anda ingin...	Kemudian pilih...
Salin hasilnya.	Salin
Unduh hasilnya.	Unduh **Note** Secara default, nama file yang diunduh adalah yang sesuai`Query id`yang ditampilkan saat kueri dijalankanAWS Clean Rooms.
Lihat hasilnya di Amazon S3.	Lihat di Amazon S3 Konsol Amazon S3 terbuka di tab terpisah.

6. Jika Anda menggunakan data terenkripsi, Anda sekarang dapatmendekripsitabel data.

   Untuk informasi selengkapnya, lihat Mendekripsi tabel data dengan klien enkripsi C3R.

Edit nilai default untuk pengaturan hasil kueri

Sebagai anggota yang dapat menerima hasil, Anda dapat mengedit nilai default untuk pengaturan hasil kueri diAWS Clean Roomskonsol.

Untuk mengedit nilai default untuk pengaturan hasil kueri

1. Masuk keAWS Management Consoledan bukaAWS Clean Roomskonsoldengan AndaAkun AWS(jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilihKolaborasi.

3. Pilih kolaborasi yang memilikiKemampuan anggota Andastatus dariMenerima hasil.
4. PadaPertanyaantab, di bawahPengaturan hasil kueri, pilihSunting.
5. PadaEdit setelan hasil kueri defaulthalaman, memodifikasi salah satu dari berikut ini, sesuai kebutuhan:

   a. Di bawahPengaturan hasil kueri, memodifikasiTujuan hasil di Amazon S3atauFormat hasil.
   b. Di bawahAkses layanan, memodifikasiMetode untuk mengotorisasiAWS Clean Roomsuntuk menulis ke bucket Amazon S3 yang Anda tetapkan.

   Yang diperbaruiPengaturan hasil kuerimuncul di halaman detail kolaborasi.

Menggunakan output kueri di lainLayanan AWS

Output kueri dariAWS Clean Roomstersedia di konsol (jika konsol digunakan untuk menjalankan kueri) dan diunduh di bucket Amazon S3 tertentu. Dari sana, Anda dapat menggunakan output kueri diLayanan AWS, seperti Amazon QuickSight dan Amazon SageMaker, tergantung pada bagaimana layanan ini menggunakan data dari Amazon S3.

Untuk informasi lebih lanjut tentang Amazon QuickSight, lihatAmazon QuickSightDokumentasi.

Untuk informasi lebih lanjut tentang Amazon SageMaker, lihatAmazon SageMakerDokumentasi.

Mendekripsi tabel data dengan klien enkripsi C3R

Ikuti prosedur ini untuk kolaborasi yang menggunakan Cryptographic Computing untukClean Roomsdan klien enkripsi C3R untuk mengenkripsi tabel data. Gunakan prosedur ini setelah Anda memilikidata yang ditanyakan dalam kolaborasi.

Kunci rahasia bersama dan ID kolaborasi diperlukan untuk prosedur ini.

Anggota yang dapat menerima hasil mendekripsi data menggunakan kunci rahasia bersama dan ID kolaborasi yang sama yang digunakan untuk mengenkripsi data untuk kolaborasi.

> **Note**
>
> AWS Clean Roomskolaborasi sudah membatasi siapa yang dapat melakukan dan melihat hasil kueri. Untuk melakukan dekripsi, siapa pun yang memiliki akses ke hasil ini memerlukan kunci rahasia bersama dan ID kolaborasi yang sama yang digunakan untuk mengenkripsi data.

Untuk mendekripsi tabel data terenkripsi

1. (Opsional)Lihat perintah yang tersedia di klien enkripsi C3R.
2. (Opsional) Arahkan ke direktori yang diinginkan dan jalankan`ls`(macOS) atau`dir`(Windows).
   - Verifikasi bahwac3r-cli.jarfile dan file data hasil kueri terenkripsi berada di direktori yang diinginkan.

     > **Note**
     >
     > Jika hasil kueri diunduh dariAWS Clean Roomsantarmuka konsol, kemungkinan besar ada diUnduhanfolder untuk akun pengguna Anda. (Misalnya,Unduhanfolder di direktori pengguna Anda padaWindowsdanmacOS.) Kami menyarankan Anda memindahkan file hasil kueri ke folder yang sama denganc3r-cli.jar.
3. Simpan kunci rahasia bersama di`C3R_SHARED_SECRET`variabel lingkungan. Untuk informasi selengkapnya, lihat Langkah 6: Simpan kunci rahasia bersama dalam variabel lingkungan.
4. DariAWS Command Line Interface(AWS CLI), jalankan perintah berikut.

java -jar c3r-cli.jar decrypt ***<name of input .csv file>*** --id=***<collaboration id>*** --output=***<output file name>***

5. Ganti masing-masing*placeholder masukan pengguna*Dengan informasi Anda sendiri:

   a. Untuk`id=`, masukkan ID kolaborasi.

   b. Untuk`output=`, masukkan nama file output (misalnya,`results-decrypted.csv`).

      Jika Anda tidak menentukan nama output, nama default akan dideskripsikan di terminal.

   c. Lihat data yang didekripsi dalam file keluaran yang ditentukan menggunakan CSV pilihan Anda atauParquetmelihat aplikasi (sepertiMicrosoft Excel, editor teks, atau aplikasi lain).

Mengelola AWS Clean Rooms

Topik berikut menjelaskan cara mengelola kolaborasi, anggota, dan tabel yang dikonfigurasi dalam AWS Clean Rooms menggunakan AWS Clean Rooms konsol.

Untuk informasi tentang cara mengelola AWS Clean Rooms menggunakan AWS SDK, lihat Referensi AWS Clean Rooms API.

Topik

Mengelola kolaborasi di AWS Clean Rooms

Topik berikut menjelaskan bagaimana pembuat kolaborasi dapat mengelola kolaborasi dalam AWS Clean Rooms menggunakan AWS Clean Rooms konsol.

Untuk informasi tentang cara mengelola kolaborasi menggunakan AWS SDK, lihat Referensi AWS Clean Rooms API.

Topik

Mengedit kolaborasi

Pelajari cara mengedit bagian kolaborasi yang berbeda.

Topik

Edit nama dan deskripsi kolaborasi

Setelah Anda membuat kolaborasi, Anda hanya dapat mengedit nama dan deskripsi kolaborasi.

> **Note**
>
> Jika Anda telah mengaktifkan Pencatatan kueri, Anda dapat mengedit apakah log kueri disimpan di akun Amazon CloudWatch Logs Anda.

Untuk mengedit nama dan deskripsi kolaborasi

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang Anda buat.
4. Pada halaman detail kolaborasi, pilih Tindakan, lalu pilih Edit kolaborasi.
5. Untuk Detail, edit Nama dan Deskripsi kolaborasi.
6. Pilih Simpan perubahan.

Edit tag kolaborasi

Sebagai pembuat kolaborasi, setelah Anda membuat kolaborasi, Anda dapat mengelola tag pada sumber kolaborasi.

Untuk mengedit tag kolaborasi

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang Anda buat.
4. Pilih salah satu dari berikut:

Jika Anda...	Lalu...
Anggota kolaborasi	Pilih tab Detail.
Pencipta kolaborasi tetapi bukan anggota kolaborasi	Gulir ke bawah halaman ke bagian Tag.

5. Untuk detail Kolaborasi, pilih Kelola tag.
6. Pada halaman Kelola tag, Anda dapat melakukan hal berikut:
   - Untuk menghapus sebuah tag, pilih Hapus.
   - Untuk menambahkan tanda, pilih Tambahkan tanda baru.
   - Untuk menyimpan perubahan, pilih Simpan perubahan

Edit tag keanggotaan

Sebagai pembuat kolaborasi, setelah Anda membuat kolaborasi, Anda dapat mengelola tag pada sumber daya keanggotaan.

Untuk mengedit tag keanggotaan

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang Anda buat.
4. Pilih tab Detail.
5. Untuk detail Keanggotaan, pilih Kelola tag.
6. Pada halaman Kelola tag keanggotaan, Anda dapat melakukan hal berikut:

- Untuk menghapus sebuah tag, pilih Hapus.
- Untuk menambahkan tanda, pilih Tambahkan tanda baru.
- Untuk menyimpan perubahan Anda, memilih Simpan perubahan.

Mengedit tag tabel terkait

Sebagai pembuat kolaborasi, setelah Anda mengaitkan tabel ke kolaborasi, Anda dapat mengelola tag pada sumber daya tabel terkait.

Untuk mengedit tag tabel terkait

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang Anda buat.
4. Pilih tab Tabel.
5. Untuk Tabel yang terkait dengan Anda, pilih tabel.
6. Pada halaman detail tabel yang dikonfigurasi, untuk Tag, pilih Kelola tag.

   Pada halaman Kelola tag, Anda dapat melakukan hal berikut:

   - Untuk menghapus sebuah tag, pilih Hapus.
   - Untuk menambahkan tanda, pilih Tambahkan tanda baru.
   - Untuk menyimpan perubahan Anda, memilih Simpan perubahan.

Edit tag templat analisis

Sebagai pembuat kolaborasi, setelah Anda membuat kolaborasi, Anda dapat mengelola tag pada sumber daya templat analisis.

Untuk mengedit tag keanggotaan

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.

3. Pilih kolaborasi yang Anda buat.
4. Pilih tab Template.
5. Pada bagian Template Analisis yang dibuat oleh Anda, pilih templat analisis.
6. Pada halaman detail tabel templat analisis, gulir ke bawah ke bagian Tag.
7. Pilih Kelola tanda.
8. Pada halaman Kelola tag, Anda dapat melakukan hal berikut:
   - Untuk menghapus sebuah tag, pilih Hapus.
   - Untuk menambahkan tanda, pilih Tambahkan tanda baru.
   - Untuk menyimpan perubahan Anda, memilih Simpan perubahan.

Edit tag kebijakan privasi diferensial

Sebagai pembuat kolaborasi, setelah Anda membuat kolaborasi, Anda dapat mengelola tag pada sumber daya templat analisis.

Untuk mengedit tag keanggotaan

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang berisi kebijakan privasi diferensial yang ingin Anda edit.
4. Pilih tab Tabel.
5. Pada tab Tabel, pilih Kelola tag.
6. Pada halaman Kelola tag, Anda dapat melakukan hal berikut:
   - Untuk menghapus sebuah tag, pilih Hapus.
   - Untuk menambahkan tanda, pilih Tambahkan tanda baru.
   - Untuk menyimpan perubahan Anda, memilih Simpan perubahan.

Menghapus kolaborasi

Sebagai pembuat kolaborasi, Anda dapat menghapus kolaborasi yang Anda buat.

> **Note**
>
> Saat menghapus kolaborasi, Anda dan semua anggota tidak dapat menjalankan kueri, menerima hasil, atau menyumbangkan data. Setiap anggota kolaborasi terus memiliki akses ke data mereka sendiri sebagai bagian dari keanggotaan mereka.

Untuk menghapus kolaborasi

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang ingin Anda hapus.
4. Di bawah Tindakan, pilih Hapus kolaborasi.
5. Konfirmasikan penghapusan dan kemudian pilih Hapus.

Melihat kolaborasi

Sebagai pembuat kolaborasi, Anda dapat melihat semua kolaborasi yang Anda buat.

Untuk melihat kolaborasi

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pada halaman Kolaborasi, di bawah Terakhir digunakan, lihat 5 kolaborasi terakhir yang digunakan.
4. Pada tab Dengan keanggotaan aktif, lihat daftar Kolaborasi dengan keanggotaan aktif.

   Anda dapat mengurutkan berdasarkan Nama, tanggal yang dibuat Keanggotaan, dan rincian anggota Anda.

   Anda dapat menggunakan bilah Pencarian untuk mencari kolaborasi.
5. Pada tab Tersedia untuk bergabung, lihat daftar Kolaborasi yang tersedia untuk bergabung.
6. Pada tab Tidak lagi tersedia, lihat daftar kolaborasi yang dihapus dan Keanggotaan untuk kolaborasi yang tidak lagi tersedia (keanggotaan dihapus).

Melihat tabel dan aturan analisis

Untuk melihat tabel yang terkait dengan kolaborasi dan aturan analisis

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pilih tab Tabel.
5. Pilih salah satu dari berikut:
    a. Untuk melihat tabel yang terkait dalam kolaborasi, untuk Tabel yang terkait dengan Anda, pilih tabel (teks biru).
    b. Untuk melihat tabel lain yang terkait dalam kolaborasi, untuk Tabel yang terkait dengan kolaborator, pilih tabel (teks biru).
6. Lihat detail tabel dan aturan analisis pada halaman detail tabel.

Melihat log penggunaan privasi diferensial

Sebagai anggota kolaborasi yang melindungi data dengan privasi diferensial, setelah Anda membuat kolaborasi dengan privasi diferensial, Anda dapat memantau penggunaan anggaran privasi.

Untuk melihat berapa banyak agregasi yang dijalankan dan berapa banyak anggaran privasi yang digunakan

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pilih tab Tabel.
5. Pilih Lihat log penggunaan (teks biru).
6. Lihat detail penggunaan, termasuk anggaran privasi dan berapa banyak utilitas yang disediakan.

Memantau status anggota

Sebagai pembuat kolaborasi, setelah Anda membuat kolaborasi, Anda dapat memantau status semua anggota di tab Anggota.

Untuk memeriksa status anggota

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang Anda buat.
4. Pilih tab Anggota.
5. Lihat status Anggota masing-masing anggota.

Menghapus anggota dari kolaborasi

> **Note**
>
> Menghapus anggota juga menghapus semua kumpulan data terkait dari kolaborasi.

Untuk menghapus anggota dari kolaborasi

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi yang Anda buat.
4. Pilih tab Anggota.
5. Pilih tombol opsi di sebelah anggota yang akan dihapus.

   > **Note**
   >
   > Pembuat kolaborasi tidak dapat memilih ID akun mereka sendiri.

6. Pilih Hapus.

7. Di kotak dialog, konfirmasikan keputusan untuk menghapus anggota dengan mengetikkan **`confirm`** bidang input teks.

> **Note**
>
> Jika Anda menghapus anggota yang membayar biaya komputasi kueri, tidak ada lagi kueri yang diizinkan untuk dijalankan dalam kolaborasi.

Meninggalkan Kolaborasi

Sebagai anggota kolaborasi, Anda dapat meninggalkan kolaborasi dengan menghapus keanggotaan Anda. Jika Anda adalah pembuat kolaborasi, Anda hanya dapat meninggalkan kolaborasi dengan menghapus kolaborasi.

> **Note**
>
> Ketika Anda menghapus keanggotaan Anda, Anda meninggalkan kolaborasi dan tidak dapat bergabung kembali. Jika Anda adalah anggota yang membayar biaya komputasi kueri dan Anda menghapus keanggotaan Anda, tidak ada lagi kueri yang diizinkan untuk dijalankan.

Untuk meninggalkan kolaborasi

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Untuk Dengan keanggotaan aktif, pilih kolaborasi di mana Anda menjadi anggota.
4. Pilih Tindakan.
5. Pilih Hapus keanggotaan.
6. Di kotak dialog, konfirmasikan keputusan untuk meninggalkan kolaborasi dengan mengetikkan **`confirm`** bidang input teks, lalu pilih Kosong dan hapus keanggotaan.

   Anda melihat pesan di konsol yang menunjukkan bahwa keanggotaan telah dihapus.

   Pembuat kolaborasi melihat status Anggota sebagai Kiri.

Mengedit asosiasi tabel yang dikonfigurasi

Sebagai anggota kolaborasi, Anda dapat mengedit asosiasi tabel yang telah dikonfigurasi yang telah Anda buat.

Untuk mengedit asosiasi tabel yang dikonfigurasi

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pilih tab Tabel.
5. Untuk Tabel yang terkait dengan Anda, pilih tabel.
6. Pada halaman detail tabel, gulir ke bawah untuk melihat detail asosiasi Tabel.
7. Pilih Edit.
8. Pada halaman Edit asosiasi tabel yang dikonfigurasi, perbarui Deskripsi atau informasi akses Layanan.
9. Pilih Simpan perubahan.

Memutuskan tabel yang dikonfigurasi

Sebagai anggota kolaborasi, Anda dapat memisahkan tabel yang dikonfigurasi dari kolaborasi. Tindakan ini mencegah anggota yang dapat melakukan kueri dari menanyakan tabel.

Untuk memisahkan tabel yang dikonfigurasi

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pilih tab Tabel.
5. Untuk Tabel yang terkait dengan Anda, pilih tombol opsi di sebelah tabel yang ingin Anda pisahkan.
6. Pilih Pisahkan.

7. Di kotak dialog, konfirmasikan keputusan untuk memisahkan tabel yang dikonfigurasi dan mencegah anggota yang dapat melakukan kueri untuk menanyakan tabel dengan memilih Disassociate.

Mengedit kebijakan privasi diferensial

Kapan saja setelah mengonfigurasi kebijakan privasi diferensial, Anda dapat memperbaruinya untuk lebih mencerminkan kebutuhan privasi Anda.

Untuk mengedit kebijakan privasi diferensial

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pada tab Tabel pada halaman kolaborasi, di bawah Tabel yang terkait dengan Anda, pilih Edit.
5. Pada halaman Edit privasi diferensial, pilih nilai baru untuk properti berikut:

   - Anggaran privasi - Pindahkan bilah geser untuk menambah atau mengurangi anggaran kapan saja selama kolaborasi. Anda tidak dapat mengurangi anggaran setelah anggota yang dapat melakukan kueri telah mulai menanyakan data Anda. Jika anggaran Privasi meningkat, AWS Clean Rooms akan terus menggunakan anggaran yang ada sampai sepenuhnya dikonsumsi sebelum memanfaatkan anggaran privasi yang baru ditambahkan.
   - Noise ditambahkan per kueri - Pindahkan bilah penggeser untuk menambah atau mengurangi Noise yang ditambahkan per kueri kapan saja selama kolaborasi.

   > **Note**
   >
   > Anda dapat memilih contoh Interaktif untuk mengeksplorasi bagaimana nilai yang berbeda dari anggaran Privasi dan Kebisingan yang ditambahkan per kueri memengaruhi jumlah fungsi agregat yang dapat Anda jalankan.

   Anda tidak dapat mengubah nilai penyegaran anggaran Privasi. Untuk mengubah pilihan Anda, Anda harus menghapus kebijakan privasi diferensial dan membuat yang baru.
6. Pilih Simpan perubahan.

Anda melihat pesan konfirmasi bahwa Anda telah berhasil mengedit kebijakan privasi diferensial.

Menghapus kebijakan privasi diferensial

Anda dapat menghapus kebijakan privasi diferensial dari tab Tabel kolaborasi.

Untuk menghapus kebijakan privasi diferensial

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pada tab Tabel pada halaman kolaborasi, di samping Kebijakan privasi diferensial, pilih Hapus.
5. Jika Anda yakin ingin menghapus kebijakan privasi diferensial, pilih Hapus.

Setelah menghapus kebijakan privasi diferensial, Anda tidak dapat mengakses log penggunaan anggaran privasi dari kebijakan tersebut. Tabel dengan privasi diferensial diaktifkan tidak dapat ditanyakan jika kebijakan privasi diferensial dihapus.

Melihat parameter privasi diferensial yang dihitung

Untuk pengguna yang memiliki keahlian dalam privasi diferensial, Anda dapat melihat parameter privasi diferensial yang dihitung dari tab Kueri kolaborasi.

Untuk melihat parameter privasi diferensial yang dihitung

1. Masuk ke AWS Management Console dan buka AWS Clean Roomskonsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Kolaborasi.
3. Pilih kolaborasi.
4. Pada tab Kueri, di bagian Hasil, pilih Lihat parameter privasi diferensial yang dihitung.

Dalam tabel parameter privasi diferensial terhitung, Anda dapat melihat nilai sensitivitas fungsi agregat, yang didefinisikan sebagai jumlah maksimum yang dapat mengubah hasil fungsi jika catatan pengguna tunggal ditambahkan, dihapus, atau dimodifikasi. Daftar ini mencakup parameter privasi diferensial berikut:

- Batas kontribusi pengguna (UCL) adalah jumlah maksimum baris yang disumbangkan oleh pengguna dalam kueri SQL. Misalnya, jika Anda ingin menghitung jumlah tayangan yang cocok dalam kampanye tertentu di mana setiap pengguna dapat memiliki beberapa tayangan, Privasi AWS Clean Rooms Diferensial harus mengikat jumlah tayangan satu pengguna untuk memastikan bahwa perhitungan privasi diferensial akurat. Dengan kata lain, jika ada pengguna yang memiliki lebih banyak tayangan daripada terikat, maka AWS Clean Rooms secara otomatis mengambil sampel acak seragam dari tayangan pengguna tersebut sesuai nilai UCL yang dihitung dan mengecualikan tayangan yang tersisa dari pengguna tersebut saat menjalankan kueri. Nilai UCL sama dengan 1 jika Anda menghitung jumlah pengguna unik. Ini karena menambahkan, menghapus, atau memodifikasi satu pengguna dapat mengubah jumlah pengguna yang berbeda paling banyak 1.
- Nilai minimum adalah batas bawah ekspresi yang digunakan dalam fungsi agregat seperti`sum()`. Misalnya, jika ekspresi adalah kolom yang dikenal sebagai`purchase_value`, nilai minimum adalah batas bawah kolom.
- Nilai maksimum adalah batas atas ekspresi yang digunakan dalam fungsi agregat seperti`sum()`. Misalnya, jika ekspresi adalah kolom yang dikenal sebagai`purchase_value`, nilai maksimum adalah batas atas kolom.

Dalam tabel parameter privasi diferensial terhitung, Anda dapat menggunakan parameter ini untuk lebih memahami jumlah total noise dalam hasil kueri. Misalnya, ketika Noise yang dikonfigurasi yang ditambahkan per kueri adalah 30 pengguna dan `COUNT DISTINCT (user_id)` kueri dijalankan, maka Privasi AWS Clean Rooms Diferensial menambahkan noise acak yang jatuh antara -30 dan 30 dengan probabilitas tinggi karena sensitivitas `COUNT DISTINCT` adalah 1. Dalam kasus `COUNT` kueri dengan konfigurasi yang sama, Privasi AWS Clean Rooms Diferensial menambahkan noise statistik yang diskalakan oleh batas kontribusi pengguna karena satu pengguna dapat menyumbangkan beberapa baris ke hasil kueri. Dalam kasus `SUM` kueri seperti `SUM (purchase_value)` di mana semua nilai kolom positif, total noise diskalakan oleh batas kontribusi pengguna dikalikan nilai maksimum. AWS Clean Rooms Privasi Diferensial secara otomatis menghitung parameter sensitivitas untuk melakukan penambahan noise pada waktu proses kueri dan menghabiskan anggaran privasi. Penipisan anggaran privasi diperlukan karena parameter sensitivitas bergantung pada data.

Mengelola tabel yang dikonfigurasi di AWS Clean Rooms

Topik berikut menjelaskan cara mengelola tabel yang dikonfigurasi dalam AWS Clean Rooms menggunakan AWS Clean Rooms konsol.

Untuk informasi tentang cara mengelola tabel yang dikonfigurasi menggunakan AWS SDK, lihat Referensi AWS Clean Rooms API.

Topik

Mengedit detail tabel yang dikonfigurasi

Sebagai anggota kolaborasi, Anda dapat mengedit detail tabel yang dikonfigurasi.

Untuk mengedit detail tabel yang dikonfigurasi

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.
3. Pilih tabel yang dikonfigurasi yang Anda buat.
4. Pada halaman detail tabel yang dikonfigurasi, gulir ke bawah ke detail tabel yang dikonfigurasi.
5. Pilih Edit.
6. Perbarui Nama atau Deskripsi tabel yang dikonfigurasi.
7. Pilih Simpan perubahan.

Mengedit tag tabel yang dikonfigurasi

Sebagai anggota kolaborasi, setelah Anda membuat tabel yang dikonfigurasi, Anda dapat mengelola tag pada sumber daya tabel yang dikonfigurasi pada tab Tabel yang dikonfigurasi.

Untuk mengedit tag tabel yang dikonfigurasi

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.
3. Pilih tabel yang dikonfigurasi yang Anda buat.

4. Pada halaman detail tabel yang dikonfigurasi, gulir ke bawah ke bagian Tag.
5. Pilih Kelola tanda.
6. Pada halaman Kelola tag, Anda dapat melakukan hal berikut:
   - Untuk menghapus sebuah tag, pilih Hapus.
   - Untuk menambahkan tanda, pilih Tambahkan tanda baru.
   - Untuk menyimpan perubahan Anda, memilih Simpan perubahan.

Mengedit aturan analisis tabel yang dikonfigurasi

Untuk mengedit aturan analisis tabel yang dikonfigurasi

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.
3. Pilih tabel yang dikonfigurasi yang Anda buat.
4. Pada halaman detail tabel yang dikonfigurasi, gulir ke bawah ke salah satu aturan analisis agregasi, aturan analisis daftar, atau bagian Aturan analisis kustom. (Pilihan Anda tergantung pada jenis aturan analisis yang Anda pilih untuk tabel yang dikonfigurasi.)
5. Pilih Edit.
6. Pada halaman aturan Edit analisis, Anda dapat:
   - Ubah definisi aturan Analisis dengan:
     - Memodifikasi editor JSON.
     - Memilih Impor dari file untuk mengunggah definisi aturan analisis baru.
   - Pratinjau apa yang akan dilihat anggota dalam kolaborasi dengan memilih dari opsi berikut:
     - Tampilan tabel
     - JSON
     - Contoh kueri
7. Pilih Simpan perubahan untuk menyimpan perubahan Anda.

Menghapus aturan analisis tabel yang dikonfigurasi

> **Warning**
>
> Tindakan ini tidak dapat dibatalkan dan berdampak pada semua sumber daya terkait.

Untuk menghapus aturan analisis tabel yang dikonfigurasi

1. Masuk ke AWS Management Console dan buka AWS Clean Rooms konsol dengan Anda Akun AWS (jika Anda belum melakukannya).
2. Di panel navigasi kiri, pilih Tabel yang dikonfigurasi.
3. Pilih tabel yang dikonfigurasi yang Anda buat.
4. Pada halaman detail tabel yang dikonfigurasi, gulir ke bawah ke salah satu aturan analisis agregasi, aturan analisis daftar, atau bagian Aturan analisis kustom. (Pilihan Anda tergantung pada jenis aturan analisis yang Anda pilih untuk tabel yang dikonfigurasi.)
5. Pilih Hapus.
6. Jika Anda yakin ingin menghapus aturan analisis, pilih Hapus.

Pemecahan masalah AWS Clean Rooms

Bagian ini menjelaskan beberapa masalah umum yang mungkin timbul saat menggunakan AWS Clean Rooms dan cara memperbaikinya.

Masalah

- Satu atau beberapa tabel yang direferensikan oleh kueri tidak dapat diakses oleh peran layanan terkait. Pemilik tabel/peran harus memberikan akses peran layanan ke tabel.
- Salah satu kumpulan data yang mendasarinya memiliki format file yang tidak didukung.
- Hasil kueri tidak seperti yang diharapkan saat menggunakan Cryptographic Computing untukClean Rooms.

Satu atau beberapa tabel yang direferensikan oleh kueri tidak dapat diakses oleh peran layanan terkait. Pemilik tabel/peran harus memberikan akses peran layanan ke tabel.

- Verifikasi bahwa izin untuk peran layanan disiapkan sesuai kebutuhan. Untuk informasi lebih lanjut, lihatMenyiapkan AWS Clean Rooms.

Salah satu kumpulan data yang mendasarinya memiliki format file yang tidak didukung.

- Pastikan kumpulan data Anda berada dalam salah satu format file yang didukung:
  - Parquet
  - RCFile
  - TextFile
  - SequenceFile
  - RegexSerde
  - OpenCSV
  - AVRO
  - JSON

Untuk informasi selengkapnya, lihat Format data untuk AWS Clean Rooms.

Hasil kueri tidak seperti yang diharapkan saat menggunakan Cryptographic Computing untukClean Rooms.

Jika Anda menggunakan Cryptographic Computing for Clean Rooms (C3R), verifikasi bahwa kueri Anda menggunakan kolom terenkripsi dengan benar:

- sealedKolom hanya digunakan dalam SELECT klausa.
- fingerprintKolom hanya digunakan dalam JOIN klausa (dan GROUP BY klausa dalam kondisi tertentu).
- Bahwa Anda hanya JOINing fingerprint kolom dengan nama yang sama jika pengaturan kolaborasi memerlukannya.

Lihat informasi yang lebih lengkap di Komputasi kriptografi dan the section called “Jenis kolom”.

Keamanan di AWS Clean Rooms

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Clean Rooms, lihat AWS Services in Scope by Compliance Program .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup kepekaan data Anda, persyaratan perusahaan, serta peraturan perundangan yang berlaku

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Clean Rooms. Ini menunjukkan kepada Anda cara mengonfigurasi AWS Clean Rooms untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan AWS Clean Rooms sumber daya Anda.

Daftar Isi

Perlindungan data di AWS Clean Rooms

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Clean Rooms. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan logging aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS Clean Rooms atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat

menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi diam

AWS Clean Rooms selalu mengenkripsi semua metadata layanan saat istirahat tanpa memerlukan konfigurasi tambahan apa pun. Enkripsi ini otomatis saat Anda menggunakannya AWS Clean Rooms.

Clean Rooms ML mengenkripsi semua data yang disimpan dalam layanan saat istirahat. AWS KMS Jika Anda memilih untuk memberikan kunci KMS Anda sendiri, konten model mirip Anda dan pekerjaan pembuatan segmen yang mirip dienkripsi saat istirahat dengan kunci KMS Anda.

> **Note**
>
> Anda dapat menggunakan opsi enkripsi di Amazon S3 untuk melindungi data Anda saat istirahat.
> Untuk informasi selengkapnya, lihat Menentukan enkripsi Amazon S3 di Panduan Pengguna Amazon S3.

Enkripsi bergerak

AWS Clean Rooms menggunakan Transport Layer Security (TLS) dan enkripsi sisi klien untuk enkripsi dalam perjalanan. Komunikasi dengan selalu AWS Clean Rooms dilakukan melalui HTTPS sehingga data Anda selalu dienkripsi saat transit. Ini termasuk semua data dalam perjalanan saat menggunakan Clean Rooms ML.

Mengenkripsi data yang mendasarinya

Untuk informasi selengkapnya tentang cara mengenkripsi data dasar Anda, lihatKomputasi Kriptografi untuk Clean Rooms.

Retensi data di AWS Clean Rooms

Saat Anda membuat model yang mirip, Clean Rooms MLakan membaca data pelatihan Anda, mengubahnya menjadi format yang sesuai untuk model ML kami, dan menyimpan parameter model terlatih di dalam Clean Rooms. Clean Rooms ML tidak menyimpan salinan data pelatihan Anda.

AWS Clean Rooms Kueri SQL tidak menyimpan data Anda setelah kueri berjalan. Clean Rooms MS kemudian menggunakan model terlatih untuk meringkas perilaku semua pengguna Anda. Clean Rooms ML menyimpan kumpulan data tingkat pengguna untuk setiap pengguna dalam data Anda selama model mirip Anda aktif.

Saat Anda memulai pekerjaan pembuatan segmen yang mirip, Clean Rooms MLakan membaca data seed, membaca ringkasan perilaku dari model mirip mirip terkait, dan membuat segmen mirip yang disimpan dalam layanan. AWS Clean Rooms Clean Rooms ML tidak menyimpan salinan data benih Anda. Clean Rooms ML menyimpan output tingkat pengguna dari pekerjaan selama pekerjaan itu aktif.

Jika Anda ingin menghapus model yang mirip atau data pekerjaan pembuatan segmen yang mirip, gunakan API untuk menghapusnya. Clean Rooms MS secara asinkron menghapus semua data yang terkait dengan model atau pekerjaan. Setelah proses ini selesai, Clean Rooms MLmenghapus metadata untuk model atau pekerjaan dan tidak lagi terlihat di API. Clean Rooms MS menyimpan data yang dihapus selama 3 hari untuk pencegahan pemulihan bencana. Setelah pekerjaan atau model tidak lagi terlihat di API dan 3 hari berlalu, semua data yang terkait dengan model atau pekerjaan telah dihapus secara permanen.

Praktik terbaik untuk kolaborasi data di AWS Clean Rooms

Topik ini menjelaskan praktik terbaik untuk melakukan kolaborasi data di AWS Clean Rooms.

AWS Clean Rooms mengikuti Model Tanggung Jawab AWS Bersama. AWS Clean Rooms menawarkan aturan analisis yang dapat Anda konfigurasikan untuk memperkuat kemampuan Anda untuk melindungi data sensitif dalam kolaborasi. Aturan analisis yang Anda konfigurasikan AWS Clean Rooms akan memberlakukan pembatasan (kontrol kueri dan kontrol keluaran kueri) yang telah Anda konfigurasikan. Anda bertanggung jawab untuk menentukan batasan dan mengonfigurasi aturan analisis yang sesuai.

Kolaborasi data mungkin melibatkan lebih dari sekedar penggunaan AWS Clean Rooms Anda. Untuk membantu Anda memaksimalkan manfaat kolaborasi data, kami menyarankan Anda melakukan praktik terbaik berikut dengan penggunaan Anda AWS Clean Rooms dan secara khusus dengan aturan analisis.

Topik

- Praktik terbaik dengan AWS Clean Rooms
- Praktik terbaik untuk menggunakan aturan analisis di AWS Clean Rooms

Praktik terbaik dengan AWS Clean Rooms

Anda bertanggung jawab untuk menilai risiko setiap kolaborasi data dan membandingkannya dengan persyaratan privasi Anda seperti program dan kebijakan kepatuhan eksternal dan internal. Kami menyarankan Anda mengambil tindakan tambahan dengan penggunaan Anda AWS Clean Rooms. Tindakan ini dapat membantu mengelola risiko lebih lanjut dan membantu mencegah upaya pihak ketiga untuk mengidentifikasi kembali data Anda (misalnya, serangan yang berbeda atau serangan saluran samping).

Misalnya, pertimbangkan untuk melakukan uji tuntas pada kolaborator Anda yang lain dan buat perjanjian hukum dengan mereka sebelum terlibat dalam kolaborasi. Untuk memantau penggunaan data Anda, pertimbangkan juga untuk mengadopsi mekanisme audit lain dengan penggunaan AWS Clean Rooms Anda.

Praktik terbaik untuk menggunakan aturan analisis di AWS Clean Rooms

Aturan analisis AWS Clean Rooms memungkinkan Anda membatasi kueri yang dapat dijalankan dengan menyetel kontrol kueri pada tabel yang dikonfigurasi. Misalnya, Anda dapat mengatur kontrol kueri untuk bagaimana tabel yang dikonfigurasi dapat digabungkan dan kolom mana yang dapat dipilih. Anda juga dapat membatasi output kueri melalui pengaturan kontrol hasil kueri seperti ambang agregasi pada baris keluaran. Layanan menolak kueri apa pun dan menghapus baris yang tidak sesuai dengan aturan analisis yang ditetapkan oleh anggota pada tabel yang dikonfigurasi dalam kueri.

Kami merekomendasikan 10 praktik terbaik berikut untuk menggunakan aturan analisis pada tabel yang dikonfigurasi:

- Buat tabel terkonfigurasi terpisah untuk kasus penggunaan kueri terpisah (misalnya, perencanaan audiens atau atribusi). Anda dapat membuat beberapa tabel yang dikonfigurasi dengan AWS Glue tabel dasar yang sama.
- Tentukan kolom dalam aturan analisis (misalnya, kolom dimensi, kolom daftar, kolom gabungan) yang diperlukan untuk kueri dalam kolaborasi. Ini dapat membantu mengurangi risiko serangan yang berbeda atau memungkinkan anggota lain untuk merekayasa balik data Anda. Gunakan fitur kolom allowlist untuk mencatat kolom lain yang mungkin ingin Anda jadikan queryable di masa mendatang. Untuk menyesuaikan kolom yang dapat digunakan untuk kolaborasi tertentu, buat tabel tambahan yang dikonfigurasi dengan AWS Glue tabel dasar yang sama.
- Tentukan fungsi dalam aturan analisis yang diperlukan untuk analisis dalam kolaborasi. Ini dapat membantu mengurangi risiko dari kesalahan fungsi langka yang dapat menyajikan informasi pada

titik data individu. Untuk menyesuaikan fungsi yang dapat digunakan untuk kolaborasi tertentu, buat tabel tambahan yang dikonfigurasi dengan AWS Glue tabel dasar yang sama.

- Tambahkan batasan agregasi pada kolom mana pun yang nilainya pada tingkat baris sensitif. Ini termasuk kolom dalam tabel yang dikonfigurasi yang juga ada di tabel anggota kolaborasi lainnya dan aturan analisis sebagai kendala agregasi. Ini juga mencakup kolom dalam tabel yang dikonfigurasi yang tidak dapat dikueri, yaitu kolom yang ada di tabel yang dikonfigurasi tetapi tidak ada dalam aturan analisis. Kendala agregasi dapat membantu mengurangi risiko dari mengkorelasikan hasil kueri dengan data di luar kolaborasi.
- Buat kolaborasi pengujian dan aturan analisis untuk menguji batasan yang dibuat dengan aturan analisis yang ditentukan.
- Tinjau tabel yang dikonfigurasi kolaborator dan aturan analisis anggota pada tabel yang dikonfigurasi untuk memeriksa apakah mereka cocok dengan apa yang disepakati untuk kolaborasi. Ini dapat membantu mengurangi risiko dari anggota lain yang merekayasa data mereka sendiri untuk menjalankan kueri yang tidak disepakati.
- Tinjau contoh kueri yang disediakan (khusus konsol) yang diaktifkan pada tabel yang dikonfigurasi setelah Anda mengatur aturan analisis.

> **Note**
>
> Selain kueri contoh yang disediakan, kueri lain dimungkinkan berdasarkan aturan analisis dan tabel anggota kolaborasi lainnya serta aturan analisis.

- Anda dapat menambahkan atau memperbarui aturan analisis untuk tabel yang dikonfigurasi dalam kolaborasi. Ketika Anda melakukannya, tinjau semua kolaborasi yang terkait dengan tabel yang dikonfigurasi dan dampaknya. Ini membantu memastikan bahwa tidak ada kolaborasi yang menggunakan aturan analisis usang.
- Tinjau kueri yang dijalankan dalam kolaborasi untuk memeriksa apakah kueri cocok dengan kasus penggunaan atau kueri yang disepakati untuk kolaborasi. (Kueri tersedia di log kueri saat fitur Pencatatan kueri diaktifkan.) Ini dapat membantu mengurangi risiko dari anggota yang menjalankan analisis yang tidak disepakati dan potensi serangan seperti serangan saluran samping.
- Tinjau kolom tabel yang dikonfigurasi yang digunakan dalam aturan analisis anggota kolaborasi dan dalam kueri untuk memeriksa apakah mereka cocok dengan apa yang disepakati dalam kolaborasi. (Kueri tersedia di log kueri saat fitur itu diaktifkan.) Ini dapat membantu mengurangi risiko dari anggota lain yang merekayasa data mereka sendiri untuk melakukan pertanyaan yang tidak disepakati.

Identity and Access Management untuk AWS Clean Rooms

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. AWS Clean Rooms IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. AWS Clean Rooms

Pengguna layanan — Jika Anda menggunakan AWS Clean Rooms layanan untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AWS Clean Rooms fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS Clean Rooms, lihat Memecahkan masalah AWS Clean Rooms identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas AWS Clean Rooms sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS Clean Rooms. Tugas Anda adalah menentukan AWS Clean Rooms fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah

izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM AWS Clean Rooms, lihatBagaimana AWS Clean Rooms bekerja dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke AWS Clean Rooms. Untuk melihat contoh kebijakan AWS Clean Rooms berbasis identitas yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk AWS Clean Rooms

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensyal yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center) atau autentikasi masuk tunggal perusahaan Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat proses penandatanganan Versi Tanda Tangan 4 di Referensi Umum AWS.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Pengguna root akun AWS kredensi dan identitas IAM di. Referensi Umum AWS

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensyal sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy).

Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Setiap entitas IAM (pengguna atau peran) dimulai tanpa izin. Secara default, pengguna tidak dapat melakukan apa pun, bahkan tidak mengubah kata sandi mereka sendiri. Untuk memberikan izin kepada pengguna untuk melakukan sesuatu, administrator harus melampirkan kebijakan izin kepada pengguna. Atau administrator dapat menambahkan pengguna ke grup yang memiliki izin yang dimaksudkan. Ketika administrator memberikan izin untuk grup, semua pengguna dalam grup tersebut akan diberi izin tersebut.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan yang dikelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran di Akun AWS Anda. Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan

yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batas izin untuk suatu entitas. Izin yang dihasilkan adalah persimpangan antara kebijakan berbasis identitas milik entitas dan batas izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS Clean Rooms bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AWS Clean Rooms, pelajari fitur IAM yang tersedia untuk digunakan. AWS Clean Rooms

Fitur IAM yang dapat Anda gunakan dengan AWS Clean Rooms

Fitur IAM	AWS Clean Rooms dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Parsial
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Parsial
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya

Fitur IAM	AWS Clean Rooms dukungan
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara AWS Clean Rooms dan Layanan AWS pekerjaan lainnya dengan sebagian besar fitur IAM, lihat Layanan AWS yang berfungsi dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk AWS Clean Rooms

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk AWS Clean Rooms

Untuk melihat contoh kebijakan AWS Clean Rooms berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Clean Rooms

Kebijakan berbasis sumber daya dalam AWS Clean Rooms

Mendukung kebijakan berbasis sumber daya	Parsial

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

AWS Clean Rooms Layanan ini hanya mendukung satu jenis kebijakan berbasis sumber daya yang disebut kebijakan sumber daya terkelola model mirip mirip yang dikonfigurasi, yang dilampirkan ke model mirip yang dikonfigurasi. Kebijakan ini menentukan prinsipal mana yang dapat melakukan tindakan pada model mirip yang dikonfigurasi.

Untuk mempelajari cara melampirkan kebijakan berbasis sumber daya ke model mirip yang dikonfigurasi, lihat. Perilaku IAM untuk AWS Clean Rooms ML

Tindakan kebijakan untuk AWS Clean Rooms

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki

nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar AWS Clean Rooms tindakan, lihat Tindakan yang ditentukan oleh AWS Clean Rooms dalam Referensi Otorisasi Layanan.

Tindakan kebijakan AWS Clean Rooms menggunakan awalan berikut sebelum tindakan.

```
cleanrooms
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "cleanrooms:action1",
      "cleanrooms:action2"
         ]
```

Untuk melihat contoh kebijakan AWS Clean Rooms berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Clean Rooms

Sumber daya kebijakan untuk AWS Clean Rooms

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis AWS Clean Rooms sumber daya dan ARNnya, lihat Sumber daya yang ditentukan oleh AWS Clean Rooms dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan AWS Clean Rooms.

Untuk melihat contoh kebijakan AWS Clean Rooms berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS Clean Rooms

Kunci kondisi kebijakan untuk AWS Clean Rooms

Mendukung kunci kondisi kebijakan khusus layanan	Parsial

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika

izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk mempelajari cara AWS Clean Rooms ML menggunakan kunci kondisi kebijakan, lihat Perilaku IAM untuk AWS Clean Rooms ML.

ACL di AWS Clean Rooms

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan AWS Clean Rooms

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal sementara dengan AWS Clean Rooms

Mendukung penggunaan kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensil sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensil sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat Peralihan peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensil sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensil sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk AWS Clean Rooms

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk

menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk AWS Clean Rooms

Mendukung peran layanan	Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak AWS Clean Rooms fungsionalitas. Edit peran layanan hanya jika AWS Clean Rooms memberikan panduan untuk melakukannya.

Peran terkait layanan untuk AWS Clean Rooms

Mendukung peran terkait layanan	Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk AWS Clean Rooms

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi AWS Clean Rooms sumber daya. Mereka juga tidak dapat melakukan tugas dengan menggunakan

AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS Clean Rooms, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi AWS Clean Rooms di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol AWS Clean Rooms
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus AWS Clean Rooms sumber daya di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.

- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam IAM dalam Panduan Pengguna IAM.

Menggunakan konsol AWS Clean Rooms

Untuk mengakses AWS Clean Rooms konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang AWS Clean Rooms sumber daya di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan AWS Clean Rooms konsol, lampirkan juga kebijakan AWS Clean Rooms `FullAccess` atau `ReadOnly` AWS terkelola

ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI 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 kebijakan terkelola untuk AWS Clean Rooms

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: **`AWSCleanRoomsReadOnlyAccess`**

Anda dapat melampirkan `AWSCleanRoomsReadOnlyAccess` ke kepala IAM Anda.

Kebijakan ini memberikan izin hanya-baca untuk sumber daya dan metadata dalam kolaborasi. `AWSCleanRoomsReadOnlyAccess`

Detail izin

Kebijakan ini mencakup izin berikut:

- `CleanRoomsRead`— Memungkinkan kepala sekolah akses hanya-baca ke layanan.
- `ConsoleDisplayTables`— Memungkinkan akses hanya-baca prinsipal ke AWS Glue metadata yang diperlukan untuk menampilkan data tentang tabel yang mendasarinya di konsol. AWS Glue
- `ConsoleLogSummaryQueryLogs`— Memungkinkan kepala sekolah untuk melihat log kueri.
- `ConsoleLogSummaryObtainLogs`— Memungkinkan kepala sekolah untuk mengambil hasil log.

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

```
"Statement": [
 {
  "Sid": "CleanRoomsRead",
  "Effect": "Allow",
  "Action": [
   "cleanrooms:BatchGet*",
   "cleanrooms:Get*",
   "cleanrooms:List*"
  ],
  "Resource": "*"
 },
 {
  "Sid": "ConsoleDisplayTables",
  "Effect": "Allow",
  "Action": [
   "glue:GetDatabase",
   "glue:GetDatabases",
   "glue:GetTable",
   "glue:GetTables",
   "glue:GetPartition",
   "glue:GetPartitions",
   "glue:GetSchema",
   "glue:GetSchemaVersion",
   "glue:BatchGetPartition"
  ],
  "Resource": "*"
 },
 {
  "Sid": "ConsoleLogSummaryQueryLogs",
  "Effect": "Allow",
  "Action": [
   "logs:StartQuery"
  ],
  "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
 },
 {
  "Sid": "ConsoleLogSummaryObtainLogs",
  "Effect": "Allow",
  "Action": [
   "logs:GetQueryResults"
  ],
  "Resource": "*"
 }
]
```

```
}
```

AWS kebijakan terkelola: **AWSCleanRoomsFullAccess**

Anda dapat melampirkan `AWSCleanRoomsFullAccess` ke kepala IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh (baca, tulis, dan perbarui) ke sumber daya dan metadata dalam suatu kolaborasi. AWS Clean Rooms Kebijakan ini mencakup akses untuk melakukan kueri.

Detail izin

Kebijakan ini mencakup izin berikut:

- `CleanRoomsAccess`— Memberikan akses penuh ke semua tindakan pada semua sumber daya untuk AWS Clean Rooms.
- `PassServiceRole`— Memberikan akses untuk meneruskan peran layanan hanya ke layanan (`PassedToService`kondisi) yang memiliki "cleanrooms" dalam namanya.
- `ListRolesToPickServiceRole`— Memungkinkan kepala sekolah untuk membuat daftar semua peran mereka untuk memilih peran layanan saat menggunakan. AWS Clean Rooms
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Memungkinkan kepala sekolah untuk melihat peran layanan dan kebijakan terkait di IAM.
- `ListPoliciesToInspectServiceRolePolicy`— Memungkinkan kepala sekolah untuk melihat peran layanan dan kebijakan terkait di IAM.
- `GetPolicyToInspectServiceRolePolicy`— Memungkinkan kepala sekolah untuk melihat peran layanan dan kebijakan terkait di IAM.
- `ConsoleDisplayTables`— Memungkinkan akses hanya-baca prinsipal ke AWS Glue metadata yang diperlukan untuk menampilkan data tentang tabel yang mendasarinya di konsol. AWS Glue
- `ConsolePickQueryResultsBucketListAll`— Memungkinkan kepala sekolah memilih bucket Amazon S3 dari daftar semua bucket S3 yang tersedia di mana hasil kueri mereka ditulis.
- `SetQueryResultsBucket`— Memungkinkan kepala sekolah untuk memilih bucket S3 di mana hasil kueri mereka ditulis.
- `ConsoleDisplayQueryResults`— Memungkinkan kepala sekolah untuk menampilkan hasil kueri kepada pelanggan, baca dari bucket S3.
- `WriteQueryResults`— Memungkinkan kepala sekolah untuk menulis hasil kueri ke dalam bucket S3 milik pelanggan.

- `EstablishLogDeliveries`— Memungkinkan prinsipal mengirimkan log kueri ke grup CloudWatch log Amazon Logs pelanggan.
- `SetupLogGroupsDescribe`— Memungkinkan kepala sekolah untuk menggunakan proses pembuatan grup CloudWatch log Amazon Logs.
- `SetupLogGroupsCreate`— Memungkinkan kepala sekolah untuk membuat grup CloudWatch log Amazon Logs.
- `SetupLogGroupsResourcePolicy`— Memungkinkan prinsipal untuk menyiapkan kebijakan sumber daya di grup CloudWatch log Amazon Logs.
- `ConsoleLogSummaryQueryLogs`— Memungkinkan kepala sekolah untuk melihat log kueri.
- `ConsoleLogSummaryObtainLogs`— Memungkinkan kepala sekolah untuk mengambil hasil log.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CleanRoomsAccess",
   "Effect": "Allow",
   "Action": [
    "cleanrooms:*"
   ],
   "Resource": "*"
  },
  {
   "Sid": "PassServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*",
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ListRolesToPickServiceRole",
   "Effect": "Allow",
   "Action": [
```

```
    "iam:ListRoles"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetRoleAndListRolePoliciesToInspectServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:GetRole",
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
   ],
   "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*"
  },
  {
   "Sid": "ListPoliciesToInspectServiceRolePolicy",
   "Effect": "Allow",
   "Action": [
    "iam:ListPolicies"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetPolicyToInspectServiceRolePolicy",
   "Effect": "Allow",
   "Action": [
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
   ],
   "Resource": "arn:aws:iam::*:policy/*cleanrooms*"
  },
  {
   "Sid": "ConsoleDisplayTables",
   "Effect": "Allow",
   "Action": [
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:GetSchema",
    "glue:GetSchemaVersion",
    "glue:BatchGetPartition"
```

```
    ],
    "Resource": "*"
   },
   {
    "Sid": "ConsolePickQueryResultsBucketListAll",
    "Effect": "Allow",
    "Action": [
     "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
   },
   {
    "Sid": "SetQueryResultsBucket",
    "Effect": "Allow",
    "Action": [
     "s3:GetBucketLocation",
     "s3:ListBucketVersions"
    ],
    "Resource": "arn:aws:s3:::cleanrooms-queryresults*"
   },
   {
    "Sid": "WriteQueryResults",
    "Effect": "Allow",
    "Action": [
     "s3:ListBucket",
     "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::cleanrooms-queryresults*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "ConsoleDisplayQueryResults",
    "Effect": "Allow",
    "Action": [
     "s3:GetObject"
    ],
    "Resource": "arn:aws:s3:::cleanrooms-queryresults*"
   },
   {
    "Sid": "EstablishLogDeliveries",
```

```
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogDelivery",
     "logs:GetLogDelivery",
     "logs:UpdateLogDelivery",
     "logs:DeleteLogDelivery",
     "logs:ListLogDeliveries"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "SetupLogGroupsDescribe",
    "Effect": "Allow",
    "Action": [
     "logs:DescribeLogGroups"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "SetupLogGroupsCreate",
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogGroup"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "SetupLogGroupsResourcePolicy",
    "Effect": "Allow",
```

```
    "Action": [
      "logs:DescribeResourcePolicies",
     "logs:PutResourcePolicy"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "ConsoleLogSummaryQueryLogs",
    "Effect": "Allow",
    "Action": [
     "logs:StartQuery"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
   },
   {
    "Sid": "ConsoleLogSummaryObtainLogs",
    "Effect": "Allow",
    "Action": [
     "logs:GetQueryResults"
    ],
    "Resource": "*"
   }
  ]
}
```

AWS kebijakan terkelola: **AWSCleanRoomsFullAccessNoQuerying**

Anda dapat melampirkan `AWSCleanRoomsFullAccessNoQuerying` ke AndaIAM principals.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh (baca, tulis, dan perbarui) ke sumber daya dan metadata dalam suatu kolaborasi. AWS Clean Rooms Kebijakan ini mengecualikan akses untuk melakukan kueri.

Detail izin

Kebijakan ini mencakup izin berikut:

- `CleanRoomsAccess`— Memberikan akses penuh ke semua tindakan pada semua sumber daya untuk AWS Clean Rooms, kecuali untuk kueri dalam kolaborasi.
- `CleanRoomsNoQuerying`— Secara eksplisit menyangkal `StartProtectedQuery` dan `UpdateProtectedQuery` mencegah kueri.
- `PassServiceRole`— Memberikan akses untuk meneruskan peran layanan hanya ke layanan (`PassedToService`kondisi) yang memiliki "cleanrooms" dalam namanya.
- `ListRolesToPickServiceRole`— Memungkinkan kepala sekolah untuk membuat daftar semua peran mereka untuk memilih peran layanan saat menggunakan. AWS Clean Rooms
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Memungkinkan kepala sekolah untuk melihat peran layanan dan kebijakan terkait di IAM.
- `ListPoliciesToInspectServiceRolePolicy`— Memungkinkan kepala sekolah untuk melihat peran layanan dan kebijakan terkait di IAM.
- `GetPolicyToInspectServiceRolePolicy`— Memungkinkan kepala sekolah untuk melihat peran layanan dan kebijakan terkait di IAM.
- `ConsoleDisplayTables`— Memungkinkan akses hanya-baca prinsipal ke AWS Glue metadata yang diperlukan untuk menampilkan data tentang tabel yang mendasarinya di konsol. AWS Glue
- `EstablishLogDeliveries`— Memungkinkan prinsipal mengirimkan log kueri ke grup CloudWatch log Amazon Logs pelanggan.
- `SetupLogGroupsDescribe`— Memungkinkan kepala sekolah untuk menggunakan proses pembuatan grup CloudWatch log Amazon Logs.
- `SetupLogGroupsCreate`— Memungkinkan kepala sekolah untuk membuat grup CloudWatch log Amazon Logs.
- `SetupLogGroupsResourcePolicy`— Memungkinkan prinsipal untuk menyiapkan kebijakan sumber daya di grup CloudWatch log Amazon Logs.
- `ConsoleLogSummaryQueryLogs`— Memungkinkan kepala sekolah untuk melihat log kueri.
- `ConsoleLogSummaryObtainLogs`— Memungkinkan kepala sekolah untuk mengambil hasil log.
- `cleanrooms`— Kelola kolaborasi, templat analisis, tabel yang dikonfigurasi, keanggotaan, dan sumber daya terkait dalam layanan. AWS Clean Rooms Lakukan berbagai operasi seperti membuat, memperbarui, menghapus, mencantumkan, dan mengambil informasi tentang sumber daya ini.
- `iam`— Lulus peran layanan dengan nama yang berisi `cleanrooms` "" ke AWS Clean Rooms layanan. Buat daftar peran, kebijakan, dan periksa peran dan kebijakan layanan yang terkait dengan AWS Clean Rooms layanan.

- `glue`— Mengambil informasi tentang database, tabel, partisi, dan skema dari. AWS Glue Ini diperlukan agar AWS Clean Rooms layanan dapat menampilkan dan berinteraksi dengan sumber data yang mendasarinya.
- `logs`— Mengelola pengiriman log, grup log, dan kebijakan sumber daya untuk CloudWatch Log. Kueri dan ambil log yang terkait dengan AWS Clean Rooms layanan. Izin ini diperlukan untuk tujuan pemantauan, audit, dan pemecahan masalah dalam layanan.

Kebijakan ini juga secara eksplisit menyangkal tindakan `cleanrooms:StartProtectedQuery` dan `cleanrooms:UpdateProtectedQuery` untuk mencegah pengguna mengeksekusi atau memperbarui kueri yang dilindungi secara langsung, yang harus dilakukan melalui mekanisme yang dikendalikan. AWS Clean Rooms

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CleanRoomsAccess",
   "Effect": "Allow",
   "Action": [
    "cleanrooms:BatchGetCollaborationAnalysisTemplate",
    "cleanrooms:BatchGetSchema",
    "cleanrooms:BatchGetSchemaAnalysisRule",
    "cleanrooms:CreateAnalysisTemplate",
    "cleanrooms:CreateCollaboration",
    "cleanrooms:CreateConfiguredTable",
    "cleanrooms:CreateConfiguredTableAnalysisRule",
    "cleanrooms:CreateConfiguredTableAssociation",
    "cleanrooms:CreateMembership",
    "cleanrooms:DeleteAnalysisTemplate",
    "cleanrooms:DeleteCollaboration",
    "cleanrooms:DeleteConfiguredTable",
    "cleanrooms:DeleteConfiguredTableAnalysisRule",
    "cleanrooms:DeleteConfiguredTableAssociation",
    "cleanrooms:DeleteMember",
    "cleanrooms:DeleteMembership",
    "cleanrooms:GetAnalysisTemplate",
    "cleanrooms:GetCollaboration",
    "cleanrooms:GetCollaborationAnalysisTemplate",
    "cleanrooms:GetConfiguredTable",
    "cleanrooms:GetConfiguredTableAnalysisRule",
    "cleanrooms:GetConfiguredTableAssociation",
```

```
    "cleanrooms:GetMembership",
    "cleanrooms:GetProtectedQuery",
    "cleanrooms:GetSchema",
    "cleanrooms:GetSchemaAnalysisRule",
    "cleanrooms:ListAnalysisTemplates",
    "cleanrooms:ListCollaborationAnalysisTemplates",
    "cleanrooms:ListCollaborations",
    "cleanrooms:ListConfiguredTableAssociations",
    "cleanrooms:ListConfiguredTables",
    "cleanrooms:ListMembers",
    "cleanrooms:ListMemberships",
    "cleanrooms:ListProtectedQueries",
    "cleanrooms:ListSchemas",
    "cleanrooms:UpdateAnalysisTemplate",
    "cleanrooms:UpdateCollaboration",
    "cleanrooms:UpdateConfiguredTable",
    "cleanrooms:UpdateConfiguredTableAnalysisRule",
    "cleanrooms:UpdateConfiguredTableAssociation",
    "cleanrooms:UpdateMembership",
    "cleanrooms:ListTagsForResource",
    "cleanrooms:UntagResource",
    "cleanrooms:TagResource"
   ],
   "Resource": "*"
  },
  {
   "Sid": "CleanRoomsNoQuerying",
   "Effect": "Deny",
   "Action": [
    "cleanrooms:StartProtectedQuery",
    "cleanrooms:UpdateProtectedQuery"
   ],
   "Resource": "*"
  },
  {
   "Sid": "PassServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*",
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": "cleanrooms.amazonaws.com"
```

```
    }
   }
  },
  {
   "Sid": "ListRolesToPickServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:ListRoles"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetRoleAndListRolePoliciesToInspectServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:GetRole",
    "iam:ListRolePolicies",
    "iam:ListAttachedRolePolicies"
   ],
   "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*"
  },
  {
   "Sid": "ListPoliciesToInspectServiceRolePolicy",
   "Effect": "Allow",
   "Action": [
    "iam:ListPolicies"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetPolicyToInspectServiceRolePolicy",
   "Effect": "Allow",
   "Action": [
    "iam:GetPolicy",
    "iam:GetPolicyVersion"
   ],
   "Resource": "arn:aws:iam::*:policy/*cleanrooms*"
  },
  {
   "Sid": "ConsoleDisplayTables",
   "Effect": "Allow",
   "Action": [
    "glue:GetDatabase",
    "glue:GetDatabases",
```

```
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:GetSchema",
    "glue:GetSchemaVersion",
    "glue:BatchGetPartition"
   ],
   "Resource": "*"
  },
  {
   "Sid": "EstablishLogDeliveries",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs:DeleteLogDelivery",
    "logs:ListLogDeliveries"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "SetupLogGroupsDescribe",
   "Effect": "Allow",
   "Action": [
    "logs:DescribeLogGroups"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "SetupLogGroupsCreate",
   "Effect": "Allow",
   "Action": [
```

```
    "logs:CreateLogGroup"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "SetupLogGroupsResourcePolicy",
   "Effect": "Allow",
   "Action": [
     "logs:DescribeResourcePolicies",
    "logs:PutResourcePolicy"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ConsoleLogSummaryQueryLogs",
   "Effect": "Allow",
   "Action": [
    "logs:StartQuery"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
   "Sid": "ConsoleLogSummaryObtainLogs",
   "Effect": "Allow",
   "Action": [
    "logs:GetQueryResults"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS kebijakan terkelola: **AWSCleanRoomsMLReadOnlyAccess**

Anda dapat melampirkan `AWSCleanRoomsMLReadOnlyAccess` ke kepala IAM Anda.

Kebijakan ini memberikan izin hanya-baca untuk sumber daya dan metadata dalam kolaborasi. `AWSCleanRoomsMLReadOnlyAccess`

Kebijakan ini mencakup izin berikut:

- `CleanRoomsConsoleNavigation`— Memberikan akses untuk melihat layar AWS Clean Rooms konsol.
- `CleanRoomsMLRead`— Memungkinkan akses hanya-baca kepala sekolah ke layanan Clean Rooms MS.

```
{
    "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 kebijakan terkelola: **AWSCleanRoomsMLFullAccess**

Anda dapat melampirkan `AWSCleanRoomsMLFullAcces` ke kepala IAM Anda. Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh (baca, tulis, dan perbarui) ke sumber daya dan metadata yang dibutuhkan oleh Clean Rooms.

Detail izin

Kebijakan ini mencakup izin berikut:

- `CleanRoomsMLFullAccess`— Memberikan akses ke semua tindakan Clean Rooms MS.
- `PassServiceRole`— Memberikan akses untuk meneruskan peran layanan hanya ke layanan (`PassedToService`kondisi) yang memiliki "cleanrooms-ml" dalam namanya.
- `CleanRoomsConsoleNavigation`— Memberikan akses untuk melihat layar AWS Clean Rooms konsol.
- `CollaborationMembershipCheck`— Saat Anda memulai pekerjaan pembuatan audiens (segmen mirip) dalam sebuah kolaborasi, layanan Clean Rooms MS memanggil `ListMembers` untuk memeriksa apakah kolaborasi tersebut valid, pemanggil adalah anggota aktif, dan pemilik model audiens yang dikonfigurasi adalah anggota aktif. Izin ini selalu diperlukan; SID navigasi konsol hanya diperlukan untuk pengguna konsol.
- `AssociateModels`— Memungkinkan kepala sekolah untuk mengaitkan model Clean Rooms MS dengan kolaborasi Anda.
- `TagAssociations`— Memungkinkan prinsipal untuk menambahkan tag ke asosiasi antara model mirip dan kolaborasi.
- `ListRolesToPickServiceRole`— Memungkinkan kepala sekolah untuk membuat daftar semua peran mereka untuk memilih peran layanan saat menggunakan. AWS Clean Rooms
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Memungkinkan kepala sekolah untuk melihat peran layanan dan kebijakan terkait di IAM.
- `ListPoliciesToInspectServiceRolePolicy`— Memungkinkan kepala sekolah untuk melihat peran layanan dan kebijakan terkait di IAM.

- `GetPolicyToInspectServiceRolePolicy`— Memungkinkan kepala sekolah untuk melihat peran layanan dan kebijakan terkait di IAM.
- `ConsoleDisplayTables`— Memungkinkan akses hanya-baca prinsipal ke AWS Glue metadata yang diperlukan untuk menampilkan data tentang tabel yang mendasarinya di konsol. AWS Glue
- `ConsolePickOutputBucket`— Memungkinkan kepala sekolah memilih bucket Amazon S3 untuk output model audiens yang dikonfigurasi.
- `ConsolePickS3Location`— Memungkinkan kepala sekolah untuk memilih lokasi dalam ember untuk output model audiens yang dikonfigurasi.

```
{
    "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 pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Clean Rooms sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat AWS Clean Rooms dokumen.

Perubahan	Deskripsi	Tanggal
AWSCleanRoomsFullAccessNoQuerying – Pembaruan ke kebijakan yang sudah ada	Menambahkan cleanrooms:BatchGetSchemaAnalysisRule ke CleanRoomsAccess.	13 Mei 2024
AWSCleanRoomsFullAccess – Pembaruan ke kebijakan yang sudah ada	Memperbarui ID Pernyataan AWSCleanRoomsFullAccess dari ConsolePickQueryResultsBucket ke SetQueryResultsBucket dalam kebijakan ini untuk merepresentasikan izin dengan lebih baik karena izin diperlukan untuk menyetel bucket hasil kueri baik dengan maupun tanpa konsol.	Maret 21, 2024
AWSCleanRoomsMLReadOnlyAccess – Kebijakan baru AWSCleanRoomsMLFullAccess – Kebijakan baru	Ditambahkan AWSCleanRoomsMLReadOnlyAccess dan AWSCleanRoomsMLFullAccess untuk mendukung AWS Clean Rooms ML.	November 29, 2023
AWSCleanRoomsFullAccessNoQuerying – Pembaruan ke kebijakan yang sudah ada	Ditambahkan cleanrooms:CreateAnalysisTemplatecleanrooms:GetAnalysisTemplate,cleanrooms:UpdateAnalysisTemplate, cleanrooms:DeleteAnalysisTemplate,cleanrooms:ListAnalysisTemplates,cleanrooms:GetCollaborationAnalysisTemplate,cleanrooms:BatchGetCollaborationAnalysisTemplate,, dan cleanrooms:ListCollaborationAnalysisTemplates CleanRoomsAccess untuk mengaktifkan fitur template analisis baru.	31 Juli 2023
AWSCleanRoomsFullAccessNoQuerying – Pembaruan ke kebijakan yang sudah ada	Ditambahkancleanrooms:ListTagsForResource,cleanrooms:UntagResource, dan cleanroom	21 Maret 2023

Perubahan	Deskripsi	Tanggal
	s:TagResource CleanRoomsAccess untuk mengaktifkan penandaan sumber daya.	
AWS Clean Rooms mulai melacak perubahan	AWS Clean Rooms mulai melacak perubahan untuk kebijakan yang AWS dikelola.	Januari 12, 2023

Memecahkan masalah AWS Clean Rooms identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Clean Rooms dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS Clean Rooms
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses AWS Clean Rooms sumber daya saya

Saya tidak berwenang untuk melakukan tindakan di AWS Clean Rooms

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya fiktif *`my-example-widget`*, tetapi tidak memiliki izin fiktif `cleanrooms:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cleanrooms:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan Mateo harus diperbarui untuk memungkinkannya mengakses *`my-example-widget`* sumber daya menggunakan `cleanrooms:`*`GetWidget`* tindakan.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran AWS Clean Rooms.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di AWS Clean Rooms. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses AWS Clean Rooms sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah AWS Clean Rooms mendukung fitur ini, lihatBagaimana AWS Clean Rooms bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.

- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

Pencegahan confused deputy lintas layanan

Masalah deputi yang bingung adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan pengguna utama layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceArn`global dalam kebijakan sumber daya untuk membatasi izin yang AWSClean Rooms memberikan layanan lain ke sumber daya. Gunakan `aws:SourceArn` jika Anda hanya ingin satu sumber daya dikaitkan dengan akses lintas layanan.

Cara paling efektif untuk melindungi dari masalah confused deputy adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Di AWSClean Rooms, Anda juga harus membandingkan dengan kunci `sts:ExternalId` kondisi.

Nilai `aws:SourceArn` harus diatur ke ARN dari keanggotaan peran yang diasumsikan.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceArn` global AWSClean Rooms untuk mencegah masalah wakil yang membingungkan.

> **Note**
>
> Contoh kebijakan berlaku untuk kebijakan kepercayaan dari peran layanan yang AWSClean Rooms digunakan untuk mengakses data pelanggan.
> Nilai *`Membershipid`* adalah ID AWSClean Rooms keanggotaan Anda dalam kolaborasi.

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

Perilaku IAM untuk AWS Clean Rooms ML

Lowongan kerja lintas akun

Clean Rooms ML memungkinkan sumber daya tertentu yang dibuat oleh seseorang Akun AWS untuk diakses dengan aman di akun mereka oleh yang lain Akun AWS. Ketika klien di Akun AWS A memanggil `StartAudienceGenerationJob` `ConfiguredAudienceModel` sumber daya yang dimiliki oleh Akun AWS B, Clean Rooms MLmembuat dua ARN untuk pekerjaan itu. Satu ARN di Akun AWS A dan satu lagi di B. Akun AWS ARN identik kecuali untuk mereka Akun AWS.

Clean Rooms MS membuat dua ARN untuk pekerjaan tersebut guna memastikan bahwa kedua akun dapat menerapkan kebijakan IAM mereka sendiri untuk pekerjaan tersebut. Misalnya, kedua akun dapat menggunakan kontrol akses berbasis tag dan menerapkan kebijakan dari AWS organisasi mereka. Pekerjaan memproses data dari kedua akun, sehingga kedua akun dapat menghapus pekerjaan dan data terkait. Tidak ada akun yang dapat memblokir akun lain dari menghapus pekerjaan.

Hanya ada satu eksekusi pekerjaan dan kedua akun dapat melihat pekerjaan ketika mereka meneleponListAudienceGenerationJobs. Kedua akun dapat memanggilGet,Delete, dan Export API di tempat kerja menggunakan ARN dengan ID mereka sendiri Akun AWS .

Tidak ada yang Akun AWS dapat mengakses pekerjaan saat menggunakan ARN dengan ID lainnya Akun AWS .

Nama pekerjaan harus unik dalam sebuah Akun AWS. Nama di Akun AWS B adalah *$ Accounta-$name*. Nama yang dipilih oleh Akun AWS A diawali dengan Akun AWS A ketika pekerjaan dilihat di Akun AWS B.

Agar lintas akun StartAudienceGenerationJob berhasil, Akun AWS B harus mengizinkan tindakan tersebut pada pekerjaan baru di Akun AWS B dan ConfiguredAudienceModel di Akun AWS B menggunakan kebijakan sumber daya yang mirip dengan contoh berikut:

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

Jika Anda menggunakan API AWS Clean Rooms API untuk membuat model mirip mirip yang dikonfigurasi dengan `manageResourcePolicies` disetel ke true, AWS Clean Rooms buat kebijakan ini untuk Anda.

Selain itu, kebijakan identitas penelepon di Akun AWS A memerlukan `StartAudienceGenerationJob` izin. `arn:aws:cleanrooms-ml:us-west-1:AccountA:audience-generation-job/*` Jadi ada tiga Sumber Daya IAM untuk Tindakan`StartAudienceGenerationJob`: pekerjaan Akun AWS A, pekerjaan Akun AWS B, dan Akun AWS B`ConfiguredAudienceModel`.

> **Warning**
>
> Akun AWS Yang memulai pekerjaan menerima peristiwa log AWS CloudTrail audit tentang pekerjaan itu. Akun AWS Yang memiliki `ConfiguredAudienceModel` tidak menerima peristiwa log AWS CloudTrail audit.

Lowongan kerja Tagging

Saat Anda menyetel `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` parameter`CreateConfiguredAudienceModel`, semua pekerjaan pembuatan segmen yang mirip dalam akun Anda yang dibuat dari model mirip mirip yang dikonfigurasi secara default untuk memiliki tag yang sama dengan model mirip yang dikonfigurasi. Model mirip yang dikonfigurasi adalah induk dan pekerjaan pembuatan segmen yang mirip adalah anak.

Jika Anda membuat pekerjaan di dalam akun Anda sendiri, tag permintaan pekerjaan akan menggantikan tag induk. Pekerjaan yang dibuat oleh akun lain tidak pernah membuat tag di akun Anda. Jika Anda menetapkan `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` dan akun lain membuat pekerjaan, ada dua salinan pekerjaan. Salinan di akun Anda memiliki tag sumber daya induk dan salinan di akun pengirim pekerjaan memiliki tag dari permintaan.

Memvalidasi kolaborator

Saat memberikan izin kepada anggota AWS Clean Rooms kolaborasi lainnya, kebijakan sumber daya harus menyertakan kunci kondisi. `cleanrooms-ml:CollaborationId` Ini memberlakukan

bahwa `collaborationId` parameter disertakan dalam StartAudienceGenerationJobpermintaan. Ketika `collaborationId` parameter disertakan dalam permintaan, Clean Rooms MS memvalidasi bahwa kolaborasi ada, pengirim pekerjaan adalah anggota aktif kolaborasi, dan pemilik model mirip yang dikonfigurasi adalah anggota aktif kolaborasi.

Saat AWS Clean Rooms mengelola kebijakan sumber daya model mirip mirip yang dikonfigurasi (`manageResourcePolicies`parameternya `TRUE` dalam CreateConfiguredAudienceModelAssociation permintaan), kunci kondisi ini akan disetel dalam kebijakan sumber daya. Oleh karena itu, Anda harus menentukan `collaborationId` in StartAudienceGenerationJob.

Akses lintas akun

Hanya `StartAudienceGenerationJob` dapat dipanggil di seluruh akun. Semua Clean Rooms MS API lainnya hanya dapat digunakan dengan sumber daya di akun Anda sendiri. Ini memastikan bahwa data pelatihan Anda, konfigurasi model yang mirip, dan informasi lainnya tetap pribadi.

Clean Rooms MS tidak pernah mengungkapkan Amazon S3 atau AWS Glue lokasi di seluruh akun. Lokasi data pelatihan, lokasi keluaran model mirip yang dikonfigurasi, dan lokasi benih pekerjaan pembuatan segmen yang mirip tidak pernah terlihat di seluruh akun. Jika Anda `Get` memiliki pekerjaan pembuatan audiens yang dikirimkan oleh akun lain, layanan tidak menampilkan lokasi benih.

Validasi kepatuhan untuk AWS Clean Rooms

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.

- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Clean Rooms

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur di AWS Clean Rooms

Sebagai layanan terkelola, AWS Clean Rooms dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Clean Rooms melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Keamanan jaringan

Saat AWS Clean Rooms membaca dari bucket S3 Anda selama eksekusi kueri, lalu lintas antara AWS Clean Rooms dan Amazon S3 dirutekan dengan aman melalui jaringan pribadi. AWS Lalu lintas

dalam penerbangan ditandatangani menggunakan protokol Amazon Signature Version 4 (SigV4) dan dienkripsi menggunakan HTTPS. Lalu lintas ini diotorisasi berdasarkan peran layanan IAM yang telah Anda siapkan untuk tabel yang dikonfigurasi.

Anda dapat terhubung secara terprogram ke AWS Clean Rooms melalui titik akhir. Untuk daftar titik akhir layanan, lihat AWS Clean Rooms titik akhir dan kuota di. Referensi Umum AWS

Semua titik akhir layanan hanya HTTP. Anda dapat menggunakan titik akhir Amazon Virtual Private Cloud (VPC) jika Anda ingin terhubung dari VPC AWS Clean Rooms Anda dan tidak ingin memiliki konektivitas internet. Untuk informasi selengkapnya, lihat Akses AWS layanan melalui AWS PrivateLinkAWS PrivateLink Panduan.

Anda dapat menetapkan kebijakan IAM ke prinsipal IAM Anda yang menggunakan kunci SourceVpce konteks aws: untuk membatasi prinsipal IAM Anda agar hanya dapat melakukan panggilan melalui titik akhir VPC dan bukan melalui AWS Clean Rooms internet.

Access AWS Clean Rooms atau AWS Clean Rooms ML menggunakan endpoint antarmuka ()AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara virtual private cloud (VPC) dan AWS Clean Rooms atau AWS Clean Rooms ML. Anda dapat mengakses AWS Clean Rooms atau AWS Clean Rooms ML seolah-olah berada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk mengakses. AWS Clean Rooms

Anda membuat koneksi pribadi ini dengan membuat titik akhir antarmuka, yang didukung oleh AWS PrivateLink. Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola pemohon yang berfungsi sebagai titik masuk untuk lalu lintas yang ditakdirkan. AWS Clean Rooms

Untuk informasi selengkapnya, lihat Mengakses Layanan AWS melalui AWS PrivateLink di Panduan AWS PrivateLink .

Pertimbangan untuk AWS Clean Rooms

Sebelum Anda menyiapkan titik akhir antarmuka AWS Clean Rooms, tinjau Pertimbangan dalam Panduan.AWS PrivateLink

AWS Clean Rooms dan dukungan AWS Clean Rooms ML membuat panggilan ke semua tindakan API mereka melalui titik akhir antarmuka.

Kebijakan titik akhir VPC tidak didukung untuk AWS Clean Rooms atau ML. AWS Clean Rooms Secara default, akses penuh ke AWS Clean Rooms dan AWS Clean Rooms ML diizinkan melalui titik akhir antarmuka. Atau, Anda dapat mengaitkan grup keamanan dengan antarmuka jaringan titik akhir untuk mengontrol lalu lintas ke AWS Clean Rooms atau AWS Clean Rooms ML melalui titik akhir antarmuka.

Buat titik akhir antarmuka untuk AWS Clean Rooms

Anda dapat membuat titik akhir antarmuka untuk AWS Clean Rooms atau AWS Clean Rooms ML menggunakan konsol Amazon VPC atau AWS Command Line Interface ().AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLink Panduan.

Buat titik akhir antarmuka untuk AWS Clean Rooms menggunakan nama layanan berikut.

```
com.amazonaws.region.cleanrooms
```

Buat endpoint antarmuka untuk AWS Clean Rooms ML menggunakan nama layanan berikut.

```
com.amazonaws.region.cleanrooms-ml
```

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API untuk AWS Clean Rooms menggunakan nama DNS Regional default. Misalnya, `cleanrooms-ml.us-east-1.amazonaws.com`.

Pemantauan AWS Clean Rooms

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja AWS Clean Rooms dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton AWS Clean Rooms, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log Anda dari instans Amazon EC2, AWS CloudTrail, dan sumber lainnya. Amazon CloudWatch Logs dapat memantau informasi dalam file log dan memberi tahu Anda ketika ambang batas tertentu terpenuhi. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.

  Clean Rooms MS memungkinkan pekerjaan lintas akun untuk tindakan API tertentu. Akun AWS Yang memulai pekerjaan menerima peristiwa log AWS CloudTrail audit untuk pekerjaan itu. Untuk informasi selengkapnya, lihat Perilaku IAM untuk AWS Clean Rooms ML
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama Anda Akun AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Mencatat panggilan API AWS Clean Rooms menggunakan AWS CloudTrail

AWS Clean Roomsterintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauLayanan AWS diAWS Clean Rooms. CloudTrail menangkap semua panggilan API untukAWS Clean Rooms sebagai kejadian. Panggilan yang direkam mencakup panggilan dari AWS Clean Rooms konsol dan panggilan kode ke operasi API AWS Clean Rooms ini. Jika membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan dari CloudTrail bucket Amazon S3, termasuk kejadian untukAWS Clean Rooms. Jika Anda tidak dapat mengonfigurasi, Anda masih dapat melihat tindakan terbaru di CloudTrail konsol di Riwayat peristiwa. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuatAWS Clean Rooms, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail lainnya.

Untuk mempelajari lebih lanjut CloudTrail, lihat PanduanAWS CloudTrail Pengguna.

AWS Clean Roomsinformasi dalam CloudTrail

CloudTrail diaktifkan pada AndaAkun AWS saat Anda membuat akun. Ketika aktivitas terjadi diAWS Clean Rooms, aktivitas tersebut dicatat dalam CloudTrail peristiwa bersama peristiwa lainnya di RiwayatLayanan AWS peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi lebih lanjut, lihat Melihat peristiwa dengan Riwayat CloudTrail peristiwa.

Untuk catatan berkelanjutan tentang peristiwa di Akun AWS, termasuk peristiwa untuk AWS Clean Rooms, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi lainnyaLayanan AWS untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail Layanan yang didukung dan integrasi
- Mengkonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima berkas CloudTrail log dari beberapa Wilayah
- Menerima berkas CloudTrail log dari beberapa akun

SemuaAWS Clean Rooms tindakan dicatat oleh CloudTrail dan didokumentasikan dalam ReferensiAWS Clean Rooms API.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Jika permintaan tersebut dibuat dengan kredensi pengguna root atau.
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan.
- Jika permintaan tersebut dibuat oleh yang lainLayanan AWS.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log AWS Clean Rooms

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail Berkas log berisi satu atau beberapa entri log. Sebuah peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail Berkas log bukan jejak tumpukan terurut dari panggilan API, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

ContohAWS Clean Rooms CloudTrail peristiwa

Contoh berikut menunjukkan CloudTrail peristiwa untuk:

Topik

- StartProtectedQuery (berhasil)
- StartProtectedQuery(gagal)

StartProtectedQuery (berhasil)

```
{
    "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(gagal)

```
{
    "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"
}
```

Menciptakan AWS Clean Rooms sumber daya dengan AWS CloudFormation

AWS Clean Rooms terintegrasi dengan AWS CloudFormation, layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya Anda. Sebagai hasil dari integrasi ini, Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat template yang menjelaskan semua AWS sumber daya yang Anda inginkan, dan menyediakan serta AWS CloudFormation mengonfigurasi sumber daya tersebut untuk Anda. Contoh sumber daya termasuk kolaborasi, tabel yang dikonfigurasi, asosiasi tabel yang dikonfigurasi, dan keanggotaan.

Ketika Anda menggunakan AWS CloudFormation, Anda dapat menggunakan kembali template Anda untuk mengatur AWS Clean Rooms sumber daya Anda secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang dalam beberapa Akun AWS dan Wilayah AWS.

AWS Clean Rooms dan AWS CloudFormation template

Untuk menyediakan dan mengonfigurasi sumber daya untuk AWS Clean Rooms dan layanan terkait, Anda harus memahami AWS CloudFormation templat. Templat adalah file teks dengan format JSON atau YAML. Template ini menjelaskan sumber daya yang ingin Anda sediakan di AWS CloudFormation tumpukan Anda. Jika Anda tidak terbiasa dengan JSON atau YAMAL, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan template. AWS CloudFormation Untuk informasi selengkapnya, lihat Apa itu AWS CloudFormation Designer? di Panduan Pengguna AWS CloudFormation .

AWS Clean Rooms mendukung pembuatan kolaborasi, tabel yang dikonfigurasi, asosiasi tabel yang dikonfigurasi, dan keanggotaan di. AWS CloudFormationUntuk informasi selengkapnya, termasuk contoh templat JSON dan YAMAL untuk kolaborasi, tabel yang dikonfigurasi, asosiasi tabel yang dikonfigurasi, dan keanggotaan, lihat referensi jenis AWS Clean Rooms sumber daya di Panduan Pengguna.AWS CloudFormation

Templat berikut ini tersedia:

- Template analisis

Tentukan templat AWS Clean Rooms analisis, termasuk nama, deskripsi, format, sumber, parameter, dan tag.

Untuk informasi selengkapnya, lihat topik berikut:

AWS::CleanRooms::AnalysisTemplate di Panduan Pengguna AWS Clean Rooms

CreateAnalysisTemplate di Referensi API AWS Clean Rooms

- Kolaborasi

  Tentukan AWS Clean Rooms kolaborasi, termasuk nama, deskripsi, jenis, parameter, dan tag.

  Untuk informasi selengkapnya, lihat topik berikut:

  AWS::CleanRooms::Collaboration di Panduan Pengguna AWS CloudFormation

  CreateCollaboration di Referensi API AWS Clean Rooms

- Tabel yang dikonfigurasi

  Tentukan tabel yang dikonfigurasi AWS Clean Rooms, termasuk kolom yang diizinkan, metode analisis, deskripsi, nama, referensi tabel, anggaran privasi, dan tag. Tabel yang dikonfigurasi mewakili referensi ke tabel yang ada di AWS Glue Data Catalog yang telah dikonfigurasi untuk digunakan dalam AWS Clean Rooms. Tabel yang dikonfigurasi berisi aturan analisis yang menentukan bagaimana data dapat digunakan.

  Untuk informasi selengkapnya, lihat topik berikut:

  AWS::CleanRooms::ConfiguredTable di Panduan Pengguna AWS CloudFormation

  CreateConfiguredTable di Referensi API AWS Clean Rooms

- Asosiasi tabel yang dikonfigurasi

  Tentukan asosiasi tabel yang dikonfigurasi di AWS Clean Rooms, termasuk ID, deskripsi, ID keanggotaan, nama, peran, Nama Sumber Daya Amazon (ARN), dan tag. Asosiasi tabel yang dikonfigurasi menautkan tabel yang dikonfigurasi dengan kolaborasi.

  Untuk informasi selengkapnya, lihat topik berikut:

  AWS::CleanRooms::ConfiguredTableAssociation di Panduan Pengguna AWS CloudFormation

CreateConfiguredTableAssociation di Referensi API AWS Clean Rooms

- Keanggotaan

  Tentukan keanggotaan untuk pengidentifikasi kolaborasi tertentu dan bergabunglah dengan kolaborasi di AWS Clean Rooms.

  Untuk informasi selengkapnya, lihat topik berikut:

  AWS::CleanRooms::Membership di Panduan Pengguna AWS CloudFormation

  CreateMembership di Referensi API AWS Clean Rooms

- Templat Anggaran Privasi

  Tentukan templat anggaran AWS Clean Rooms privasi, termasuk anggaran privasi, kebisingan yang ditambahkan per kueri, dan penyegaran anggaran privasi bulanan.

  Untuk informasi selengkapnya, lihat topik berikut:

  AWS::CleanRooms::PrivacyBudgetTemplate di Panduan Pengguna AWS CloudFormation

  CreatePrivacyBudgetTemplate di Referensi API AWS Clean Rooms

- Buat kumpulan data pelatihan

  Tentukan kumpulan data pelatihan untuk model Clean Rooms MS dari AWS Glue tabel.

  Untuk informasi selengkapnya, lihat topik berikut:

  AWS::CleanRoomsML::TrainingDataset di Panduan Pengguna AWS CloudFormation

  CreateTrainingDatasetdi Referensi API Clean Rooms

Pelajari lebih lanjut tentang AWS CloudFormation

Untuk mempelajari selengkapnya AWS CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormation Panduan Pengguna
- AWS CloudFormation Referensi API
- Panduan Pengguna Antarmuka Baris Perintah AWS CloudFormation

Kuota untuk AWS Clean Rooms

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk masing-masing. Layanan AWS Kecuali dinyatakan lain, setiap kuota khusus untuk. Wilayah AWS Anda dapat meminta kenaikan untuk beberapa kuota, dan kuota lainnya tidak dapat ditingkatkan.

Untuk melihat kuota AWS Clean Rooms, buka konsol Service Quotas. Di panel navigasi, pilih layanan AWS dan pilih AWS Clean Rooms.

Untuk meminta peningkatan kuota, lihat Meminta Peningkatan Kuota dalam Panduan Pengguna Service Quotas. Jika kuota belum tersedia di Service Quotas, gunakan formulir peningkatan batas Layanan.

Anda Akun AWS memiliki kuota berikut yang terkait AWS Clean Rooms dengan.

Sumber Daya	Default	Deskripsi
Anggota diundang per kolaborasi	5	Jumlah maksimum anggota yang diundang per kolaborasi
Keanggotaan per akun	100	Jumlah maksimum keanggotaan untuk akun
Kolaborasi dibuat per akun	10	Jumlah maksimum kolaborasi yang dibuat per akun
Tabel yang dikonfigurasi per akun	60	Jumlah maksimum tabel yang dikonfigurasi yang dapat dibuat oleh akun
Asosiasi tabel per keanggotaan	25	Jumlah maksimum tabel yang terkait per keanggotaan aktif
Kueri berkelanjutan bersamaan per keanggotaan	5	Jumlah maksimum kueri yang sedang berlangsung bersamaan per keanggotaan

Sumber Daya	Default	Deskripsi
Kolom per daftar izinkan tabel yang dikonfigurasi	100	Jumlah maksimum kolom yang dapat diizinkanterdaftar per tabel yang dikonfigurasi
Tabel yang dikonfigurasi per kueri yang dilindungi	15	Jumlah maksimum tabel yang dikonfigurasi dalam kueri yang dilindungi
Templat analisis per keanggotaan	25	Jumlah maksimum templat analisis per keanggotaan
Asosiasi model mirip (model audiens) yang dikonfigurasi per keanggotaan	5	Jumlah maksimum asosiasi model mirip yang dikonfigurasi per keanggotaan.

Batas parameter sumber daya

Sumber Daya	Default	Deskripsi
Ukuran aturan analisis	100 KB	Ukuran maksimum JSON untuk aturan analisis
Panjang teks kueri	90 KB (8KB untuk kueri privasi diferensial)	Panjang teks maksimum untuk pernyataan kueri SQL
Waktu berjalan kueri	12 jam	Durasi maksimum kueri dijalankan sebelum batas waktu
Ukuran keluaran file data kueri	6,2 GB	Ukuran maksimum file keluaran dari kueri yang dilindungi

Anda Akun AWS memiliki transaksi API per detik (TPS) per akun per kuota titik akhir berikut.

Kuota pelambatan API

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `BatchGetCollaborationAnalysisTemplate`	5 TPS	Jumlah maksimum panggilan `BatchGetCollaborationAnalysisTemplate` API per detik
Permintaan tarif `BatchGetSchema`	5 TPS	Jumlah maksimum panggilan `BatchGetSchema` API per detik
Permintaan tarif `CreateAnalysisTemplate`	5 TPS	Jumlah maksimum panggilan `CreateAnalysisTemplate` API per detik
Permintaan tarif `CreateCollaboration`	5 TPS	Jumlah maksimum panggilan `CreateCollaboration` API per detik
Permintaan tarif `CreateConfiguredAudienceModelAssociation`	5 TPS	Jumlah maksimum `CreateConfiguredAudienceModelAssociation` panggilan per detik
Permintaan tarif `CreateConfiguredTable`	5 TPS	Jumlah maksimum `CreateConfiguredTable` panggilan per detik
Permintaan tarif `CreateConfiguredTableAnalysisRule`	5 TPS	Jumlah maksimum `CreateConfiguredTableAnalysisRule` panggilan per detik
Permintaan tarif `CreateConfiguredTableAssociation`	5 TPS	Jumlah maksimum `CreateConfiguredTableAssociation` panggilan per detik

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `CreateMembership`	5 TPS	Jumlah maksimum `CreateMembership` panggilan per detik
Permintaan tarif `CreatePrivacyBudgetTempate`	5 TPS	Jumlah maksimum `CreatePrivacyBudgetTemplate` panggilan per detik
Permintaan tarif `DeleteAnalysisTemplate`	5 TPS	Jumlah maksimum `DeleteAnalysisTemplate` panggilan per detik
Permintaan tarif `DeleteCollaboration`	5 TPS	Jumlah maksimum `DeleteCollaboration` panggilan per detik
Permintaan tarif `DeleteConfiguredAudienceModelAssociation`	5 TPS	Jumlah maksimum `DeleteConfiguredAudienceModelAssociation` panggilan per detik
Permintaan tarif `DeleteConfiguredTable`	5 TPS	Jumlah maksimum `DeleteConfiguredTable` panggilan per detik
Permintaan tarif `DeleteConfiguredTableAnalysisRule`	5 TPS	Jumlah maksimum `DeleteConfiguredTableAnalysisRule` panggilan per detik
Permintaan tarif `DeleteConfiguredTableAssociation`	5 TPS	Jumlah maksimum `DeleteConfiguredTableAssociation` panggilan per detik

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `DeleteMember`	5 TPS	Jumlah maksimum `DeleteMember` panggilan per detik
Permintaan tarif `DeleteMembership`	5 TPS	Jumlah maksimum `DeleteMembership` panggilan per detik
Permintaan tarif `DeletePrivacyBudgetTemplate`	5 TPS	Jumlah maksimum `DeletePrivacyBudgetTemplate` panggilan per detik
Permintaan tarif `GetAnalysisTemplate`	5 TPS	Jumlah maksimum `GetAnalysisTemplate` panggilan per detik
Permintaan tarif `GetCollaboration`	5 TPS	Jumlah maksimum `GetCollaboration` panggilan per detik
Permintaan tarif `GetCollaborationConfiguredAudienceModelAssociation`	5 TPS	Jumlah maksimum `GetCollaborationConfiguredAudienceModelAssociation` panggilan per detik
Permintaan tarif `GetCollaborationPrivacyBudgetTemplate`	5 TPS	Jumlah maksimum `GetCollaborationPrivacyBudgetTemplate` panggilan per detik
Permintaan tarif `GetConfiguredAudienceModelAssociation`	5 TPS	Jumlah maksimum `GetConfiguredAudienceModelAssociation` panggilan per detik

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `GetConfiguredTable`	5 TPS	Jumlah maksimum `GetConfiguredTable` panggilan per detik
Permintaan tarif `GetConfiguredTableAnalysisRule`	5 TPS	Jumlah maksimum `GetConfiguredTableAnalysisRule` panggilan per detik
Permintaan tarif `GetConfiguredTableAssociation`	20 TPS	Jumlah maksimum `GetConfiguredTableAssociation` panggilan per detik
Permintaan tarif `GetMembership`	5 TPS	Jumlah maksimum `GetMembership` panggilan per detik
Permintaan tarif `GetPrivacyBudgetTemplate`	5 TPS	Jumlah maksimum `GetPrivacyBudgetTemplate` panggilan per detik
Permintaan tarif `GetProtectedQuery`	20 TPS	Jumlah maksimum `GetProtectedQuery` panggilan per detik
Permintaan tarif `GetSchema`	5 TPS	Jumlah maksimum `GetSchema` panggilan per detik
Permintaan tarif `GetSchemaAnalysisRule`	5 TPS	Jumlah maksimum `GetSchemaAnalysisRule` panggilan per detik

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `ListAnalysisTemplates`	5 TPS	Jumlah maksimum `ListAnalysisTemplates` panggilan per detik
Permintaan tarif `ListCollaborationConfiguredAudienceModelAssociations`	5 TPS	Jumlah maksimum `ListCollaborationConfiguredAudienceModelAssociations` panggilan per detik
Permintaan tarif `ListCollaborationPrivacyBudgets`	5 TPS	Jumlah maksimum `ListCollaborationPrivacyBudgets` panggilan per detik
Permintaan tarif `ListCollaborationPrivacyBudgetTemplates`	5 TPS	Jumlah maksimum `ListCollaborationPrivacyBudgetTemplates` panggilan per detik
Permintaan tarif `ListCollaborations`	5 TPS	Jumlah maksimum `ListCollaborations` panggilan per detik
Permintaan tarif `ListConfiguredAudienceModelAssociations`	5 TPS	Jumlah maksimum `ListConfiguredAudienceModelAssociations` panggilan per detik
Permintaan tarif `ListConfiguredTableAssociations`	5 TPS	Jumlah maksimum `ListConfiguredTableAssociations` panggilan per detik

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `ListConfiguredTables`	5 TPS	Jumlah maksimum `ListConfiguredTables` panggilan per detik
Permintaan tarif `ListMembers`	5 TPS	Jumlah maksimum `ListMembers` panggilan per detik
Permintaan tarif `ListMemberships`	5 TPS	Jumlah maksimum `ListMemberships` panggilan per detik
Permintaan tarif `ListPrivacyBudgets`	5 TPS	Jumlah maksimum `ListPrivacyBudgets` panggilan per detik
Permintaan tarif `ListPrivacyBudgetTemplates`	5 TPS	Jumlah maksimum `ListPrivacyBudgetTemplates` panggilan per detik
Permintaan tarif `ListProtectedQueries`	5 TPS	Jumlah maksimum `ListProtectedQueries` panggilan per detik
Permintaan tarif `ListSchemas`	5 TPS	Jumlah maksimum `ListSchemas` panggilan per detik
Permintaan tarif `StartProtectedQuery`	5 TPS	Jumlah maksimum `StartProtectedQuery` panggilan per detik
Permintaan tarif `UpdateAnalysisTemplate`	5 TPS	Jumlah maksimum `UpdateAnalysisTemplate` panggilan per detik

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `UpdateCollaboration`	5 TPS	Jumlah maksimum `UpdateCollaboration` panggilan per detik
Permintaan tarif `UpdateConfiguredAudienceModelAssociation`	5 TPS	Jumlah maksimum `UpdateConfiguredAudienceModelAssociation` panggilan per detik
Permintaan tarif `UpdateConfiguredTable`	5 TPS	Jumlah maksimum `UpdateConfiguredTable` panggilan per detik
Permintaan tarif `UpdateConfiguredTableAnalysisRule`	5 TPS	Jumlah maksimum `UpdateConfiguredTableAnalysisRule` panggilan per detik
Permintaan tarif `UpdateConfiguredTableAssociation`	5 TPS	Jumlah maksimum `UpdateConfiguredTableAssociation` panggilan per detik
Permintaan tarif `UpdatePrivacyBudgetTemplate`	5 TPS	Jumlah maksimum `UpdatePrivacyBudgetTemplate` panggilan per detik

AWS Clean Rooms Kuota pelambatan API API

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `CreateAudienceModel`	1 tingkat TPS, 3 TPS meledak	Jumlah maksimum panggilan `CreateAudienceModel` API per detik

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `CreateConfiguredAudienceModel`	10 TPS	Jumlah maksimum panggilan `CreateConfiguredAudienceModel` API per detik
Permintaan tarif `CreateTrainingDataset`	10 TPS	Jumlah maksimum panggilan `CreateTrainingDataset` API per detik
Permintaan tarif `DeleteAudienceGenerationJob`	2 tingkat TPS, 10 TPS meledak	Jumlah maksimum panggilan `DeleteAudienceGenerationJob` API per detik
Permintaan tarif `DeleteAudienceModel`	2 tingkat TPS, 10 TPS meledak	Jumlah maksimum panggilan `DeleteAudienceModel` API per detik
Permintaan tarif `DeleteConfiguredAudienceModel`	10 TPS	Jumlah maksimum panggilan `DeleteConfiguredAudienceModel` API per detik
Permintaan tarif `DeleteConfiguredAudienceModelPolicy`	25 TPS	Jumlah maksimum panggilan `DeleteConfiguredAudienceModelPolicy` API per detik
Permintaan tarif `DeleteTrainingDataset`	10 TPS	Jumlah maksimum panggilan `DeleteTrainingDataset` API per detik
Permintaan tarif `GetAudienceGenerationJob`	50 TPS	Jumlah maksimum panggilan `GetAudienceGenerationJob` API per detik

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `GetAudienceModel`	50 TPS	Jumlah maksimum panggilan `GetAudienceModel` API per detik
Permintaan tarif `GetConfiguredAudienceModel`	50 TPS	Jumlah maksimum panggilan `GetConfiguredAudienceModel` API per detik
Permintaan tarif `GetConfiguredAudienceModelPolicy`	50 TPS	Jumlah maksimum panggilan `GetConfiguredAudienceModelPolicy` API per detik
Permintaan tarif `GetTrainingDataset`	50 TPS	Jumlah maksimum panggilan `GetTrainingDataset` API per detik
Permintaan tarif `ListAudienceExportJobs`	50 TPS	Jumlah maksimum panggilan `ListAudienceExportJobs` API per detik
Permintaan tarif `ListAudienceGenerationJobs`	50 TPS	Jumlah maksimum panggilan `ListAudienceGenerationJobs` API per detik
Permintaan tarif `ListAudienceModels`	50 TPS	Jumlah maksimum panggilan `ListAudienceModels` API per detik
Permintaan tarif `ListConfiguredAudienceModels`	50 TPS	Jumlah maksimum panggilan `ListConfiguredAudienceModels` API per detik
Permintaan tarif `ListTagsForResource`	50 TPS	Jumlah maksimum panggilan `ListTagsForResource` API per detik

Sumber Daya	Batas tarif	Deskripsi
Permintaan tarif `ListTrainingDatasets`	50 TPS	Jumlah maksimum panggilan `ListTrainingDatasets` API per detik
Permintaan tarif `PutConfiguredAudienceModelPolicy`	25 TPS	Jumlah maksimum panggilan `PutConfiguredAudienceModelPolicy` API per detik
Permintaan tarif `StartAudienceExportJob`	1 tingkat TPS, 3 TPS meledak	Jumlah maksimum panggilan `StartAudienceExportJob` API per detik
Permintaan tarif `StartAudienceGenerationJob`	1 tingkat TPS, 5 TPS meledak	Jumlah maksimum panggilan `StartAudienceGenerationJob` API per detik
Permintaan tarif `TagResource`	10 TPS	Jumlah maksimum panggilan `TagResource` API per detik
Permintaan tarif `UntagResource`	50 TPS	Jumlah maksimum panggilan `UntagResource` API per detik
Permintaan tarif `UpdateConfiguredAudienceModel`	10 TPS	Jumlah maksimum panggilan `UpdateConfiguredAudienceModel` API per detik

Nama	Default	Dapat disesuaikan	Deskripsi
Pekerjaan ekspor audiens aktif per pekerjaan pembuatan audiens	Setiap Wilayah yang didukung: 25	Tidak	Jumlah maksimum pekerjaan ekspor audiens

Nama	Default	Dapat disesuaikan	Deskripsi
			aktif untuk pekerjaan generasi audiens
Pekerjaan ekspor audiens yang tertunda/sedang berlangsung per pelanggan	Setiap Wilayah yang didukung: 20	Tidak	Jumlah maksimum pekerjaan ekspor audiens yang sedang berlangsung per pelanggan
Pekerjaan pembuatan audiens yang tertunda/dalam proses per pelanggan	Setiap Wilayah yang didukung: 10	Ya	Jumlah maksimum pekerjaan pembuatan audiens yang sedang berlangsung per pelanggan
Model audiens yang tertunda/dalam proses per pelanggan	Setiap Wilayah yang didukung: 2	Ya	Jumlah maksimum pekerjaan pelatihan model audiens yang sedang berlangsung per pelanggan

Kuota Kamar Bersih

Sumber Daya	Default	Deskripsi
Dataset	per pekerjaan	
Jumlah maksimum interaksi	20 miliar	Jumlah maksimum interaksi yang diizinkan dalam data pelatihan. Input yang lebih besar diambil sampelnya.
Minimal jumlah interaksi	1 juta.	

Sumber Daya	Default	Deskripsi
Jumlah maksimum pengguna berbeda untuk pelatihan model mirip	1 juta.	Jika lebih banyak dimasukkan, hanya 100 juta teratas yang digunakan, diberi peringkat berdasarkan jumlah interaksi.
Jumlah minimum pengguna yang berbeda untuk pelatihan model mirip	100.000	
Jumlah maksimum pengguna untuk pekerjaan segmen mirip ekspor (audiens)	10.000	
Jumlah maksimum item berbeda yang digunakan untuk pelatihan model.	1 juta.	Anda dapat memasukkan hingga 50 juta item, tetapi hanya 1 juta yang paling populer yang digunakan.
Jumlah maksimum kolom fitur dalam kumpulan data pelatihan.	10	
Jumlah minimum item berbeda per pengguna	2	AWS Clean Rooms ML mengharuskan setiap baris atau pengguna memiliki dua item atau lebih, termasuk item berulang.
Ukuran maksimum audiens benih	500.000	
Ukuran minimum audiens benih	500	Penyedia data pelatihan dapat menetapkan nilai ini serendah 25.
API	per pelanggan	

Sumber Daya	Default	Deskripsi
Jumlah total kumpulan data pelatihan aktif	500	
Jumlah total model mirip aktif (model audiens)	500	
Jumlah total model mirip yang dikonfigurasi aktif (model audiens)	10.000	
Jumlah total pekerjaan pembuatan segmen mirip (audiens) yang diselesaikan	Tidak ada batas	
Jumlah total pekerjaan segmen mirip ekspor (audiens) yang diselesaikan	Tidak ada batas	
Durasi maksimum pekerjaan pembuatan model mirip (model audiens)	1 hari (24 jam)	
Durasi maksimum pekerjaan pembuatan segmen mirip (audiens)	10 jam	Setelah Anda memberikan benih, Clean Rooms MLmembutuhkan waktu maksimal 10 jam untuk menghasilkan segmen yang mirip.
Persentase minimum untuk bin ukuran segmen (audiens)	1%	
Persentase maksimum untuk tempat sampah ukuran segmen (audiens)	20%	

Sumber Daya	Default	Deskripsi
Ukuran absolut minimum untuk bin ukuran segmen (audiens)	1% dari jumlah pengguna yang berbeda	
Ukuran absolut maksimum untuk tempat sampah ukuran segmen (audiens)	20% dari jumlah pengguna yang berbeda	

Riwayat dokumen untuk Panduan AWS Clean Rooms Pengguna

Tabel berikut menjelaskan rilis dokumentasi untuk AWS Clean Rooms.

Untuk notifikasi tentang pembaruan-pembaruan dokumentasi ini, Anda dapat berlangganan ke sebuah umpan RSS. Untuk berlangganan pembaruan RSS, Anda harus mengaktifkan plug-in RSS untuk browser yang Anda gunakan.

Perubahan	Deskripsi	Tanggal
Perbarui ke kebijakan yang ada	Izin baru berikut telah ditambahkan ke kebijakan `AWSCleanRoomsFullAccessNoQuerying` terkelola:`cleanrooms:BatchGetSchemaAnalysisRule` .	13 Mei 2024
AWS Clean Rooms ML sekarang sepenuhnya tersedia	AWS Clean Rooms ML menyediakan metode peningkatan privasi bagi dua pihak untuk mengidentifikasi pengguna serupa dalam data mereka tanpa perlu berbagi data mereka satu sama lain.	April 3, 2024
Perbarui ke kebijakan yang ada	ID Pernyataan dalam kebijakan `AWSCleanRoomsFullAccess` terkelola telah diperbarui dari ConsolePickQueryResultsBucket ke SetQueryResultsBucket untuk mewakili izin dengan lebih baik sejak izin.	Maret 21, 2024

Kebijakan terkelola baru untuk AWS Clean Rooms ML	Dua kebijakan terkelola baru telah ditambahkan: `AWSCleanRoomsMLReadOnlyAccess` dan`AWSCleanRoomsMLFullAccess` .	November 29, 2023
AWS Clean Rooms ML (pratinjau)	AWS Clean Rooms ML menyediakan metode peningkatan privasi bagi dua pihak untuk mengidentifikasi pengguna serupa dalam data mereka tanpa perlu berbagi data mereka satu sama lain.	November 29, 2023
AWS Clean Rooms Privasi Diferensial (pratinjau)	Pelanggan sekarang dapat menggunakan Privasi AWS Clean Rooms Diferensial untuk membantu melindungi privasi pengguna mereka.	November 29, 2023
Konfigurasi pembayaran	Pembuat kolaborasi sekarang dapat mengonfigurasi anggota yang dapat menjalankan kueri atau anggota lain dalam kolaborasi yang akan ditagih untuk biaya komputasi kueri.	14 November 2023
Waktu berjalan kueri - perbarui	Durasi maksimum kueri dijalankan sebelum batas waktu diperbarui dari 4 jam menjadi 12 jam.	Oktober 6, 2023

AWS CloudFormation sumber daya - perbarui	AWS Clean Rooms telah menambahkan sumber daya baru berikut:`AWS::CleanRooms::Membership Protected QueryOutputConfiguration` ,`AWS::CleanRooms::Membership ProtectedQueryResultConfiguration` , dan`AWS::CleanRooms::Membership Protected QueryS3OutputConfiguration` .	7 September 2023
AWS CloudFormation sumber daya - perbarui	AWS Clean Rooms telah menambahkan sumber daya baru berikut: `AWS::CleanRooms::AnalysisTemplate` dan`AWS::CleanRooms::ConfiguredTable AnalysisRuleCustom` .	31 Agustus 2023
Kemampuan anggota terpisah	Pembuat kolaborasi sekarang dapat menunjuk satu anggota sebagai anggota yang dapat meminta dan anggota lain sebagai anggota yang dapat menerima hasil. Ini memberi pembuat kolaborasi kemampuan untuk memastikan bahwa anggota yang dapat melakukan kueri tidak memiliki akses ke hasil kueri.	Agustus 30, 2023

AWS Clean Rooms Glosarium	Pembaruan khusus dokumentasi untuk menambahkan glosarium istilah. AWS Clean Rooms	Agustus 30, 2023
Support untuk Apache Iceberg tabel (pratinjau)	AWS Clean Rooms sekarang mendukung Apache Iceberg tabel (pratinjau).	Agustus 25, 2023
Pembaruan kuota	Bagian Kuota telah diperbarui untuk mencerminkan kuota default baru untuk keanggotaan per akun.	9 Agustus 2023
Perbarui ke kebijakan yang ada	Izin baru berikut telah ditambahkan ke kebijakan `AWSCleanRoomsFullAccessNoQuerying` terkelola:`cleanrooms:CreateAnalysisTemplate` ,,`cleanrooms:GetAnalysisTemplate` ,`cleanrooms:UpdateAnalysisTemplate` , `cleanrooms:DeleteAnalysisTemplate` ,`cleanrooms:ListAnalysisTemplates` , `cleanrooms:GetCollaborationAnalysisTemplate` `cleanrooms:BatchGetCollaborationAnalysisTemplate` , dan `cleanrooms:ListCollaborationAnalysisTemplates` .	31 Juli 2023

Template analisis dan aturan analisis kustom	AWS Clean Rooms sekarang mendukung template analisis dan aturan analisis Kustom. Template analisis memungkinkan kolaborator untuk membangun atau mengimpor kueri SQL kustom mereka sendiri untuk digunakan dalam kolaborasi. Dengan aturan analisis Kustom, pemilik tabel dapat menyetujui kueri SQL kustom pada tabel yang dikonfigurasi.	31 Juli 2023
Aturan analisis mendukung kondisi OR logis	AWS Clean Rooms aturan analisis sekarang mendukung kondisi OR logis dalam JOIN klausa.	29 Juni 2023
CloudFormation integrasi	AWS Clean Rooms sekarang terintegrasi dengan AWS CloudFormation.	15 Juni 2023
Pembuat analisis	Anggota yang dapat menanyakan dan menerima hasil sekarang memiliki kemampuan untuk menjalankan kueri pada beberapa tabel tanpa menulis kode SQL dengan menggunakan UI pembuat Analisis.	15 Juni 2023
Fungsi SQL	Pembaruan khusus dokumentasi untuk memperjelas fungsi SQL yang didukung.	5 Mei 2023

Pemecahan Masalah	Pembaruan khusus dokumentasi untuk menambahkan bagian Pemecahan Masalah untuk masalah umum.	27 April 2023
Tipe data yang didukung untuk AWS Clean Rooms	Pembaruan khusus dokumentasi untuk menambahkan bagian baru yang mencantumkan tipe data yang didukung AWS Glue Data Catalog .	April 26, 2023
Contoh AWS CloudTrail acara	Pembaruan khusus dokumentasi untuk menambahkan contoh CloudTrail peristiwa untuk StartProtectedQuery (berhasil) dan StartProtectedQuery (gagal).	20 April 2023
Perbarui ke kebijakan yang ada	Izin baru berikut telah ditambahkan ke kebijakan `AWSCleanRoomsFullAccessNoQuerying` terkelola:`cleanrooms:ListTagsForResource` ,`cleanrooms:UntagResource` , dan`cleanrooms:TagResource` . Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS.	21 Maret 2023
Ketersediaan umum	AWS Clean Rooms sekarang tersedia secara umum.	21 Maret 2023

Rilis pratinjau	Pratinjau rilis Panduan AWS Clean Rooms Pengguna	Januari 12, 2023

AWS Clean Rooms Glosarium

Konsultasikan glosarium ini untuk menjadi akrab dengan terminologi yang digunakan untuk. AWS Clean Rooms

Aturan analisis agregasi

Pembatasan kueri yang memungkinkan kueri yang menggunakan analisis agregatCOUNT,SUM, atau AVG berfungsi sepanjang dimensi opsional. Kueri ini tidak akan mengungkapkan informasi tingkat baris.

Mendukung kasus penggunaan seperti perencanaan kampanye, jangkauan media, frekuensi, dan pengukuran konversi.

Jenis aturan analisis lainnya adalah kustom dan daftar.

Aturan analisis

Pembatasan kueri yang mengotorisasi jenis kueri tertentu.

Jenis aturan analisis menentukan jenis analisis apa yang dapat dijalankan pada tabel yang dikonfigurasi. Setiap jenis memiliki struktur kueri yang telah ditentukan sebelumnya. Anda mengontrol bagaimana kolom tabel Anda dapat digunakan dalam struktur melalui kontrol kueri.

Jenis aturan analisis adalah agregasi, daftar, dan kustom.

Template analisis

Kueri khusus kolaborasi dan disetujui sebelumnya yang dapat digunakan kembali.

Mendukung kueri SQL kustom yang didukung di. AWS Clean Rooms

Dapat berisi parameter di mana pun nilai literal biasanya dapat muncul dalam kueri SQL. Untuk informasi selengkapnya tentang tipe parameter yang didukung, lihat Tipe data di Referensi AWS Clean Rooms SQL.

Template analisis hanya berfungsi dengan aturan analisis khusus.

Klien enkripsi C3R

Klien enkripsi Cryptographic Computing for Clean Rooms (C3R).

Digunakan untuk mengenkripsi dan mendekripsi data, C3R adalah SDK enkripsi sisi klien dengan antarmuka baris perintah.

Kolom Cleartext

Kolom yang tidak dilindungi secara kriptografi untuk konstruksi JOIN atau SELECT SQL.

Kolom Cleartext dapat digunakan di bagian manapun dari query SQL.

Kolaborasi

Batas logis yang aman AWS Clean Rooms di mana anggota dapat melakukan kueri SQL pada tabel yang dikonfigurasi.

Kolaborasi dibuat oleh pencipta kolaborasi.

Hanya anggota yang telah diundang ke kolaborasi yang dapat bergabung dalam kolaborasi.

Kolaborasi hanya dapat memiliki satu anggota yang dapat meminta data, satu anggota yang dapat menerima hasil, dan satu anggota membayar biaya komputasi kueri.

Semua anggota dapat melihat daftar peserta yang diundang dalam kolaborasi sebelum mereka bergabung dalam kolaborasi.

Pencipta kolaborasi

Anggota yang menciptakan kolaborasi.

Hanya ada satu pembuat kolaborasi per kolaborasi.

Hanya pembuat kolaborasi yang dapat menghapus anggota dari kolaborasi atau menghapus kolaborasi.

Tabel yang dikonfigurasikan

Setiap tabel dikonfigurasi mewakili referensi ke tabel yang ada di AWS Glue Data Catalog yang telah dikonfigurasi untuk digunakan dalam AWS Clean Rooms. Tabel yang dikonfigurasi berisi aturan analisis yang menentukan bagaimana data dapat digunakan.

Saat ini, AWS Clean Rooms mendukung data asosiasi yang disimpan di Amazon Simple Storage Service (Amazon S3) yang dikatalogkan melalui katalog. AWS Glue

Untuk informasi selengkapnya AWS Glue, lihat Panduan AWS Glue Pengembang.

Tabel yang dikonfigurasi dapat dikaitkan dengan satu atau lebih kolaborasi.

> **Note**
>
> AWS Clean Rooms saat ini tidak mendukung lokasi bucket Amazon S3 yang terdaftar. AWS Lake Formation

Aturan analisis khusus

Pembatasan kueri yang memungkinkan serangkaian kueri tertentu yang telah disetujui sebelumnya (templat analisis) atau memungkinkan serangkaian akun tertentu yang dapat memberikan kueri yang menggunakan data Anda.

Mendukung kasus penggunaan seperti atribusi sentuhan pertama, analisis inkremental, dan analisis penemuan audiens.

Mendukung privasi diferensial.

Dekripsi

Proses mengubah data terenkripsi kembali ke bentuk aslinya. Dekripsi hanya dapat dilakukan jika Anda memiliki akses ke kunci rahasia.

Privasi diferensial

Teknik matematikal-ketat yang melindungi data kolaborasi dari anggota yang dapat menerima hasil belajar tentang individu tertentu.

Enkripsi

Proses pengkodean data ke dalam bentuk yang muncul acak menggunakan nilai rahasia yang disebut kunci. Tidak mungkin menentukan plaintext asli tanpa akses ke kunci.

Kolom sidik jari

Kolom yang dilindungi secara kriptografi untuk konstruksi JOIN SQL.

Aturan analisis daftar

Pembatasan kueri yang memungkinkan kueri yang menampilkan analisis atribut tingkat baris dari tumpang tindih antara tabel ini dan tabel anggota yang dapat melakukan kueri.

Mendukung kasus penggunaan seperti pengayaan dan pembangunan audiens atau penindasan.

Anggota

AWS Pelanggan yang merupakan peserta dalam kolaborasi.

Seorang anggota diidentifikasi menggunakan mereka Akun AWS.

Semua anggota dapat menyumbangkan data.

Anggota yang dapat menanyakan

Anggota yang dapat meminta data dalam kolaborasi.

Hanya ada satu anggota yang dapat meminta per kolaborasi, dan anggota itu tidak dapat diubah.

Pengguna administratif dapat menggunakan izin AWS Identity and Access Management (IAM) untuk mengontrol prinsip IAM mereka (seperti pengguna atau peran) yang dapat menanyakan data dalam kolaborasi. Untuk informasi selengkapnya, lihat Membuat peran layanan untuk membaca data.

Anggota yang dapat menerima hasil

Anggota yang dapat menerima hasil kueri. Anggota yang dapat menerima hasil menentukan setelan hasil kueri untuk tujuan Amazon S3 dan format hasil kueri.

Hanya ada satu anggota yang dapat menerima hasil per kolaborasi, dan anggota itu tidak dapat diubah.

Anggota membayar biaya komputasi kueri

Anggota yang bertanggung jawab untuk membayar biaya komputasi kueri.

Hanya ada satu anggota yang bertanggung jawab untuk membayar biaya komputasi kueri per kolaborasi, dan anggota itu tidak dapat diubah.

Jika pembuat kolaborasi belum menetapkan siapa pun sebagai anggota yang membayar biaya komputasi kueri, maka anggota yang dapat melakukan kueri adalah pembayar default.

Anggota yang membayar biaya komputasi kueri menerima tagihan untuk kueri yang telah dijalankan dalam kolaborasi.

Keanggotaan

Sumber daya yang dibuat saat anggota bergabung dengan kolaborasi.

Semua sumber daya yang diasosiasikan anggota untuk kolaborasi adalah bagian dari keanggotaan atau terkait dengan keanggotaan.

Hanya anggota yang memiliki keanggotaan yang dapat menambah, menghapus, atau mengedit sumber daya dalam keanggotaan tersebut.

Kolom tertutup

Kolom yang dilindungi secara kriptografi untuk konstruksi SELECT SQL.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.