aws

User Guide

AWS Clean Rooms

AWS Clean Rooms: User Guide

Table of Contents

Was ist AWS Clean Rooms?

AWS Clean Rooms hilft Ihnen und Ihren Partnern, Ihre kollektiven Datensätze zu analysieren und gemeinsam daran zu arbeiten, um neue Erkenntnisse zu gewinnen, ohne sich gegenseitig die zugrunde liegenden Daten preiszugeben. Sie können einen sicheren Arbeitsbereich für die Zusammenarbeit verwenden AWS Clean Rooms, um innerhalb von Minuten Ihre eigenen Reinräume einzurichten und mit nur wenigen Schritten mit der Analyse Ihrer kollektiven Datensätze zu beginnen. Sie können die Partner auswählen, mit denen Sie zusammenarbeiten möchten, deren Datensätze auswählen und Einschränkungen für die Teilnehmer konfigurieren.

Mit AWS Clean Rooms können Sie mit Tausenden von Unternehmen zusammenarbeiten, die dies bereits nutzen AWS. Für die Zusammenarbeit müssen Daten nicht aus einer anderen Plattform verschoben AWS oder auf eine andere Plattform geladen werden. Wenn Sie Abfragen ausführen, AWS Clean Rooms liest es Daten von ihrem ursprünglichen Speicherort und wendet integrierte Analyseregeln an, damit Sie die Kontrolle über die Daten behalten.

AWS Clean Rooms bietet integrierte Datenzugriffskontrollen und Kontrollfunktionen zur Unterstützung von Audits, die Sie konfigurieren können. Zu diesen Kontrollen gehören:

- Analyseregeln zur Einschränkung von SQL-Abfragen und zur Bereitstellung von Ausgabebeschränkungen
- Kryptografisches Rechnen, Clean Rooms um Daten auch bei der Verarbeitung von Abfragen verschlüsselt zu halten, um strenge Datenverarbeitungsrichtlinien einzuhalten
- Abfragen von Protokollen zur Überprüfung von Anfragen und zur Unterstützung von Audits
- Differenzierter Datenschutz zum Schutz vor Versuchen zur Benutzeridentifikation. AWS Clean Rooms Differential Privacy ist eine vollständig verwaltete Funktion, die die Privatsphäre Ihrer Benutzer mit mathematisch gestützten Techniken und intuitiven Steuerelementen schützt, die Sie mit wenigen Klicks anwenden können.
- AWS Clean Rooms ML ermöglicht es zwei Parteien, ähnliche Benutzer in ihren Daten zu identifizieren, ohne ihre Daten miteinander teilen zu müssen. Die erste Partei erstellt und konfiguriert anhand ihrer Trainingsdaten ein Lookalike-Modell. Die zweite Partei bringt ihre Ausgangsdaten in eine Kollaboration ein und erstellt ein Lookalike-Segment, das den Trainingsdaten ähnelt.

Das folgende Video erklärt mehr darüber AWS Clean Rooms.

AWS Clean Rooms

Sind Sie ein AWS Clean Rooms Erstbenutzer?

Wenn Sie zum ersten Mal Benutzer von sind AWS Clean Rooms, empfehlen wir Ihnen, zunächst die folgenden Abschnitte zu lesen:

- Wie funktioniert AWS Clean Rooms
- Zugreifen AWS Clean Rooms
- Einrichten AWS Clean Rooms
- AWS Clean Rooms Glossar

Wie funktioniert AWS Clean Rooms

Der folgende Arbeitsablauf geht davon aus, dass:

- Das Kollaborationsmitglied hat seine Datentabellen bereits auf Amazon S3 hochgeladen und eine AWS Glue Tabelle erstellt.
- (Optional) Nur für verschlüsselte Datentabellen hat das Kollaborationsmitglied bereits verschlüsselte Datentabellen mit dem C3R-Verschlüsselungsclient erstellt.

Zusammenfassend lässt sich sagen, dass der Arbeitsablauf für wie AWS Clean Rooms folgt aussieht:

1. Der Ersteller der Kollaboration führt die folgenden Aufgaben aus:
   - Erstellt eine Kollaboration.
   - Lädt ein oder mehrere Mitglieder zur Kollaboration ein.
   - Weist Mitgliedern Fähigkeiten zu, z. B. dem Mitglied, das Abfragen durchführen kann, und dem Mitglied, das Ergebnisse empfangen kann.

     Wenn der Ersteller der Kollaboration auch das Mitglied ist, das Ergebnisse empfangen kann, gibt er das Ziel und das Format der Abfrageergebnisse an. Sie bieten auch eine Servicerolle Amazon Resource Name (ARN), um die Ergebnisse in das Ziel der Abfrageergebnisse zu schreiben.
   - Konfiguriert, welches Mitglied für die Bezahlung der Abfrageberechnungskosten im Rahmen der Zusammenarbeit verantwortlich ist.

2. Das eingeladene Mitglied tritt der Kollaboration bei, indem es eine Mitgliederressource erstellt.

   Wenn das eingeladene Mitglied das Mitglied ist, das Ergebnisse erhalten kann, gibt es das Ziel und das Format der Abfrageergebnisse an. Sie stellen auch eine Dienstrolle ARN bereit, um in das Ziel der Abfrageergebnisse zu schreiben.

   Wenn es sich bei dem eingeladenen Mitglied um das Mitglied handelt, das für die Bezahlung der Abfrage-Rechenkosten verantwortlich ist, akzeptiert es seine Zahlungsverpflichtungen, bevor es der Kollaboration beitritt.

3. Das Mitglied konfiguriert eine bestehende AWS Glue Tabelle zur Verwendung in AWS Clean Rooms. (Dieser Schritt kann vor oder nach dem Beitritt zu einer Kollaboration ausgeführt werden, es sei denn, Sie verwenden Cryptographic Computing forClean Rooms.)

   > **Note**
   >
   > AWS Clean Rooms unterstützt AWS Glue Tabellen. Weitere Hinweise zur Eingabe Ihrer Daten finden Sie unterSchritt 3: Laden Sie Ihre Datentabelle auf Amazon S3 hoch. AWS Glue

   1. Das Mitglied benennt die konfigurierte Tabelle und wählt aus, welche Spalten in der Kollaboration verwendet werden sollen.
   2. Das Mitglied konfiguriert eine der folgenden Analyseregeln für die konfigurierte Tabelle:
      - Aggregationsanalyseregel oder Listenanalyseregel — Zur Steuerung der Art der Analyse, die für die Tabelle ausgeführt werden kann.
      - Benutzerdefinierte Analyseregel — Um einen bestimmten Satz vorab genehmigter Abfragen oder eine bestimmte Gruppe von Konten zuzulassen, die Abfragen bereitstellen können, die Ihre Daten verwenden. Ermöglicht es dem Mitglied, den differenziellen Datenschutz zu aktivieren, um sich vor Versuchen zur Benutzeridentifizierung zu schützen.

      > **Note**
      >
      > Das Mitglied kann die Analyseregel jederzeit konfigurieren, bevor es seine konfigurierten Tabellen der Kollaboration zuordnet.

4. Das Mitglied ordnet seine konfigurierten Tabellen der Kollaboration zu und weist AWS Clean Rooms eine Servicerolle für den Zugriff auf seine AWS Glue Tabellen zu.

> **Note**
>
> Diese Servicerolle hat Berechtigungen für die Tabellen. Die Servicerolle kann nur übernommen werden AWS Clean Rooms , um zulässige Abfragen im Namen des Mitglieds auszuführen, das Abfragen durchführen kann. Keine Kollaborationsmitglieder (außer dem Datenbesitzer) haben Zugriff auf die zugrunde liegenden Tabellen in der Kollaboration. Der Datenbesitzer kann den differenziellen Datenschutz aktivieren, um seine Tabellen für Abfragen durch andere Mitglieder verfügbar zu machen.

5. Das Mitglied, das Abfragen durchführen kann, führt SQL-Abfragen für die konfigurierten Tabellen aus.

   Abfragen können nur ausgeführt werden, wenn das Mitglied, das für die Berechnung der Abfragen verantwortlich ist, der Kollaboration als aktives Mitglied beigetreten ist.

   Die Analyseregeln und Ausgabebeschränkungen werden automatisch durchgesetzt. AWS Clean Rooms gibt nur die Ergebnisse zurück, die den in Schritt 3.b definierten Analyseregeln entsprechen.

   Bei Abfragen zu verschlüsselten Daten erhält das Mitglied, das Ergebnisse empfangen kann, die verschlüsselte Ausgabe AWS Clean Rooms , die entschlüsselt werden muss (siehe Schritt 8).
6. Das Mitglied, das Ergebnisse erhalten kann, überprüft die Ergebnisse entweder in der AWS Clean Rooms Konsole oder im angegebenen Amazon S3 S3-Bucket.
7. Dem Mitglied, das die Kosten für die Berechnung von Abfragen bezahlt, werden die im Rahmen der Kollaboration ausgeführten Abfragen in Rechnung gestellt.
8. (Optional) Nur bei verschlüsselten Datentabellen entschlüsselt das Mitglied, das Ergebnisse empfangen kann, die Abfrageergebnisse, indem es den C3R-Verschlüsselungsclient im Entschlüsselungsmodus ausführt.

Zugehörige Services

Folgendes bezieht AWS-Services sich auf: AWS Clean Rooms

- Amazon S3

  Mitglieder der Kollaboration können Daten, die sie einbringen, AWS Clean Rooms in Amazon S3 speichern.

Weitere Informationen finden Sie unter den folgenden Themen:

Vorbereiten von Datentabellen für Abfragen in AWS Clean Rooms

Was ist Amazon S3? im Amazon Simple Storage Service-Benutzerhandbuch

- AWS Glue

  Mitglieder der Kollaboration können aus ihren Daten in Amazon S3 AWS Glue Tabellen zur Verwendung in erstellen AWS Clean Rooms.

  Weitere Informationen finden Sie unter den folgenden Themen:

  Vorbereiten von Datentabellen für Abfragen in AWS Clean Rooms

  Was ist AWS Glue? im Entwicklerhandbuch für AWS Glue

- AWS CloudFormation

  Erstellen Sie die folgenden Ressourcen in AWS CloudFormation: Kollaborationen, konfigurierte Tabellen, konfigurierte Tabellenzuordnungen und Mitgliedschaften

  Weitere Informationen finden Sie unter AWS Clean Rooms Ressourcen erstellen mit AWS CloudFormation.

- AWS CloudTrail

  Verwenden Sie es AWS Clean Rooms zusammen mit CloudTrail Protokollen, um Ihre Aktivitätsanalyse zu verbessern. AWS-Service

  Weitere Informationen finden Sie unter Protokollieren von AWS Clean Rooms-API-Aufrufen mithilfe von AWS CloudTrail.

Zugreifen AWS Clean Rooms

Sie können AWS Clean Rooms über die folgenden Optionen darauf zugreifen:

- Direkt über die AWS Clean Rooms Konsole unter https://console.aws.amazon.com/cleanrooms/.
- Programmgesteuert über die AWS Clean Rooms API. Weitere Informationen finden Sie in der AWS Clean Rooms -API-Referenz.

Preisgestaltung für AWS Clean Rooms

Preisinformationen finden Sie unter AWS Clean Rooms – Preise.

Abrechnung für AWS Clean Rooms

AWS Clean Rooms gibt dem Kollaborationsersteller die Möglichkeit, zu konfigurieren, welches Mitglied für die Kosten der Query-Compute in der Kollaboration bezahlt.

In den meisten Fällen sind das Mitglied, das Abfragen durchführen kann, und das Mitglied, das die Kosten für die Query-Compute bezahlt, identisch. Wenn jedoch das Mitglied, das Abfragen durchführen kann, und das Mitglied, das die Kosten für die Query Compute bezahlt, unterschiedlich sind, wird, wenn das Mitglied, das Abfragen durchführen kann, Abfragen für seine eigene Mitgliedschaftsressource ausführt, der Mitgliedschaftsressource des Mitglieds, das die Kosten für die Abfrage-Compute bezahlt, in Rechnung gestellt.

Das Mitglied, das die Kosten für die Abfragerechnung bezahlt, sieht in seinem Ereignisverlauf kein CloudTrail Ereignis für ausgeführte Abfragen, da der Zahler weder derjenige ist, der die Abfragen ausführt, noch der Besitzer der Ressource ist, für die die Abfragen ausgeführt werden. Der Zahler sieht jedoch die Rechnungen, die auf seiner Mitgliedschaftsressource für alle Abfragen des Mitglieds generiert wurden, das Abfragen in der Kollaboration ausführen kann.

Weitere Informationen zum Erstellen einer Kollaboration und zur Konfiguration des Mitglieds, das die Kosten für die Berechnung von Abfragen bezahlt, finden Sie unterErstellen Sie eine Kollaboration.

Analyseregeln in AWS Clean Rooms

Um eine Tabelle AWS Clean Rooms für die Kollaborationsanalyse zu aktivieren, muss das Kollaborationsmitglied eine Analyseregel konfigurieren.

Bei einer Analyseregel handelt es sich um eine Kontrolle zur Verbesserung des Datenschutzes, die jeder Datenbesitzer in einer konfigurierten Tabelle einrichtet. Eine Analyseregel bestimmt, wie die konfigurierte Tabelle analysiert werden kann.

Bei der Analyseregel handelt es sich um eine Kontrolle auf Kontoebene für die konfigurierte Tabelle (eine Ressource auf Kontoebene). Sie wird in jeder Zusammenarbeit durchgesetzt, der die konfigurierte Tabelle zugeordnet ist. Wenn keine Analyseregel konfiguriert ist, kann die konfigurierte Tabelle Kollaborationen zugeordnet, aber nicht abgefragt werden. Abfragen können nur auf konfigurierte Tabellen mit demselben Analyseregeltyp verweisen.

Um eine Analyseregel zu konfigurieren, wählen Sie zuerst einen Analysetyp aus und geben dann die Analyseregel an. Bei beiden Schritten sollten Sie berücksichtigen, welchen Anwendungsfall Sie aktivieren möchten und wie Sie Ihre zugrunde liegenden Daten schützen möchten.

AWS Clean Rooms erzwingt die restriktiveren Kontrollen für alle konfigurierten Tabellen, auf die in einer Abfrage verwiesen wird.

Die folgenden Beispiele veranschaulichen die restriktiven Kontrollen.

Example Restriktive Kontrolle: Ausgabebeschränkung

- Mitarbeiter A hat eine Ausgabebeschränkung für die Kennungsspalte 100.
- Mitarbeiter B hat eine Ausgabebeschränkung für die Identifikatorspalte von 150.

  Eine Aggregationsabfrage, die auf beide konfigurierten Tabellen verweist, benötigt mindestens 150 unterschiedliche Bezeichnerwerte innerhalb einer Ausgabezeile, damit sie in der Abfrageausgabe angezeigt werden kann. Die Abfrageausgabe gibt nicht an, dass Ergebnisse aufgrund der Ausgabebeschränkung entfernt wurden.

Example Restriktive Kontrolle: Analysevorlage nicht genehmigt

- Mitarbeiter A hat eine Analysevorlage mit einer Abfrage zugelassen, die in ihrer benutzerdefinierten Analyseregel auf konfigurierte Tabellen von Collaborator A und Collaborator B verweist.

- Mitarbeiter B hat die Analysevorlage nicht zugelassen.

  Da Mitarbeiter B die Analysevorlage nicht zugelassen hat, kann das Mitglied, das Abfragen durchführen kann, diese Analysevorlage nicht ausführen.

Typen von Analyseregeln

Es gibt drei Arten von Analyseregeln: Aggregationsregeln, Listenregeln und benutzerdefinierte Regeln. In den folgenden Tabellen werden die Analyseregeltypen verglichen. Jeder Typ hat einen eigenen Abschnitt, in dem die Angabe der Analyseregel beschrieben wird.

Die folgenden Tabellen enthalten eine Vergleichszusammenfassung der Analyseregeltypen.

Unterstützte Anwendungsfälle

Die folgenden Tabellen enthalten eine Vergleichszusammenfassung der unterstützten Anwendungsfälle für jeden Analyseregeltyp.

Anwendungsfall	Aggregation	Liste	Custom (Benutzer definiert)
Unterstützte Analysen	Abfragen, die Statistiken mithilfe der Funktionen COUNT, SUM und AVG anhand optionaler Dimensionen aggregieren	Abfragen, die Listen mit Überschneidungen zwischen mehreren Tabellen auf Zeilenebene ausgeben	Jede benutzerdefinierte Analyse, sofern die Analysevorlage oder der Analyseersteller überprüft und zugelassen wurden

Anwendungsfall	Aggregation	Liste	Custom (Benutzer definiert)
Allgemeine Anwendungsfälle	Segmentanalyse, Messung, Zuordnung	Bereicherung, Segmentbildung	Zuordnung auf Anhieb, inkrementelle Analysen, Zielgruppenfindung
SQL-Konstrukte	• JOIN-Anweisungen: INNER JOIN • Aggregatfunktionen: COUNT/ COUNT DISTINCT, SUM/ SUM DISTINCT und AVG • Skalarfunktionen: Eingeschränkte Teilmenge	• JOIN-Anweisungen: INNER JOIN • Skalarfunktionen: Keine	Die meisten SQL-Funktionen und SQL-Konstrukte sind mit dem SELECT-Befehl verfügbar

Anwendungsfall	Aggregation	Liste	Custom (Benutzer definiert)
Unterabfragen und allgemeine Tabellenausdrücke (CTEs)	Nein	Nein	Ja
Vorlagen für Analysen	Nein	Nein	Ja

Unterstützte Steuerelemente

Die folgenden Tabellen zeigen eine vergleichende Zusammenfassung darüber, wie die einzelnen Analyseregeltypen Ihre zugrunde liegenden Daten schützen.

Kontrolle	Aggregation	Liste	Custom (Benutzer definiert)
Kontrollmechanismus	Steuern Sie, wie Daten in der Tabelle in einer Abfrage verwendet werden können (Lassen Sie beispielsweise	Steuern Sie, wie Daten in der Tabelle in einer Abfrage verwendet werden können (Erlauben Sie beispiels	Steuern Sie, welche Abfragen in der Tabelle ausgeführt werden dürfen (Lassen Sie beispielsweise nur Abfragen zu, die

Kontrolle	Aggregation	Liste	Custom (Benutzer definiert)
	COUNT und SUM der Spalte hashed_email zu.)	weise die Verwendung der Spalte hashed_email nur für den Beitritt.)	in den Analysevorlagen „Benutzer definierte Abfrage 1" definiert sind.)
Integrierte Techniken zur Verbesserung der Privatsphäre	• Blindes Spiel • Aggregation erforderlich • Minimaler Aggregationsschwellenwert >= • 2 Vordefinierte Abfragestruktur	• Blindes Spiel • Überlappung erforderlich • Vordefinierte Abfragestruktur	Differenzierter Datenschutz

Kontrolle	Aggregation	Liste	Custom (Benutzer definiert)
Überprüfen Sie die Abfrage, bevor sie ausgeführt werden kann	Nein	Nein	Ja, mithilfe von Analysevorlagen

Weitere Informationen zu den Analyseregeln, die in verfügbar sind AWS Clean Rooms, finden Sie in den folgenden Themen.

- Regel für die Aggregationsanalyse
- Analyseregel auflisten
- Benutzerdefinierte Analyseregel in AWS Clean Rooms

Regel für die Aggregationsanalyse

In generiert AWS Clean Roomseine Aggregationsanalyseregel aggregierte Statistiken mithilfe der Funktionen COUNT, SUM und/oder AVG in optionalen Dimensionen. Wenn die Aggregationsanalyseregel zu einer konfigurierten Tabelle hinzugefügt wird, kann das Mitglied, das abfragen kann, Abfragen für die konfigurierte Tabelle ausführen.

Die Regel zur Aggregationsanalyse unterstützt Anwendungsfälle wie Kampagnenplanung, Medienreichweite, Frequenzmessung und Zuordnung.

Die unterstützte Abfragestruktur und Syntax sind in definiertStruktur und Syntax der Aggregationsabfrage.

Zu den Parametern der Analyseregel, die in definiert sindAggregationsanalyseregel – Abfragesteuerungen, gehören Abfragesteuerelemente und Abfrageergebnissteuerelemente. Zu den Abfragekontrollen gehört die Möglichkeit, zu verlangen, dass eine konfigurierte Tabelle mit mindestens einer konfigurierten Tabelle verbunden wird, die dem Mitglied gehört, das sie direkt oder

transitiv abfragen kann. Mit dieser Anforderung können Sie sicherstellen, dass die Abfrage auf der Schnittmenge (INNERJOIN) Ihrer Tabelle und ihrer Tabelle ausgeführt wird.

Struktur und Syntax der Aggregationsabfrage

Abfragen für Tabellen mit einer Aggregationsanalyseregel müssen der folgenden Syntax entsprechen.

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

In der folgenden Tabelle wird jeder Ausdruck erläutert, der in der vorherigen Syntax aufgeführt ist.

Expression	Definition	Beispiele
select_aggregate_function_expression	Eine durch Komma getrennte Liste mit den folgenden Ausdrücken:	`SELECT SUM(PRICE), user_segment`

Expression	Definition	Beispiele
	• `select_aggregation_function_expression` • `select_aggregate_expression` **Note** Es muss mindestens eine `select_aggregation_function_expression` in der gebenselect_aggregate_expression .	

Expression	Definition	Beispiele

select_aggregation_function_expression	Eine oder mehrere unterstützte Aggregationsfunktionen, die auf eine oder mehrere Spalten angewendet werden. Nur Spalten sind als Argumente für Aggregationsfunktionen zulässig.
	
	Note
	Es muss mindestens eine `select_aggregation_function_expression` in der geben`select_aggregate_expression`.
		`AVG(PRICE)`
		
		`COUNT(DISTINCT user_id)`

Expression	Definition	Beispiele

select_grouping_column_expression	Ein Ausdruck, der einen beliebigen Ausdruck enthalten kann, der Folgendes verwendet:
	• Tabellenspaltennamen
	• Unterstützte skalare Funktionen
	• Zeichenfolgeliterale
	• Numerische Literale
	
	Note
	`select_aggregate_expression` kann Spalten mit oder ohne den `AS` Parameter als Alias verwenden. Weitere Informationen finden Sie in der AWS Clean Rooms SQL-Referenz .
		`TRUNC(timestampColumn)`
		
		`UPPER(campaignName)`

Expression	Definition	Beispiele
table_expression	Eine Tabelle oder Join von Tabellen, die bedingte Join-Ausdrücke mit verbinden `join_condition` . `join_condition` gibt einen booleschen Wert zurück. Die `table_expression` unterstützt: • Ein bestimmter JOIN Typ (INNERJOIN) • Die Gleichheitsverglei chsbedingung innerhalb einer `join_condition` (=) • Logische Operatoren (`AND`, `OR`).	`FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2`

Expression	Definition	Beispiele

where_expression	Ein bedingter Ausdruck, der einen booleschen Wert zurückgibt. Es kann aus folgenden Komponenten bestehen:
	• Tabellenspaltennamen
	• Unterstützte skalare Funktionen
	• Mathematische Operatoren
	• Zeichenfolgeliterale
	• Numerische Literale
	
	Unterstützte Vergleichsbedingungen sind (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Unterstützte logische Operatoren sind (`AND, OR`).
	
	Die `where_expression` ist optional.
		`WHERE where_condition`
		
		`WHERE price > 100`
		
		`WHERE TRUNC(timestampColumn) = '1/1/2022'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

group_by_expression	Eine durch Komma getrennte Liste von Ausdrücken, die den Anforderungen für entsprechen `enselect_grouping_column_expression` .	`GROUP BY TRUNC(timestampColumn), UPPER(campaignName), segment`

Expression	Definition	Beispiele
having_expression	Ein bedingter Ausdruck, der einen booleschen Wert zurückgibt. Sie haben eine unterstützte Aggregati onsfunktion, die auf eine einzelne Spalte angewende t wird (z. B. `SUM(price )`), und werden mit einem numerischen Literal vergliche n. Unterstützte Bedingungen sind (`=, >, <, <=, >=, <>, !=`). Unterstützte logische Operatoren sind (`AND, OR`). Die `having_expression` ist optional.	`HAVING SUM(SALES) > 500`

Expression	Definition	Beispiele
order_by_expression	Eine durch Komma getrennte Liste von Ausdrücken, die mit denselben Anforderungen kompatibel ist, die zuvor `select_aggregate_expression` definiert wurden. Die `order_by_expression` ist optional. **Note** `order_by_expression` erlaubt - ASC und -DESCParameter. Weitere Informationen finden Sie unter ASC DESC-Parameter in der AWS Clean Rooms SQL-Referenz.	`ORDER BY SUM(SALES), UPPER(campaignName)`

Beachten Sie bei der Struktur und Syntax von Aggregationsabfragen Folgendes:

- Andere SQL-Befehle als SELECT werden nicht unterstützt.
- Unterabfragen und allgemeine Tabellenausdrücke (z. B. WITH) werden nicht unterstützt.
- Operatoren, die mehrere Abfragen kombinieren (z. B. UNION), werden nicht unterstützt.
- TOPDie OFFSET Parameter LIMIT, und werden nicht unterstützt.

Aggregationsanalyseregel – Abfragesteuerungen

Mit Aggregationsabfragesteuerelementen können Sie steuern, wie die Spalten in Ihrer Tabelle zum Abfragen der Tabelle verwendet werden. Sie können beispielsweise steuern, welche Spalte für die Verknüpfung verwendet wird, welche Spalte gezählt werden kann oder welche Spalte in WHERE Anweisungen verwendet werden kann.

In den folgenden Abschnitten werden die einzelnen Kontrollen erläutert.

Themen

Aggregationskontrollen

Mithilfe von Aggregationssteuerungen können Sie definieren, welche Aggregationsfunktionen zugelassen werden sollen und auf welche Spalten sie angewendet werden müssen. Aggregationsfunktionen können in den ORDER BY Ausdrücken SELECTHAVING, und verwendet werden.

Kontrolle	Definition	Verwendung
`aggregateColumns`	Spalten mit konfigurierten Tabellenspalten, die Sie für die Verwendung in Aggregati onsfunktionen zulassen.	`aggregateColumns` kann innerhalb einer Aggregati onsfunktion in den ORDER BY Ausdrücken SELECTHAVING, und verwendet werden. Einige `aggregateColumns` können auch als kategorisiert werden `joinColumn` (wird später definiert). Bei `aggregateColumn` kann nicht auch als

Kontrolle	Definition	Verwendung
		`dimensionColumn` (weiter unten definiert) kategorisiert werden.
`function`	Die Funktionen COUNT, SUM und AVG, die Sie für die Verwendung zusätzlich zur zulassen`aggregate Columns` .	`function` kann auf eine angewendet werden`aggregate Columns` , die ihr zugeordnet ist.

Join-Steuerelemente

Eine `JOIN` Klausel wird verwendet, um Zeilen aus zwei oder mehr Tabellen zu kombinieren, basierend auf einer zugehörigen Spalte zwischen ihnen.

Sie können Join-Steuerelemente verwenden, um zu steuern, wie Ihre Tabelle mit anderen Tabellen in der verknüpft werden kann`table_expression`. unterstützt AWS Clean Rooms nur INNER JOIN. -INNERJOINAnweisungen können nur Spalten verwenden, die `joinColumn` in Ihrer Analyseregel explizit als kategorisiert wurden, abhängig von den von Ihnen definierten Steuerelementen.

Der INNER JOIN muss mit einem `joinColumn` aus Ihrer konfigurierten Tabelle und einem `joinColumn` aus einer anderen konfigurierten Tabelle in der Zusammenarbeit arbeiten. Sie entscheiden, welche Spalten aus Ihrer Tabelle als verwendet werden können`joinColumn`.

Jede Übereinstimmungsbedingung innerhalb der -ONKlausel ist erforderlich, um die Gleichheitsvergleichsbedingung (=) zwischen zwei Spalten zu verwenden.

Mehrere Übereinstimmungsbedingungen innerhalb einer -ONKlausel können sein:

- Kombiniert mit dem `AND` logischen Operator
- Getrennt durch den `OR` logischen Operator

> **Note**
>
> Alle JOIN Übereinstimmungsbedingungen müssen mit einer Zeile von jeder Seite des übereinstimmenJOIN. Alle Bedingungen, die durch einen OR oder einen AND logischen Operator verbunden sind, müssen ebenfalls diese Anforderung erfüllen.

Im Folgenden finden Sie ein Beispiel für eine Abfrage mit einem AND logischen Operator.

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

Im Folgenden finden Sie ein Beispiel für eine Abfrage mit einem OR logischen Operator.

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

Kontrolle	Definition	Verwendung
`joinColumns`	Die Spalten (falls vorhanden), die dem Mitglied, das abfragen kann, erlauben soll, in der INNER JOIN Anweisung zu verwenden.	Ein bestimmter `joinColumn` kann auch als kategorisiert werden `aggregateColumn` (siehe Aggregationskontrollen). Die gleiche Spalte kann nicht sowohl als auch verwendet werden `joinColumn` `dimensionColumns` (siehe später). Sofern es nicht auch als kategorisiert wurde`aggregateColumn` ,

Kontrolle	Definition	Verwendung
		`joinColumn` kann ein nicht in anderen Teilen der Abfrage verwendet werden, außer in der INNER JOIN.
`joinRequired`	Steuern Sie, ob Sie einen INNER JOIN mit einer konfigurierten Tabelle des Mitglieds benötigen, das abfragen kann.	Wenn Sie diesen Parameter aktivieren, INNER JOIN ist ein erforderlich. Wenn Sie diesen Parameter nicht aktivieren, INNER JOIN ist optional. Unter der Annahme, dass Sie diesen Parameter aktiviere n, muss das Mitglied, das abfragen kann, eine Tabelle, deren Eigentümer es ist, in die aufnehmenINNERJOIN. Sie müssen JOIN Ihre Tabelle mit ihren Tabellen direkt oder transitiv verbinden (d. h. ihre Tabelle mit einer anderen Tabelle verknüpfen, die selbst mit Ihrer Tabelle verbunden ist).

Im Folgenden finden Sie ein Beispiel für Transitivität.

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

> **Note**
>
> Das Mitglied, das abfragen kann, kann auch den -`joinRequired`Parameter verwenden. In diesem Fall muss die Abfrage ihre Tabelle mit mindestens einer anderen Tabelle verbinden.

Dimensionssteuerungen

Dimensionssteuerelemente steuern die Spalte, nach der die Aggregationsspalten gefiltert, gruppiert oder aggregiert werden können.

Kontrolle	Definition	Verwendung
`dimensionColumns`	Die Spalten (falls vorhanden), die Sie dem Mitglied erlauben, die abfragen könnenWHERE, in SELECT, GROUPBY, und zu verwendenORDERBY.	Ein `dimensionColumn` kann in SELECT (`select_grouping_column_expression`), WHEREGROUPBY, und verwendet werdenORDERBY. Die gleiche Spalte kann nicht sowohl ein `dimensionColumn` , ein `joinColumn` und/oder ein seinaggregateColumn .

Skalarfunktionen

Skalare Funktionen steuern, welche skalaren Funktionen für Dimensionsspalten verwendet werden können.

Kontrolle	Definition	Verwendung
`scalarFunctions`	Die skalaren Funktionen, die `dimensionColumns` in der	Gibt die skalaren Funktionen (falls vorhanden) an, die Sie zulassen (z. B. CAST), um auf angewende

Kontrolle	Definition	Verwendung
	Abfrage verwendet werden können.	t zu werden`dimension Columns` . Skalare Funktionen können nicht zusätzlich zu anderen Funktionen oder innerhalb anderer Funktionen verwendet werden. Argumente für skalare Funktionen können Spalten, Zeichenfolgeliterale oder numerische Literale sein.

Die folgenden skalaren Funktionen werden unterstützt:

- Mathematische Funktionen – ABS, CEILING, FLOOR, LOG, LN, ROUND, SQRT
- Funktionen zur Datentypformatierung – CAST, CONVERT, TO_CHAR, TO_DATE, TO_NUMBER, TO_TIMESTAMP
- Zeichenfolgenfunktionen – LOWER, UPPER, TRIM, RTRIM, SUBSTRING
  - Für RTRIM sind benutzerdefinierte Zeichensätze zum Kürzen nicht zulässig.
- Bedingte Ausdrücke – COALESCE
- Datumsfunktionen – EXTRACT, GETDATE, CURRENT_DATE, DATEADD
- Andere Funktionen – TRUNC

Weitere Informationen finden Sie in der AWS Clean Rooms SQL-Referenz .

Regel zur Aggregationsanalyse – Abfrageergebnissteuerelemente

Mit den Steuerelementen für Aggregationsabfrageergebnisse können Sie steuern, welche Ergebnisse zurückgegeben werden, indem Sie eine oder mehrere Bedingungen angeben, die jede Ausgabezeile erfüllen muss, damit sie zurückgegeben werden kann. AWS Clean Rooms unterstützt Aggregationseinschränkungen in Form von `COUNT (DISTINCT column) >= X`. Dieses Formular erfordert, dass jede Zeile mindestens X unterschiedliche Werte einer Auswahl aus Ihrer konfigurierten Tabelle aggregiert (z. B. eine Mindestanzahl unterschiedlicher `user_id` Werte). Dieser Mindestschwellenwert wird automatisch durchgesetzt, auch wenn die übermittelte Abfrage selbst

nicht die angegebene Spalte verwendet. Sie werden gemeinsam für jede konfigurierte Tabelle in der Abfrage aus den konfigurierten Tabellen jedes Mitglieds der Zusammenarbeit durchgesetzt.

Jede konfigurierte Tabelle muss mindestens eine Aggregationsbeschränkung in ihrer Analyseregel haben. Konfigurierte Tabellenbesitzer können mehrere `columnName` und zugehörige hinzufügen `minimum` und sie werden gemeinsam durchgesetzt.

Aggregationseinschränkungen

Aggregationseinschränkungen steuern, welche Zeilen in den Abfrageergebnissen zurückgegeben werden. Um zurückgegeben werden zu können, muss eine Zeile die angegebene Mindestanzahl unterschiedlicher Werte in jeder Spalte erfüllen, die in der Aggregationseinschränkung angegeben ist. Diese Anforderung gilt auch dann, wenn die Spalte nicht explizit in der Abfrage oder in anderen Teilen der Analyseregel erwähnt wird.

Kontrolle	Definition	Verwendung
`columnName`	Die `aggregateColumn` , die in der Bedingung verwendet wird, die jede Ausgabezeile erfüllen muss.	Kann eine beliebige Spalte in der konfigurierten Tabelle sein.
`minimum`	Die Mindestanzahl unterschiedlicher Werte für die zugehörige `aggregateColumn` , die die Ausgabezeile haben muss (z. B. COUNT DISTINCT), damit sie in den Abfrageergebnissen zurückgegeben wird.	Der `minimum` muss mindestens den Wert 2 haben.

Struktur der Regel für die Aggregationsanalyse

Das folgende Beispiel zeigt eine vordefinierte Struktur für eine Aggregationsanalyseregel.

Im folgenden Beispiel *`MyTable`* bezieht sich auf Ihre Datentabelle. Sie können jeden *`Platzhalter für Benutzereingaben`* durch Ihre eigenen Informationen ersetzen.

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

Aggregationsanalyseregel – Beispiel

Das folgende Beispiel zeigt, wie zwei Unternehmen AWS Clean Rooms mithilfe der Aggregationsanalyse zusammenarbeiten können.

Unternehmen A verfügt über Kunden- und Verkaufsdaten. Unternehmen A ist daran interessiert, die Produktrückgabeaktivität zu verstehen. Unternehmen B ist eines der Lebensmittel von Unternehmen A und hat Daten zurückgegeben. Unternehmen B verfügt auch über Segmentattribute für Kunden, die für Unternehmen A nützlich sind (z. B. bei dem Kauf verwandter Produkte wird der Kundenservice des Einzelhandels verwendet). Unternehmen B möchte keine Kundenrückgabedaten und Attributinformationen auf Zeilenebene bereitstellen. Unternehmen B möchte nur eine Reihe von Abfragen für Unternehmen A aktivieren, um aggregierte Statistiken zu überlappenden Kunden mit einem minimalen Aggregationsschwellenwert zu erhalten.

Unternehmen A und Unternehmen B entscheiden sich für eine Zusammenarbeit, damit Unternehmen A die Produktrückgabeaktivitäten verstehen und bessere Produkte in Unternehmen B und anderen Kanälen bereitstellen kann.

Um die Zusammenarbeit zu erstellen und eine Aggregationsanalyse durchzuführen, gehen die Unternehmen wie folgt vor:

1. Unternehmen A erstellt eine Zusammenarbeit und eine Mitgliedschaft. Die Zusammenarbeit hat Unternehmen B als weiteres Mitglied der Zusammenarbeit. Unternehmen A aktiviert die Abfrageprotokollierung in der Zusammenarbeit und die Abfrageprotokollierung in seinem Konto.

2. Unternehmen B erstellt eine Mitgliedschaft in der Zusammenarbeit. Es aktiviert die Abfrageprotokollierung in seinem Konto.
3. Unternehmen A erstellt eine vertriebskonfigurierte Tabelle.
4. Unternehmen A fügt die folgende Aggregationsanalyseregel zur Tabelle hinzu, die für den Verkauf konfiguriert ist.

```
{
  "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` – Unternehmen A möchte die Anzahl der eindeutigen Kunden in der Überschneidung zwischen Verkaufsdaten und Rückgabedaten zählen. Unternehmen A möchte auch die Anzahl der , die gemacht `purchases` wurden, summieren, um sie mit der Anzahl von zu vergleichen`returns`.

`joinColumns` – Unternehmen A möchte verwenden`identifier`, um Kunden aus Verkaufsdaten mit Kunden aus Rückgabedaten abzugleichen. Dies hilft Unternehmen A dabei, zu den richtigen Käufen zurückzukehren. Es hilft auch Unternehmen A, sich überschneidende Kunden zu segmentieren.

`dimensionColumns` – Unternehmen A verwendet , `dimensionColumns` um nach dem spezifischen Produkt zu filtern, Käufe und Rückgaben über einen bestimmten Zeitraum zu vergleichen, sicherzustellen, dass das Rückgabedatum nach dem Produktdatum liegt, und um überlappende Kunden zu segmentieren.

`scalarFunctions` – Unternehmen A wählt eine `CAST` skalare Funktion aus, um bei Bedarf Datentypformate basierend auf der konfigurierten Tabelle zu aktualisieren, die Unternehmen A der Zusammenarbeit zuordnet. Es fügt auch skalare Funktionen hinzu, um bei Bedarf die Formatierung von Spalten zu unterstützen.

`outputConstraints` – Unternehmen A legt Mindestausgabeeinschränkungen fest. Es muss die Ergebnisse nicht einschränken, da der Analyst Daten auf Zeilenebene aus seiner Verkaufstabelle sehen darf

> **Note**
>
> Unternehmen A nimmt nicht `joinRequired` in die Analyseregel auf. Sie bietet ihrem Analysten Flexibilität, die Verkaufstabelle allein abzufragen.

5. Unternehmen B erstellt eine rückgabekonfigurierte Tabelle.
6. Unternehmen B fügt der konfigurierten Rückgabetabelle die folgende Aggregationsanalyseregel hinzu.

```
{
  "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` – Unternehmen B ermöglicht es Unternehmen A, Summen vorzunehmen`returns`, um sie mit der Anzahl der Käufe zu vergleichen. Sie haben mindestens eine Aggregatspalte, da sie eine Aggregatabfrage aktivieren.

`joinColumns` – Unternehmen B ermöglicht es Unternehmen A, beizutreten`identifier`, um Kunden aus Rückgabedaten aus Verkaufsdaten mit Kunden zu verknüpfen. -`identifier`Daten sind besonders sensibel und stellen `joinColumn` sicher, dass die Daten niemals in einer Abfrage ausgegeben werden.

`joinRequired` – Unternehmen B verlangt, dass sich Abfragen der Rückgabedaten mit den Verkaufsdaten überschneiden. Sie möchten nicht Unternehmen A ermöglichen, alle Personen in ihrem Datensatz abzufragen. Sie haben sich auch in ihrer Zusammenarbeitsvereinbarung auf diese Einschränkung geeinigt.

`dimensionColumns` – Unternehmen B ermöglicht es Unternehmen A, nach `state`, und zu filtern und zu gruppierenpopularpurchases, `customerserviceuser` wobei es sich um eindeutige Attribute handelt, die dazu beitragen könnten, die Analyse für Unternehmen A durchzuführen. Unternehmen B ermöglicht Unternehmen A, zu verwenden`returndate`, um Ausgaben zu filtern`returndate`, die nach auftretenpurchasedate. Mit dieser Filterung ist die Ausgabe genauer, um die Auswirkungen der Produktänderung zu bewerten.

`scalarFunctions` – Unternehmen B ermöglicht Folgendes:

- TRUNC für Datumsangaben
- LOWER und UPPER, falls die in einem anderen Format in ihren Daten eingegeben `producttype` wird
- CAST wenn Unternehmen A Datentypen in Verkäufen konvertieren muss, damit sie den Datentypen in Rückgaben entsprechen

Unternehmen A aktiviert keine anderen skalaren Funktionen, da sie nicht glauben, dass sie für Abfragen erforderlich sind.

`outputConstraints` – Unternehmen B legt Mindestausgabeeinschränkungen für fest`hashedemail`, um die Fähigkeit zur Neuidentifizierung von Kunden zu verringern. Außerdem wird eine Mindestausgabeeinschränkung für hinzugefügt, `producttype` um die Möglichkeit zu verringern, bestimmte zurückgegebene Produkte neu zu identifizieren. Bestimmte Produkttypen könnten basierend auf den Dimensionen der Ausgabe dominanter sein (z. B. `state`). Ihre Ausgabeeinschränkungen werden immer durchgesetzt, unabhängig von den Ausgabeeinschränkungen, die Unternehmen A ihren Daten hinzugefügt hat.

7. Unternehmen A erstellt eine Zuordnung von Verkaufstabellen zur Zusammenarbeit.
8. Unternehmen B erstellt eine Zuordnung von Rückgabetabellen zur Zusammenarbeit.
9. Unternehmen A führt Abfragen wie das folgende Beispiel aus, um die Menge der Rückgaben in Unternehmen B besser zu verstehen als die Gesamtzahl der Käufe nach Standort im Jahr 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. Unternehmen A und Unternehmen B überprüfen Abfrageprotokolle. Unternehmen B überprüft, ob die Abfrage mit dem übereinstimmt, was in der Zusammenarbeitsvereinbarung vereinbarten wurde.

Beheben von Problemen mit Aggregationsanalyseregeln

Verwenden Sie die hier aufgeführten Informationen, um häufige Probleme zu diagnostizieren und zu beheben, wenn Sie mit Aggregationsanalyseregeln arbeiten.

Problembereiche

- Meine Abfrage hat keine Ergebnisse zurückgegeben

Meine Abfrage hat keine Ergebnisse zurückgegeben

Dies kann passieren, wenn es keine übereinstimmenden Ergebnisse gibt oder wenn die übereinstimmenden Ergebnisse nicht einen oder mehrere minimale Aggregationsschwellenwerte erreichen.

Weitere Informationen zu minimalen Aggregationsschwellenwerten finden Sie unter Aggregationsanalyseregel – Beispiel.

Analyseregel auflisten

In gibt eine Regel zur Listenanalyse Listen auf Zeilenebene ausAWS Clean Rooms, die sich zwischen der konfigurierten Tabelle, der sie hinzugefügt wird, und den konfigurierten Tabellen des Mitglieds, das sie abfragen kann, überschneiden. Das Mitglied, das Abfragen durchführen kann, führt Abfragen aus, die eine Listenanalyseregel enthalten.

Der Regeltyp Listenanalyse unterstützt Anwendungsfälle wie Anreicherung und Zielgruppenerstellung.

Weitere Informationen zur vordefinierten Abfragestruktur und Syntax für diese Analyseregel finden Sie unter Vordefinierte Struktur der Analyseregel auflisten.

Die Parameter der Regel zur Listenanalyse, definiert in Analyseregel auflisten – Abfragesteuerungen, haben Abfragesteuerelemente. Zu seinen Abfragesteuerungen gehört die Möglichkeit, die Spalten auszuwählen, die in der Ausgabe aufgeführt werden können. Die Abfrage muss mindestens einen Join mit einer konfigurierten Tabelle des Mitglieds haben, das Abfragen direkt oder transitiv durchführen kann.

Es gibt keine Steuerelemente für Abfrageergebnisse wie für die Aggregationsanalyseregel .

Listenabfragen können nur mathematische Operatoren verwenden. Sie können keine anderen Funktionen (wie Aggregation oder Skalar) verwenden.

Themen

- Auflisten der Abfragestruktur und -syntax
- Analyseregel auflisten – Abfragesteuerungen
- Vordefinierte Struktur der Analyseregel auflisten

- Analyseregel auflisten – Beispiel

Auflisten der Abfragestruktur und -syntax

Abfragen für Tabellen, die eine Regel zur Listenanalyse haben, müssen der folgenden Syntax entsprechen.

```
--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]
```

In der folgenden Tabelle wird jeder Ausdruck erläutert, der in der vorherigen Syntax aufgeführt ist.

Expression	Definition	Beispiele
select_list_expression	Eine durch Komma getrennte Liste, die mindestens einen Tabellenspaltennamen enthält. Ein `DISTINCT` Parameter ist erforderlich. **Note** Der `select_list_expression` kann Spalten mit oder ohne den `AS`	`SELECT DISTINCT segment`

Expression	Definition	Beispiele
	Parameter als Alias verwenden. Es unterstützt auch den -T0PParameter. Weitere Informationen finden Sie in der AWS Clean Rooms SQL-Referenz .	
table_expression	Eine Tabelle oder ein Join von Tabellen mit , `join_condition` um sie mit zu verbinden`join_condition` . `join_condition` gibt einen booleschen Wert zurück. Die `table_expression` unterstützt: • Ein bestimmter JOIN-Typ (INNER JOIN) • Die Gleichheitsverglei chsbedingungen innerhalb einer `join_condition` (=) • Logische Operatoren (AND, OR).	`FROM consumer_table INNER JOIN provider_ table ON consumer_table.ide ntifier1 = provider_ table.identifier1 AND consumer_table .identifier2 = provider_table.ide ntifier2`

Expression	Definition	Beispiele

where_expression	Ein bedingter Ausdruck, der einen booleschen Wert zurückgibt. Es kann aus folgenden Komponenten bestehen:
	• Tabellenspaltennamen
	• Mathematische Operatoren
	• Zeichenfolgeliterale
	• Numerische Literale
	
	Unterstützte Vergleich sbedingungen sind (`=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL`).
	
	Unterstützte logische Operatoren sind (`AND, OR`).
	
	Die `where_expression` ist optional.
		`WHERE state + '_' + city = 'NY_NYC'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

limit_expression	Dieser Ausdruck muss eine positive Ganzzahl annehmen. Es kann auch mit einem TOP-Parameter ausgetauscht werden. Die `limit_expression` ist optional.	`LIMIT 100`

Beachten Sie bei der Struktur und Syntax von Listenabfragen Folgendes:

- Andere SQL-Befehle als SELECT werden nicht unterstützt.

- Unterabfragen und allgemeine Tabellenausdrücke (z. B. WITH) werden nicht unterstützt
- HAVING-BY, GROUP - und ORDER-BYKlauseln werden nicht unterstützt
- Der Parameter OFFSET wird nicht unterstützt

Analyseregel auflisten – Abfragesteuerungen

Mit den Steuerelementen zum Auflisten von Abfragen können Sie steuern, wie die Spalten in Ihrer Tabelle zum Abfragen der Tabelle verwendet werden. Sie können beispielsweise steuern, welche Spalte für die Verknüpfung verwendet wird oder welche Spalte in der SELECT-Anweisung und -WHEREKlausel verwendet werden kann.

In den folgenden Abschnitten werden die einzelnen Kontrollen erläutert.

Themen

Join-Steuerelemente

Mit Join-Steuerelementen können Sie steuern, wie Ihre Tabelle mit anderen Tabellen im table_expression verbunden werden kann. unterstützt AWS Clean Rooms nur INNER JOIN. In der Regel zur Listenanalyse ist mindestens eine INNER JOIN erforderlich und das Mitglied, das die Abfrage durchführen kann, muss eine Tabelle, deren Eigentümer sie sind, in die INNER JOIN aufnehmen. Das bedeutet, dass sie Ihrer Tabelle entweder direkt oder transitiv beitreten müssen.

Im Folgenden finden Sie ein Beispiel für Transitivität.

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

INNER JOIN-Anweisungen können nur Spalten verwenden, die `joinColumn` in Ihrer Analyseregel explizit als kategorisiert wurden.

Die INNER JOIN muss für eine `joinColumn` aus Ihrer konfigurierten Tabelle und für eine `joinColumn` aus einer anderen konfigurierten Tabelle in der Zusammenarbeit ausgeführt werden. Sie entscheiden, welche Spalten aus Ihrer Tabelle als verwendet werden können`joinColumn`.

Jede Übereinstimmungsbedingung innerhalb der -ONKlausel ist erforderlich, um die Gleichheitsvergleichsbedingung (=) zwischen zwei Spalten zu verwenden.

Mehrere Übereinstimmungsbedingungen innerhalb einer -ONKlausel können sein:

- Kombiniert mit dem `AND` logischen Operator
- Getrennt mit dem `OR` logischen Operator

> **Note**
>
> Alle JOIN Übereinstimmungsbedingungen müssen mit einer Zeile von jeder Seite des übereinstimmenJOIN. Alle Bedingungen, die durch einen `OR` oder einen `AND` logischen Operator verbunden sind, müssen ebenfalls diese Anforderung erfüllen.

Im Folgenden finden Sie ein Beispiel für eine Abfrage mit einem `AND` logischen Operator.

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

Im Folgenden finden Sie ein Beispiel für eine Abfrage mit einem `OR` logischen Operator.

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

Kontrolle	Definition	Verwendung
`joinColumns`	Die Spalten, die das Mitglied abfragen kann, um es in der	Die gleiche Spalte kann nicht sowohl als als auch als kategorisiert werden

Kontrolle	Definition	Verwendung
	INNER JOIN-Anweisung zu verwenden.	`joinColumn` `listColumn` (siehe Auflisten von Kontrollen). `joinColumn` kann nur in INNER JOIN verwendet werden.

Auflisten von Kontrollen

Listensteuerelemente steuern die Spalten, die in der Abfrageausgabe aufgelistet (d. h. in der SELECT-Anweisung verwendet) oder zum Filtern von Ergebnissen verwendet werden können (d. h. in der WHERE Anweisung verwendet).

Kontrolle	Definition	Verwendung
`listColumns`	Die Spalten, die das Mitglied abfragen kann, um in SELECT und zu verwenden WHERE	Ein `listColumn` kann in SELECT und verwendet werdenWHERE. Die gleiche Spalte kann nicht als `listColumn` und verwendet werden`joinColumn` .

Vordefinierte Struktur der Analyseregel auflisten

Das folgende Beispiel enthält eine vordefinierte Struktur, die zeigt, wie Sie eine Listenanalyseregel abschließen.

Im folgenden Beispiel *`MyTable`* bezieht sich auf Ihre Datentabelle. Sie können jeden *`Platzhalter für Benutzereingaben`* durch Ihre eigenen Informationen ersetzen.

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

```
}
```

Analyseregel auflisten – Beispiel

Das folgende Beispiel zeigt, wie zwei Unternehmen AWS Clean Rooms mithilfe der Listenanalyse zusammenarbeiten können.

Unternehmen A verfügt über CRM-Daten (Customer Relationship Management). Unternehmen A möchte zusätzliche Segmentdaten zu seinen Kunden abrufen, um mehr über ihre Kunden zu erfahren und möglicherweise Attribute als Eingabe für andere Analysen zu verwenden. Unternehmen B verfügt über Segmentdaten, die aus eindeutigen Segmentattributen bestehen, die es auf der Grundlage seiner Daten der ersten Partei erstellt hat. Unternehmen B möchte die eindeutigen Segmentattribute nur für Kunden bereitstellen, die sich zwischen ihren Daten und den Daten von Unternehmen A überschneiden.

Die Unternehmen entscheiden sich für eine Zusammenarbeit, damit Unternehmen A die überlappenden Daten anreichern kann. Unternehmen A ist das Mitglied, das Abfragen durchführen kann, und Unternehmen B ist der Mitwirkende.

Um eine Zusammenarbeit zu erstellen und eine Listenanalyse in Zusammenarbeit durchzuführen, gehen die Unternehmen wie folgt vor:

1. Unternehmen A erstellt eine Zusammenarbeit und eine Mitgliedschaft. Die Zusammenarbeit hat Unternehmen B als weiteres Mitglied der Zusammenarbeit. Unternehmen A aktiviert die Abfrageprotokollierung in der Zusammenarbeit und die Abfrageprotokollierung in seinem Konto.
2. Unternehmen B erstellt eine Mitgliedschaft in der Zusammenarbeit. Es aktiviert die Abfrageprotokollierung in seinem Konto.
3. Unternehmen A erstellt eine CRM-konfigurierte Tabelle
4. Unternehmen A fügt die Analyseregel der vom Kunden konfigurierten Tabelle hinzu, wie im folgenden Beispiel gezeigt.

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

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

`joinColumns` – Unternehmen A möchte `hashedemail` und/oder `thirdpartyid` (von einem Identitätsanbieter bezogen) verwenden, um Kunden aus CRM-Daten mit Kunden aus Segmentdaten abzugleichen. Dadurch wird sichergestellt, dass Unternehmen A mit den anreicherten Daten für die richtigen Kunden übereinstimmt. Sie verfügen über zwei joinColumns, um die Übereinstimmungsrate der Analyse möglicherweise zu verbessern.

`listColumns` – Unternehmen A verwendet `listColumns`, um anreicherte Spalten neben einem abzurufen, den `internalid` sie in ihren eigenen Systemen verwenden. Sie fügen `segment1`, und hinzu`segment2`, `customercategory` um die Anreicherung möglicherweise auf bestimmte Segmente zu beschränken, indem sie sie in Filtern verwenden.

5. Unternehmen B erstellt eine segmentkonfigurierte Tabelle.
6. Unternehmen B fügt die Analyseregel der segmentkonfigurierten Tabelle hinzu.

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

`joinColumns` – Unternehmen B ermöglicht es Unternehmen A, sich bei anzumeldenidentifier2, um Kunden aus Segmentdaten mit CRM-Daten abzugleichen. Unternehmen A und Unternehmen B haben mit dem Identitätsanbieter zusammengearbeitetidentifier2, um die für diese Zusammenarbeit passenden zu erhalten. Sie haben keine anderen hinzugefügt, `joinColumns` da sie glauben, dass sie die höchste und genaueste Übereinstimmungsrate `identifier2` bieten und andere Kennungen für die Abfragen nicht erforderlich sind.

`listColumns` – Unternehmen B ermöglicht es Unternehmen A, seine Daten mit - `segment3` und -`segment4`Attributen zu ergänzen, bei denen es sich um eindeutige Attribute handelt, die sie (mit Kunde A) erstellt, gesammelt und abgestimmt haben, um Teil der Datenanreicherung zu sein. Sie

möchten, dass Unternehmen A diese Segmente für die Überlappung auf Zeilenebene erhält, da dies eine Zusammenarbeit zur Datenanreicherung ist.

7. Unternehmen A erstellt eine CRM-Tabellenzuordnung zur Zusammenarbeit.
8. Unternehmen B erstellt eine Segmenttabellenzuordnung zur Zusammenarbeit.
9. Unternehmen A führt Abfragen wie die folgenden aus, um überlappende Kundendaten zu ergänzen.

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

10. Unternehmen A und Unternehmen B überprüfen Abfrageprotokolle. Unternehmen B überprüft, ob die Abfrage mit dem übereinstimmt, was in der Zusammenarbeitsvereinbarung vereinbarten wurde.

Benutzerdefinierte Analyseregel in AWS Clean Rooms

In AWS Clean Rooms ist eine benutzerdefinierte Analyseregel ein neuer Typ von Analyseregel, mit dem benutzerdefinierte Abfragen für die konfigurierte Tabelle ausgeführt werden können. Benutzerdefinierte SQL-Abfragen sind weiterhin darauf beschränkt, nur den SELECT Befehl zu verwenden, können aber mehr SQL-Konstrukte als Aggregations - und Listenabfragen verwenden (z. B. Fensterfunktionen, OUTER JOIN, CTEs oder Unterabfragen; eine vollständige Liste finden Sie in der AWS Clean Rooms SQL-Referenz). Benutzerdefinierte SQL-Abfragen müssen nicht wie Aggregations - und Listenabfragen einer Abfragestruktur folgen.

Die benutzerdefinierte Analyseregel unterstützt komplexere Anwendungsfälle als solche, die von der Aggregations- und Listenanalyseregel unterstützt werden können, z. B. benutzerdefinierte Attributionsanalysen, Benchmarking, Inkrementalitätsanalysen und Zielgruppenerkennung. Dies gilt zusätzlich zu einer Vielzahl von Anwendungsfällen, die von der Aggregations- und Listenanalyseregel unterstützt werden.

Die benutzerdefinierte Analyseregel unterstützt auch den differenziellen Datenschutz. Differential Privacy ist ein mathematisch strenges Rahmenwerk für den Datenschutz. Weitere Informationen finden Sie unter AWS Clean Rooms Differenzierter Datenschutz. Wenn Sie eine Analysevorlage erstellen, überprüft AWS Clean Rooms Differential Privacy die Vorlage, um festzustellen, ob sie mit der allgemeinen Abfragestruktur für Differential Privacy kompatibel ist. AWS Clean Rooms Durch

diese Überprüfung wird sichergestellt, dass Sie keine Analysevorlage erstellen, die in einer durch Differential Privacy geschützten Tabelle nicht zulässig ist.

Um die benutzerdefinierte Analyseregel zu konfigurieren, können Datenbesitzer festlegen, dass bestimmte benutzerdefinierte Abfragen, die in Analysevorlagen gespeichert sind, für ihre konfigurierten Tabellen ausgeführt werden. Datenbesitzer überprüfen Analysevorlagen, bevor sie sie der zulässigen Analysesteuerung in der benutzerdefinierten Analyseregel hinzufügen. Analysevorlagen sind nur in der Kollaboration verfügbar und sichtbar, in der sie erstellt wurden (auch wenn die Tabelle mit anderen Kollaborationen verknüpft ist). Sie können nur von dem Mitglied ausgeführt werden, das in dieser Kollaboration Abfragen durchführen kann.

Alternativ können sich Mitglieder dafür entscheiden, anderen Mitgliedern (Abfrageanbietern) zu gestatten, Abfragen ohne Überprüfung zu erstellen. Mitglieder fügen in der benutzerdefinierten Analyseregel Konten von Abfrageanbietern hinzu, die über die zulässigen Abfrageanbieter verfügen. Wenn der Abfrageanbieter das Mitglied ist, das Abfragen durchführen kann, könnten sie jede Abfrage direkt in der konfigurierten Tabelle ausführen. Abfrageanbieter könnten Abfragen auch erstellen, indem sie Analysevorlagen erstellen. Alle Abfragen, die von den Abfrageanbietern erstellt wurden, dürfen automatisch für die Tabelle in allen Kollaborationen ausgeführt werden, in denen die AWS-Konto vorhanden und die Tabelle verknüpft ist.

Datenbesitzer können nur Analysevorlagen oder Konten erlauben, Abfragen zu erstellen, nicht beides. Wenn der Datenbesitzer dieses Feld leer lässt, kann das Mitglied, das Abfragen durchführen kann, keine Abfragen für die konfigurierte Tabelle ausführen.

Themen

Benutzerdefinierte Analyseregel, vordefinierte Struktur

Das folgende Beispiel enthält eine vordefinierte Struktur, die zeigt, wie Sie eine benutzerdefinierte Analyseregel mit aktiviertem differenziellen Datenschutz abschließen. Der `userIdentifier` Wert ist die Spalte, die Ihre Benutzer eindeutig identifiziert, z. B. user_id. Wenn Sie in einer Kollaboration zwei oder mehr Tabellen mit aktiviertem differenziellen Datenschutz haben, AWS Clean Rooms müssen Sie in beiden Analyseregeln dieselbe Spalte wie die Benutzer-ID-Spalte konfigurieren, um eine konsistente Definition der Benutzer in allen Tabellen aufrechtzuerhalten.

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

Führen Sie dazu einen der folgenden Schritte aus:

- Fügen Sie ARNs für Analysevorlagen zur Steuerung der zulässigen Analysen hinzu. In diesem Fall ist das `allowedAnalysisProviders` Steuerelement nicht enthalten.

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

- Fügen Sie dem `allowedAnalysisProviders` Steuerelement AWS-Konto Mitglieds-IDs hinzu. In diesem Fall fügen Sie dem `allowedAnalyses` Steuerelement etwas `ANY_QUERY` hinzu.

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

Beispiel für eine benutzerdefinierte Analyseregel

Das folgende Beispiel zeigt, wie zwei Unternehmen AWS Clean Rooms mithilfe der benutzerdefinierten Analyseregel zusammenarbeiten können.

Unternehmen A verfügt über Kunden- und Vertriebsdaten. Unternehmen A ist daran interessiert, die Umsatzsteigerung einer Werbekampagne auf der Website von Unternehmen B zu verstehen. Unternehmen B verfügt über Zuschauerdaten und Segmentattribute, die für Unternehmen nützlich sind (z. B. das Gerät, mit dem sie sich die Werbung angesehen haben).

Unternehmen A hat eine spezielle Inkrementalitätsabfrage, die im Rahmen der Zusammenarbeit ausgeführt werden soll.

Um eine Zusammenarbeit zu erstellen und gemeinsam eine benutzerdefinierte Analyse durchzuführen, gehen die Unternehmen wie folgt vor:

1. Unternehmen A erstellt eine Kollaboration und erstellt eine Mitgliedschaft. Die Kollaboration hat Firma B als weiteres Mitglied der Kollaboration. Unternehmen A aktiviert die Abfrageprotokollierung in der Kollaboration und sie aktiviert die Abfrageprotokollierung in ihrem Konto.
2. Unternehmen B erstellt eine Mitgliedschaft in der Kollaboration. Es aktiviert die Abfrageprotokollierung in seinem Konto.
3. Firma A erstellt eine für CRM konfigurierte Tabelle
4. Unternehmen A fügt der für den Vertrieb konfigurierten Tabelle eine leere benutzerdefinierte Analyseregel hinzu.
5. Firma A ordnet der Kollaboration eine für den Vertrieb konfigurierte Tabelle zu.
6. Unternehmen B erstellt eine für die Zuschauerzahl konfigurierte Tabelle.
7. Unternehmen B fügt der für die Zuschauerzahl konfigurierten Tabelle eine leere benutzerdefinierte Analyseregel hinzu.
8. Unternehmen B ordnet der Kollaboration eine für die Zuschauerzahl konfigurierte Tabelle zu.
9. Unternehmen A zeigt die der Kollaboration zugeordnete Verkaufstabelle und die Tabelle mit den Zuschauerzahlen an und erstellt eine Analysevorlage, in der die Inkrementalitätsabfrage und der Parameter für den Kampagnenmonat hinzugefügt werden.

```
{
    "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. Unternehmen A fügt sein Konto (z. B. 444455556666) zur Steuerung des zulässigen Analyseanbieters in der benutzerdefinierten Analyseregel hinzu. Sie verwenden das Steuerelement für zugelassene Analyseanbieter, weil sie zulassen möchten, dass alle von ihnen erstellten Abfragen in ihrer für den Vertrieb konfigurierten Tabelle ausgeführt werden.

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

11. Unternehmen B sieht die erstellte Analysevorlage in der Kollaboration und überprüft ihren Inhalt, einschließlich der Abfragezeichenfolge und des Parameters.

12. Unternehmen B stellt fest, dass die Analysevorlage den Anwendungsfall Inkrementalität erfüllt und die Datenschutzanforderungen hinsichtlich der Art und Weise, wie die für die Zuschauerzahl konfigurierte Tabelle abgefragt werden kann, erfüllt.

13. Unternehmen B fügt den ARN der Analysevorlage zur zulässigen Analysesteuerung in der benutzerdefinierten Analyseregel der Zuschauerschaftstabelle hinzu. Sie verwenden das zulässige Analysesteuerelement, weil sie nur zulassen möchten, dass die Inkrementalitätsabfrage für ihre für die Zuschauerzahl konfigurierte Tabelle ausgeführt wird.

```
{
```

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

14. Unternehmen A führt die Analysevorlage aus und verwendet den Parameterwert. `05-01-2023`

Benutzerdefinierte Analyseregel mit differenziellem Datenschutz

In AWS Clean Rooms, die benutzerdefinierte Analyseregel unterstützt differenziellen Datenschutz. Differential Privacy ist ein mathematisch strenger Rahmen für den Datenschutz, der Ihnen hilft, Ihre Daten vor Reidentifikationsversuchen zu schützen.

Differential Privacy unterstützt aggregierte Analysen wie die Planung und post-ad-campaign Messung von Werbekampagnen, Benchmarking in einem Konsortium von Finanzinstituten und A/B-Tests für die Gesundheitsforschung.

Die unterstützte Abfragestruktur und Syntax sind in definiert. Struktur und Syntax der Abfrage

Beispiel für eine benutzerdefinierte Analyseregel mit differenziertem Datenschutz

Sehen Sie sich das Beispiel für eine benutzerdefinierte Analyseregel an, das im vorherigen Abschnitt vorgestellt wurde. Dieses Beispiel zeigt, wie Sie Differential Privacy nutzen können, um Ihre Daten vor Reidentifikationsversuchen zu schützen und gleichzeitig Ihrem Partner die Möglichkeit zu geben, geschäftskritische Erkenntnisse aus Ihren Daten zu gewinnen. Gehen Sie davon aus, dass Unternehmen B, das über die Zuschauerdaten verfügt, seine Daten mithilfe von Differential Privacy schützen möchte. Um die Einrichtung des differenzierten Datenschutzes abzuschließen, führt Unternehmen B die folgenden Schritte durch:

1. Unternehmen B aktiviert den differenziellen Datenschutz und fügt gleichzeitig eine benutzerdefinierte Analyseregel zur konfigurierten Tabelle für die Zuschauerzahl hinzu. Unternehmen B wählt diese `viewershipdata.hashedemail` Spalte als Benutzer-ID aus.
2. Unternehmen B fügt der Zusammenarbeit eine differenzierte Datenschutzrichtlinie hinzu, um die Tabelle mit den Zuschauerzahlen für Abfragen verfügbar zu machen. Unternehmen B wählt die Standardrichtlinie aus, um die Einrichtung schnell abzuschließen.

Unternehmen A, das die Umsatzsteigerung einer Werbekampagne auf der Website von Unternehmen B verstehen möchte, führt die Analysevorlage aus. Da die Abfrage mit der allgemeinen

Abfragestruktur von AWS Clean Rooms Differential Privacy kompatibel ist, wird die Abfrage erfolgreich ausgeführt.

Struktur und Syntax der Abfrage

Abfragen, die mindestens eine Tabelle enthalten, für die Differential Privacy aktiviert ist, müssen der folgenden Syntax entsprechen.

```
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**
>
> Beachten Sie bei der Struktur und Syntax von Differential Privacy Abfragen Folgendes:
>
> - Unterabfragen werden nicht unterstützt.
> - Common Table Expressions (CTEs) sollten die Benutzer-ID-Spalte ausgeben, wenn eine Tabelle oder ein CTE Daten enthält, die durch Differential Privacy geschützt sind. Filter, Gruppierungen und Aggregationen sollten auf Benutzerebene vorgenommen werden.
> - Final_Select ermöglicht die Aggregatfunktionen COUNT DISTINCT, COUNT, SUM, AVG und STDDEV.

Weitere Informationen darüber, welche SQL-Schlüsselwörter für Differential Privacy unterstützt werden, finden Sie unter. SQL-Funktionen von AWS Clean Rooms Differential Privacy

AWS Clean Rooms Differenzierter Datenschutz

AWS Clean Rooms Differential Privacy hilft Ihnen dabei, die Privatsphäre Ihrer Benutzer mit einer mathematisch gestützten Technik zu schützen, die mit intuitiven Steuerungen mit wenigen Klicks implementiert wird. Da es sich um eine vollständig verwaltete Funktion handelt, sind keine vorherigen Erfahrungen mit differenziertem Datenschutz erforderlich, um die erneute Identifizierung Ihrer Benutzer zu verhindern. AWS Clean Rooms fügt den Abfrageergebnissen zur Laufzeit automatisch eine sorgfältig kalibrierte Menge an Rauschen hinzu, um Ihre Daten auf individueller Ebene zu schützen.

AWS Clean Rooms Differential Privacy unterstützt eine Vielzahl analytischer Abfragen und eignet sich für eine Vielzahl von Anwendungsfällen, bei denen ein geringfügiger Fehler in den Abfrageergebnissen die Nützlichkeit Ihrer Analyse nicht beeinträchtigt. Damit können Ihre Partner geschäftskritische Erkenntnisse über Werbekampagnen, Investitionsentscheidungen, klinische Studien und mehr gewinnen, ohne dass Ihre Partner zusätzliche Einstellungen vornehmen müssen.

AWS Clean Rooms Differential Privacy schützt vor Überlauffehlern oder ungültigen Umwandlungsfehlern, bei denen Skalarfunktionen oder mathematische Operatorsymbole auf böswillige Weise verwendet werden.

Weitere Informationen zu AWS Clean Rooms Differential Privacy finden Sie in den folgenden Themen.

Themen

Differentieller Datenschutz

Differenzierter Datenschutz ermöglicht nur aggregierte Erkenntnisse und verschleiert den Beitrag der Daten einer Person zu diesen Erkenntnissen. Differentieller Datenschutz schützt die

Kooperationsdaten vor dem Mitglied, das Ergebnisse erhalten kann, wenn es mehr über eine bestimmte Person erfährt. Ohne Differential Privacy kann das Mitglied, das Ergebnisse erhalten kann, versuchen, individuelle Benutzerdaten abzuleiten, indem es Datensätze über eine Person hinzufügt oder entfernt und die Unterschiede bei den Abfrageergebnissen beobachtet.

Wenn die Option „Differenzierter Datenschutz“ aktiviert ist, wird den Abfrageergebnissen eine bestimmte Menge an Rauschen hinzugefügt, um den Beitrag einzelner Benutzer zu verschleiern. Wenn das Mitglied, das Ergebnisse erhalten kann, versucht, den Unterschied in den Abfrageergebnissen zu beobachten, nachdem es Datensätze über eine Person aus seinem Datensatz entfernt hat, verhindert die Variabilität des Abfrageergebnisses, dass die Daten der Person identifiziert werden können. AWS Clean Rooms Differential Privacy verwendet den SampCertSampler, eine bewährte Correct-Sampler-Implementierung, die von entwickelt wurde. AWS

So funktioniert Differential Privacy AWS Clean Rooms

Der Workflow zur Aktivierung des differenziellen AWS Clean Rooms Datenschutzes in erfordert die folgenden zusätzlichen Schritte, wenn der Workflow abgeschlossen wird für AWS Clean Rooms:

1. Sie aktivieren den differenziellen Datenschutz, wenn Sie eine benutzerdefinierte Analyseregel hinzufügen.
2. Sie konfigurieren die differenzielle Datenschutzrichtlinie für die Zusammenarbeit, um Ihre Datentabellen, die mit differentiellem Datenschutz geschützt sind, für Abfragen verfügbar zu machen.

Nachdem Sie diese Schritte abgeschlossen haben, kann das Mitglied, das Abfragen durchführen kann, Abfragen für durch Differential Privacy geschützte Daten ausführen. AWS Clean Rooms gibt Ergebnisse zurück, die der differenziellen Datenschutzrichtlinie entsprechen. AWS Clean Rooms Differential Privacy verfolgt die geschätzte Anzahl der verbleibenden Abfragen, die Sie ausführen können, ähnlich der Tankanzeige in einem Auto, die Ihnen den aktuellen Kraftstoffstand des Fahrzeugs anzeigt. Die Anzahl der Abfragen, die ein Mitglied, das Abfragen durchführen kann, ist durch das Datenschutzbudget und die in der festgelegten Parameter für die Anzahl der pro Abfrage hinzugefügten Störungen begrenztDifferenzielle Datenschutzrichtlinie.

Überlegungen

Beachten Sie bei der Verwendung von Differential Privacy in AWS Clean Rooms Folgendes:

- Das Mitglied, das Ergebnisse erhalten kann, kann Differential Privacy nicht verwenden. Sie konfigurieren eine benutzerdefinierte Analyseregel mit deaktiviertem Differential Privacy für ihre konfigurierten Tabellen.
- Das Mitglied, das Abfragen durchführen kann, kann keine Tabellen von zwei oder mehr Datenanbietern verknüpfen, wenn für beide der differenzielle Datenschutz aktiviert ist.

Differenzielle Datenschutzrichtlinie

Die differenzielle Datenschutzrichtlinie legt fest, wie viele Aggregationsfunktionen das Mitglied, das Abfragen durchführen kann, in einer Kollaboration ausführen darf. Das Datenschutzbudget definiert eine gemeinsame, begrenzte Ressource, die auf alle Tabellen in einer Kollaboration angewendet wird. Das pro Abfrage hinzugefügte Rauschen bestimmt die Geschwindigkeit, mit der das Datenschutzbudget aufgebraucht wird.

Eine differenzielle Datenschutzrichtlinie ist erforderlich, um Ihre durch Differentialdatenschutz geschützten Tabellen für Abfragen verfügbar zu machen. Dies ist ein einmaliger Schritt in einer Zusammenarbeit und umfasst zwei Eingaben:

- Datenschutzbudget — In Epsilon ausgedrückt, bestimmt das Datenschutzbudget das Datenschutzniveau. Es handelt sich um eine gemeinsame, begrenzte Ressource, die für all Ihre Tabellen verwendet wird, die in der Zusammenarbeit mit unterschiedlichem Datenschutz geschützt sind, da das Ziel darin besteht, die Privatsphäre Ihrer Benutzer zu schützen, deren Informationen in mehreren Tabellen vorhanden sein können.

  Das Datenschutzbudget wird jedes Mal aufgebraucht, wenn eine Abfrage an Ihren Tabellen ausgeführt wird. Wenn das Datenschutzbudget vollständig aufgebraucht ist, kann das Collaboration-Mitglied, das Abfragen durchführen kann, keine weiteren Abfragen ausführen, bis es erhöht oder aktualisiert wird. Durch die Festlegung eines höheren Datenschutzbudgets kann das Mitglied, das Ergebnisse erhalten kann, seine Unsicherheit über die einzelnen Personen in den Daten verringern. Wählen Sie nach Rücksprache mit Geschäftsträgern ein Datenschutzbudget, das Ihre Anforderungen an die Zusammenarbeit mit Ihren Datenschutzanforderungen in Einklang bringt.

  Sie können die Option Datenschutzbudget monatlich aktualisieren auswählen, um jeden Kalendermonat automatisch ein neues Datenschutzbudget zu erstellen, wenn Sie planen, regelmäßig neue Daten in die Zusammenarbeit einzubeziehen. Wenn Sie diese Option wählen, können beliebig viele Informationen über Datenzeilen angezeigt werden, wenn diese bei

Aktualisierungen wiederholt abgefragt werden. Vermeiden Sie diese Option, wenn dieselben Zeilen zwischen Aktualisierungen des Datenschutzbudgets wiederholt abgefragt werden.

- Das pro Anfrage hinzugefügte Rauschen wird anhand der Anzahl der Nutzer gemessen, deren Beiträge Sie unkenntlich machen möchten. Dieser Wert bestimmt, wie schnell das Datenschutzbudget aufgebraucht wird. Ein höherer Rauschwert verringert die Geschwindigkeit, mit der das Datenschutzbudget aufgebraucht wird, und ermöglicht somit, dass mehr Abfragen mit Ihren Daten ausgeführt werden können. Dies sollte jedoch gegen die Veröffentlichung weniger genauer Dateneinblicke abgewogen werden. Berücksichtigen Sie bei der Festlegung dieses Werts die gewünschte Genauigkeit für Erkenntnisse aus der Zusammenarbeit.

Sie können die standardmäßige differenzielle Datenschutzrichtlinie verwenden, um die Einrichtung schnell abzuschließen, oder Ihre differenzielle Datenschutzrichtlinie an Ihren Anwendungsfall anpassen. AWS Clean Rooms Differential Privacy bietet intuitive Steuerelemente zur Konfiguration der Richtlinie. AWS Clean Rooms Mit Differential Privacy können Sie eine Vorschau des Dienstprogramms im Hinblick auf die Anzahl der möglichen Aggregationen für alle Abfragen Ihrer Daten anzeigen und abschätzen, wie viele Abfragen in einer Datenzusammenarbeit ausgeführt werden können.

Anhand der interaktiven Beispiele können Sie sich ein Bild davon machen, wie sich unterschiedliche Werte für Privacy Budget und Noise, die pro Abfrage hinzugefügt werden, auf die Ergebnisse verschiedener Typen von SQL-Abfragen auswirken würden. Im Allgemeinen müssen Sie Ihre Datenschutzanforderungen mit der Anzahl der Abfragen, die Sie zulassen möchten, und der Genauigkeit dieser Abfragen abwägen. Ein kleineres Datenschutzbudget oder mehr Rauschen pro Anfrage können die Privatsphäre der Nutzer besser schützen, bieten Ihren Kooperationspartnern aber weniger aussagekräftige Erkenntnisse.

Wenn Sie das Datenschutzbudget erhöhen und gleichzeitig den Parameter „Pro Abfrage hinzugefügtes Rauschen“ beibehalten, kann das Mitglied, das Abfragen durchführen kann, mehr Aggregationen für Ihre Tabellen in der Kollaboration ausführen. Sie können das Datenschutzbudget jederzeit während der Zusammenarbeit erhöhen. Wenn Sie das Datenschutzbudget verringern und gleichzeitig den Parameter „Pro Abfrage hinzugefügtes Rauschen“ beibehalten, kann das Mitglied, das Abfragen durchführen kann, weniger Aggregationen ausführen. Sie können das Datenschutzbudget nicht verringern, nachdem das Mitglied, das Abfragen durchführen kann, mit der Analyse Ihrer Daten begonnen hat.

Wenn Sie die Anzahl der pro Abfrage hinzugefügten Störungen erhöhen und gleichzeitig die Eingabe für das Datenschutzbudget beibehalten, kann das Mitglied, das Abfragen durchführen kann, mehr

Aggregationen für Ihre Tabellen in der Kollaboration ausführen. Wenn Sie die Anzahl der pro Abfrage hinzugefügten Störungen verringern und gleichzeitig die Eingabe für das Datenschutzbudget beibehalten, kann das Mitglied, das Abfragen durchführen kann, weniger Aggregationen ausführen. Sie können das pro Abfrage hinzugefügte Rauschen jederzeit während der Zusammenarbeit erhöhen oder verringern.

Die differenzierte Datenschutzrichtlinie wird durch die API-Aktionen für die Vorlage „Datenschutzbudget“ verwaltet.

SQL-Funktionen von AWS Clean Rooms Differential Privacy

AWS Clean Rooms Differential Privacy verwendet eine allgemeine Abfragestruktur zur Unterstützung komplexer SQL-Abfragen. Benutzerdefinierte Analysevorlagen werden anhand dieser Struktur validiert, um sicherzustellen, dass sie auf Tabellen ausgeführt werden können, die durch Differential Privacy geschützt sind. Die folgende Tabelle zeigt, welche Funktionen unterstützt werden. Weitere Informationen finden Sie unter Struktur und Syntax der Abfrage.

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Aggregationsfunktionen	• Funktion ANY_VALUE • Die Funktion APPROXIMATE PERCENTILE_DISC • Die Funktion AVG • Die Funktionen COUNT und COUNT DISTINCT • Die Funktion LISTAGG • Die Funktion MAX • Die Funktion MEDIAN • Die Funktion MIN	Wird unter der Bedingung unterstützt, dass CTEs, die differenziell datenschutzgeschützte Tabellen verwenden, zu Daten mit Datensätzen auf Benutzerebene führen müssen. Sie sollten den SELECT-Ausdruck in diesen CTEs im Format schreiben. `SELECT userIdentifierColumn...'	Unterstützte Aggregationen: AVG, COUNT, COUNT DISTINCT, STDDEV und SUM.

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
	• Die Funktion PERCENTILE_CONT • Die Funktionen STDDEV_SAMP und STDDEV_POP • Funktionen SUM und SUM DISTINCT • Die Funktionen VAR_SAMP und VAR_POP		
CTEs	WITH-Klausel, WITH-Klausel-Unterabfrage	Wird unter der Bedingung unterstützt, dass CTEs, die differenziell datenschutzgeschützte Tabellen verwenden, zu Daten mit Datensätzen auf Benutzerebene führen müssen. Sie sollten den SELECT-Ausdruck in diesen CTEs im Format schreiben. `` `SELECT userIdentifierColumn...' ``	N/A

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Unterabfragen	SELECT-Listen-Unterabfrage, FROM-Klausel-Unterabfrage, WHERE-Klausel-Unterabfrage	Nicht unterstützt Unterabfragen in der Abfrage, die auf eine Tabelle mit aktiviertem Differential Privacy verweist, werden nicht unterstützt. Schreiben Sie Ihre Unterabfragen in Common Table Expressions (CTEs) um.	
Klauseln verbinden	• INNER JOIN • LEFT JOIN • RIGHT JOIN • VOLLSTÄNDIGER BEITRITT • [BEITRETEN] ODER Operator • CROSS JOIN	Wird unter der Bedingung unterstützt, dass nur JOIN-Funktionen unterstützt werden, bei denen es sich um Gleichverknüpfungen für Benutzer-ID-Spalten handelt. Diese sind erforderlich, wenn zwei oder mehr Tabellen mit aktiviertem Differential Privacy abgefragt werden. Stellen Sie sicher, dass die obligatorischen Equi-Join-Bedingungen korrekt sind. Vergewissern Sie sich, dass der Tabellenbesitzer in allen Tabellen dieselbe Benutzer-ID-Spalte konfiguriert hat, sodass die Definition eines Benutzers tabellenübergreifend konsistent bleibt. CROSS JOIN-Funktionen werden nicht unterstützt, wenn zwei oder mehr Beziehungen mit aktiviertem Differential Privacy kombiniert werden.	
Satzoperatoren	UNION, UNION ALL, INTERSECT, EXCEPT | MINUS (das sind Synonyme)	Alle werden unterstützt	Nicht unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Fensterfunktionen	Aggregationsfunktionen • Die Fensterfunktion AVG • Die Fensterfunktion COUNT • CUME_DIST-Fensterfunktion • Die Fensterfunktion DENSE_RANK • Die Fensterfunktion FIRST_VALUE • Die Fensterfunktion LAG • Die Fensterfunktion LAST_VALUE • Die Fensterfunktion LEAD • MAX-Fensterfunktionen • Funktionen des MEDIAN-Fensters • Funktionen im MIN-Fenster • Die Fensterfunktion NTH_VALUE • Die Fensterfunktion RATIO_TO_REPORT	Alle werden unter der Bedingung unterstützt, dass die Benutzer-ID-Spalte in der Partitionsklausel der Fensterfunktion erforderlich ist, wenn Sie eine Beziehung mit aktiviertem Differential Privacy abfragen.	Nicht unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
	• Fensterfunktionen STDDEV_SAMP und STDDEV_POP (STDDEV_SAMP und STDDEV sind Synonyme) • SUM-Fensterfunktionen • Fensterfunktionen VAR_SAMP und VAR_POP (VAR_SAMP und VARIANCE sind Synonyme)		
	Rangfestlegungsfunktionen • Die Fensterfunktion DENSE_RANK • Die Fensterfunktion NTILE • Die Fensterfunktion PERCENT_RANK • Die Fensterfunktion RANK • Die Fensterfunktion ROW_NUMBER		

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Bedingte Ausdrücke	• CASE-Bedingungsausdruck • COALESCE-Ausdruck • Funktionen GREATEST und LEAST • NVL- und COALESCE-Funktionen • Funktion NVL2 • NULLIF-Funktion	Alle werden unterstützt	Alle werden unterstützt
Bedingungen	• Vergleichsbedingung • Logische Bedingungen • Patternmatching-Bedingungen • Bedingungen zwischen den Reichweiten • „Null“-Bedingung	`EXISTS`und `IN` können nicht verwendet werden, da sie Unterabfragen erfordern. Alle anderen werden unterstützt.	Alle werden unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Funktionen für Datum und Uhrzeit	• Datums- und Zeitfunktionen in Transaktionen • Verkettungsoperator • ADD_MONTHS-Funktionen • Funktion CONVERT_TIMEZONE • Funktion CURRENT_DATE • Funktion DATEADD • Funktion DATEDIFF • DATE_PART-Funktionen • Funktion DATE_TRUNC • Funktion EXTRACT • Funktion GETDATE • TIMEOFDAY-Funktionen • Funktion TO_TIMESTAMP • Datumsteile für Datums- oder Zeitstempelfunktionen	Alle werden unterstützt	Alle werden unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Zeichenfolgenfunktionen	• || (Verkettungs-) Operator • Die Funktion BTRIM • Die Funktion CHAR_LENGTH • Die Funktion CHARACTER_LENGTH • Funktion CHARINDEX • Funktion CONCAT • Die Funktionen LEFT und RIGHT • Die Funktion LEN • Die Funktion LENGTH • Die Funktion LOWER • Die Funktionen LPAD und RPAD • Die Funktion LTRIM • POSITION-Funktionen • Die Funktion REGEXP_COUNT • Die Funktion REGEXP_INSTR • Die Funktion REGEXP_REPLACE	Alle werden unterstützt	Alle werden unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
	• Die Funktion REGEXP_SUBSTR • Die Funktion REPEAT • Die Funktion REPLACE • Die Funktion REPLICATE • Die Funktion REVERSE • Die Funktion RTRIM • Funktion SOUNDEX • Die Funktion SPLIT_PART • Die Funktion STRPOS • Die Funktion SUBSTRING • Die Funktion TEXTLEN • Die Funktion TRANSLATE • TRIM-Funktionen • Die Funktion UPPER		

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Funktionen für die Datentypformatierung	• CAST-Funktion • TO_CHAR • TO_DATE-Funktion • TO_NUMBER • Datum-/Uhrzeit-Formatzeichenfolgen • Numerische Formatzeichenfolgen	Alle werden unterstützt	Alle werden unterstützt
Hash-Funktionen	• Die Funktion MD5 • Die Funktion SHA • Die Funktion SHA1 • Die Funktion SHA2 • MURMUR3_32_HASH	Alle werden unterstützt	Alle werden unterstützt
Symbole für mathematische Operatoren	+, -, *,/,% und @	Alle werden unterstützt	Alle werden unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Mathematische Funktionen	• Funktion ABS • Die Funktion ACOS • Die Funktion ASIN • Die Funktion ATAN • Die Funktion ATAN2 • Die Funktion CBRT • Die Funktion CEILING (oder CEIL) • Die Funktion COS • Die Funktion COT • Die Funktion DEGREES • Die Funktion DEXP • Die Funktion LTRIM • Die Funktion DLOG1 • Die Funktion DLOG10 • Die Funktion EXP • Die Funktion FLOOR • Die Funktion LN • Die Funktion LOG • Die Funktion MOD • Die Funktion PI • Die Funktion POWER	Alle werden unterstützt	Alle werden unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
	• Die Funktion RADIANS • Die Funktion RANDOM • Die Funktion ROUND • Die Funktion SIGN • Die Funktion SIN • SQRT-Funktionen • Die Funktion TRUNC		

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Funktionen für SUPER-Typinformationen	• Die Funktion DECIMAL_PRECISION • Die Funktion DECIMAL_SCALE • Die Funktion IS_ARRAY • Die Funktion IS_BIGINT • Die Funktion IS_CHAR • Die Funktion IS_DECIMAL • Die Funktion IS_FLOAT • Die Funktion IS_INTEGER • Die Funktion IS_OBJECT • Die Funktion IS_SCALAR • Die Funktion IS_SMALLINT • Die Funktion IS_VARCHAR • Die Funktion JSON_TYPEOF	Alle werden unterstützt	Alle werden unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
VARBYTE-Funktionen	• Funktion FROM_HEX • Funktion FROM_VARBYTE • Funktion TO_HEX • Funktion TO_VARBYTE	Alle werden unterstützt	Alle werden unterstützt
JSON	• Funktion CAN_JSON_PARSE • Die Funktion „JSON_EXTRACT_ARRAY_ELEMENT_TEXT“ • Die Funktion JSON_EXTRACT_PATH_TEXT • Funktion JSON_PARSE • Funktion JSON_SERIALISE • Funktion JSON_SERALIZE_TO_VARBYTE	Alle werden unterstützt	Alle werden unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Array-Funktionen	• array-Funktion • array_concat-Funktion • array_flatten-Funktion • get_array_length-Funktion • split_to_array-Funktion • subarray-Funktion	Nicht unterstützt	Nicht unterstützt
Erweiterte GRUPPE VON	GRUPPIERUNGSSÄTZE, ROLLUP, WÜRFEL	Nicht unterstützt	Nicht unterstützt
Vorgang sortieren	ORDER BY	Wird unter der Bedingung unterstützt, dass eine ORDER BY-Klausel nur in der Partitionsklausel einer Fensterfunktion unterstützt wird, wenn Tabellen mit aktiviertem Differential Privacy abgefragt werden.	Unterstützt
Zeilenbegrenzungen	LIMIT, OFFSET	Wird in CTEs, die differenziell datenschutzgeschützte Tabellen verwenden, nicht unterstützt	Alle werden unterstützt

Kurzname	SQL-Konstrukte	Allgemeine Tabellenausdrücke (CTEs)	Letzte SELECT-Klausel
Aliasing von Tabellen und Spalten		Unterstützt	Unterstützt
Mathematische Funktionen für Aggregatfunktionen		Unterstützt	Unterstützt
Skalarfunktionen innerhalb von Aggregatfunktionen		Unterstützt	Unterstützt

Allgemeine Alternativen für nicht unterstützte SQL-Konstrukte

Kategorie	SQL-Konstrukt	Alternative
Fensterfunktionen	• LISTAGG • PERCENTILE_CONT • PERCENTILE_DISC	Sie können die entsprechende Aggregatfunktion mit GROUP BY verwenden.
Symbole für mathematische Operatoren	• $column ||/ 2 • $Spalte |/ 2 • $Spalte ^ 2	• CBRT • SQRT • MACHT ($Spalte, 2)
Skalarfunktionen	• SYSDATE • $column: :Ganzzahl • konvertieren (Typ, $Spalte)	• CURRENT_DATE • CAST $column ALS Ganzzahl • CAST $column ALS Typ
Literale	INTERVALL '1 SEKUNDE'	INTERVALL '1' SEKUNDE
Zeilenbegrenzung	TOP n	GRENZE n
Join	• USING	Die ON-Klausel sollte explizit ein Join-Kriterium enthalten.

Kategorie	SQL-Konstrukt	Alternative
	• NATURAL	

Tipps und Beispiele für Differential Privacy-Abfragen

AWS Clean Rooms Differential Privacy verwendet eine allgemeine Abfragestruktur, um eine Vielzahl von SQL-Konstrukten wie Common Table Expressions (CTEs) für die Datenaufbereitung und häufig verwendete Aggregatfunktionen wie, oder zu unterstützen. `COUNT` `SUM` Um den Beitrag jedes möglichen Benutzers zu Ihren Daten zu verschleiern, indem den aggregierten Abfrageergebnissen zur Laufzeit Rauschen hinzugefügt wird, erfordert AWS Clean Rooms Differential Privacy, dass Aggregatfunktionen in der Endversion auf Daten auf Benutzerebene ausgeführt werden. `SELECT statement`

Im folgenden Beispiel werden zwei Tabellen mit dem Namen `socialco_impressions` und `socialco_users` von einem Medienverlag verwendet, der Daten mithilfe von Differential Privacy schützen möchte, während er mit einer Sportmarke mit Daten zusammenarbeitet. `athletic_brand_sales` Der Medienherausgeber hat die `user_id` Spalte als Benutzer-ID-Spalte konfiguriert und gleichzeitig den differenziellen Datenschutz in AWS Clean Rooms aktiviert. Der Werbetreibende benötigt keinen differenzierten Datenschutz und möchte eine Abfrage mithilfe von CTEs für kombinierte Daten ausführen. Da sein CTE differenzielle datenschutzgeschützte Tabellen verwendet, nimmt der Werbetreibende die Benutzer-ID-Spalte aus diesen geschützten Tabellen in die Liste der CTE-Spalten auf und verknüpft die geschützten Tabellen in der Benutzer-ID-Spalte.

```
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
```

Ebenso müssen Sie, wenn Sie Fensterfunktionen für Tabellen mit differenziellen datenschutzgeschützten Daten ausführen möchten, die Spalte mit der Benutzerkennung in die Klausel aufnehmen. `PARTITION BY`

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

Einschränkungen von AWS Clean Rooms Differential Privacy

AWS Clean Rooms Differential Privacy befasst sich nicht mit den folgenden Situationen:

1. AWS Clean Rooms Differential Privacy befasst sich nicht mit Timing-Angriffen. Diese Angriffe sind beispielsweise in Szenarien möglich, in denen ein einzelner Benutzer eine große Anzahl von Zeilen beisteuert und das Hinzufügen oder Entfernen dieses Benutzers die Berechnungszeit für Abfragen erheblich verändert.
2. AWS Clean Rooms Differential Privacy garantiert keinen differenzierten Datenschutz, wenn eine SQL-Abfrage aufgrund der Verwendung bestimmter SQL-Konstrukte zur Laufzeit zu Überlauffehlern oder ungültigen Cast-Fehlern führen kann. Die folgende Tabelle enthält eine Liste einiger, aber nicht aller SQL-Konstrukte, die zu Laufzeitfehlern führen können und die in Analysevorlagen verifiziert werden sollten. Es wird empfohlen, Analysevorlagen zu genehmigen, die die Wahrscheinlichkeit solcher Laufzeitfehler minimieren, und die Abfrageprotokolle regelmäßig zu überprüfen, um festzustellen, ob die Abfragen mit der Kooperationsvereinbarung übereinstimmen.

   Die folgenden SQL-Konstrukte sind anfällig für Überlauffehler:

   - Aggregatfunktionen — AVG, LISTAVG, PERCENTILE_COUNT, PERCENTILE_DISC, SUM/SUM_DISTINCT

- Funktionen zur Formatierung von Datentypen — TO_TIMESTAMP, TO_DATE
- Datums- und Uhrzeitfunktionen — ADD_MONTHS, DATEADD, DATEDIFF
- Mathematische Funktionen - +, -, *,/, POWER
- Zeichenkettenfunktionen - ||, CONCAT, REPEAT, REPLICATE
- Fensterfunktionen — AVG, LISTAGG, PERCENTILE_COUNT, PERCENTILE_DISC, RATIO_TO_REPORT, SUM

Die Formatierungsfunktion für den CAST-Datentyp ist anfällig für ungültige Umwandlungsfehler.

AWS Clean Rooms ML

AWS Clean Rooms ML

AWS Clean Rooms ML bietet eine Methode zur Wahrung der Privatsphäre, mit der zwei Parteien ähnliche Benutzer in ihren Daten identifizieren können, ohne ihre Daten miteinander teilen zu müssen. Die erste Partei stellt die Trainingsdaten zur Verfügung, AWS Clean Rooms sodass sie ein ähnliches Modell erstellen und konfigurieren und es mit einer Zusammenarbeit verknüpfen kann. Die zweite Partei überträgt dann ihre Ausgangsdaten in ein ähnliches Segment, das den Trainingsdaten ähnelt, AWS Clean Rooms und generiert dort ein ähnliches Segment.

Eine detailliertere Erklärung, wie das funktioniert, finden Sie unterKontoübergreifende Jobs.

- Anbieter von Trainingsdaten — Die Partei, die die Trainingsdaten bereitstellt, ein Lookalike-Modell erstellt und konfiguriert und dieses Lookalike-Modell dann einer Zusammenarbeit zuordnet.
- Seed-Datenanbieter — Die Partei, die die Ausgangsdaten bereitstellt, generiert ein Lookalike-Segment und exportiert ihr Lookalike-Segment.
- Trainingsdaten — Die Daten des Trainingsdatenanbieters, die zur Generierung eines Lookalike-Modells verwendet werden. Die Trainingsdaten werden verwendet, um die Ähnlichkeit des Benutzerverhaltens zu messen.

  Die Trainingsdaten müssen eine Benutzer-ID, eine Element-ID und eine Zeitstempelspalte enthalten. Optional können die Trainingsdaten auch andere Interaktionen als numerische oder kategoriale Merkmale enthalten. Beispiele für Interaktionen sind eine Liste von angesehenen Videos, gekauften Artikeln oder gelesenen Artikeln.
- Seed-Daten — Die Daten des Seed-Datenanbieters, die zur Erstellung eines Lookalike-Segments verwendet werden. Bei der Ausgabe des Lookalike-Segments handelt es sich um eine Gruppe von Benutzern aus den Trainingsdaten, die den Seed-Benutzern am ähnlichsten sind.
- Lookalike-Modell — Ein maschinelles Lernmodell der Trainingsdaten, das verwendet wird, um ähnliche Benutzer in anderen Datensätzen zu finden.

  Bei der Verwendung der API wird der Begriff Zielgruppenmodell gleichwertig mit dem Lookalike-Modell verwendet. Beispielsweise verwenden Sie die CreateAudienceModel-API, um ein Lookalike-Modell zu erstellen.
- Lookalike-Segment — Eine Teilmenge der Trainingsdaten, die den Ausgangsdaten am ähnlichsten ist.

Wenn Sie die API verwenden, erstellen Sie mit der API ein Lookalike-Segment. StartAudienceGenerationJob

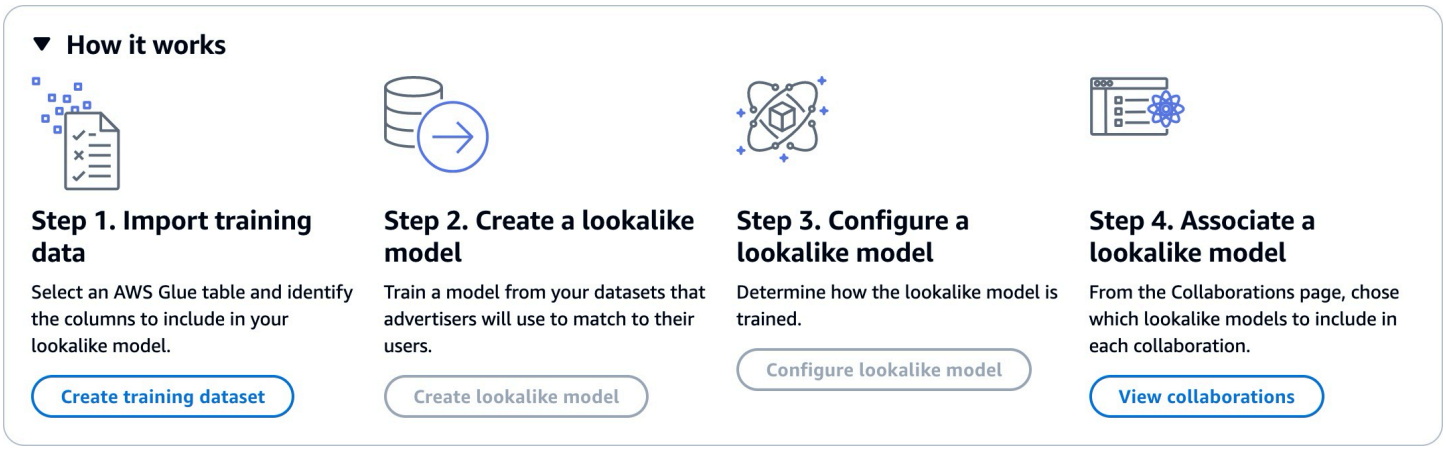
Die Daten des Trainingsdatenanbieters werden niemals mit dem Startdatenanbieter geteilt, und die Daten des Ausgangsdatenanbieters werden niemals mit dem Trainingsdatenanbieter geteilt. Die Ausgabe des Lookalike-Segments wird mit dem Trainingsdatenanbieter geteilt, aber niemals mit dem Seed-Datenanbieter.

Weitere Informationen zu Lookalike-Modellen finden Sie in den folgenden Themen.

Themen

- Wie funktioniert AWS Clean Rooms ML

Wie funktioniert AWS Clean Rooms ML



Clean Rooms ML erfordert, dass zwei Parteien, ein Anbieter von Trainingsdaten und ein Anbieter von Startdaten, nacheinander zusammenarbeiten, AWS Clean Rooms um ihre Daten in eine Zusammenarbeit einzubringen. Dies ist der Workflow, den der Trainingsdatenanbieter zuerst abschließen muss:

1. Die Daten des Trainingsdatenanbieters müssen in einer AWS Glue Datenkatalogtabelle mit Interaktionen zwischen Benutzern und Elementen gespeichert werden. Die Trainingsdaten müssen mindestens eine Benutzer-ID-Spalte, eine Interaktions-ID-Spalte und eine Zeitstempelspalte enthalten.
2. Der Trainingsdatenanbieter registriert die Trainingsdaten bei AWS Clean Rooms.

3. Der Trainingsdatenanbieter erstellt ein Lookalike-Modell, das mit mehreren Startdatenanbietern gemeinsam genutzt werden kann. Das Lookalike-Modell ist ein tiefes neuronales Netzwerk, dessen Training bis zu 24 Stunden dauern kann. Es wird nicht automatisch neu trainiert und wir empfehlen Ihnen, das Modell wöchentlich neu zu schulen.
4. Der Anbieter von Trainingsdaten konfiguriert das Lookalike-Modell, einschließlich der Frage, ob Relevanzkennzahlen und der Amazon S3 S3-Speicherort der Ausgabesegmente geteilt werden sollen. Der Anbieter von Trainingsdaten kann mehrere konfigurierte Lookalike-Modelle aus einem einzigen Lookalike-Modell erstellen.
5. Der Anbieter von Trainingsdaten ordnet das konfigurierte Zielgruppenmodell einer Kollaboration zu, die mit einem Startdatenanbieter geteilt wird.

Dies ist der Workflow, den der Seed-Datenanbieter als Nächstes abschließen muss:

1. Die Daten des Seed-Datenanbieters müssen in einem Amazon S3 S3-Bucket gespeichert werden.
2. Der Seed-Datenanbieter eröffnet die Zusammenarbeit, die er mit dem Trainingsdatenanbieter teilt.
3. Der Seed-Datenanbieter erstellt auf der Registerkarte Clean Rooms ML der Kollaborationsseite ein ähnliches Segment.
4. Der Seed-Datenanbieter kann die Relevanzkennzahlen auswerten, sofern sie geteilt wurden, und das Lookalike-Segment zur externen Verwendung exportieren. AWS Clean Rooms

Datenschutz durch ML AWS Clean Rooms

Clean Rooms ML wurde entwickelt, um das Risiko von Inferenzangriffen auf Mitglieder zu verringern. Dabei kann der Anbieter der Trainingsdaten herausfinden, wer in den Startdaten enthalten ist, und der Anbieter der Startdaten kann herausfinden, wer in den Trainingsdaten enthalten ist. Es wurden mehrere Schritte unternommen, um diesen Angriff zu verhindern.

Erstens beobachten Anbieter von Saatgutdaten die Ergebnisse von Clean Rooms ML nicht direkt, und Anbieter von Trainingsdaten können die Saatgutdaten niemals beobachten. Anbieter von Saatgutdaten können sich dafür entscheiden, die Ausgangsdaten in das Output-Segment aufzunehmen.

Als Nächstes wird das Lookalike-Modell aus einer Zufallsstichprobe der Trainingsdaten erstellt. Diese Stichprobe umfasst eine beträchtliche Anzahl von Benutzern, die nicht der Stammzielgruppe entsprechen. Durch dieses Verfahren ist es schwieriger festzustellen, ob ein Benutzer nicht in den Daten enthalten war. Dies ist eine weitere Möglichkeit, Rückschlüsse auf die Mitgliedschaft zu ziehen.

Außerdem können mehrere Startkunden für jeden Parameter des samenspezifischen Lookalike-Modell-Trainings verwendet werden. Dadurch wird begrenzt, wie stark das Modell übermäßig angepasst werden kann und wie viel Rückschlüsse auf einen Benutzer gezogen werden können. Daher empfehlen wir, dass die Mindestgröße der Ausgangsdaten 500 Benutzer beträgt.

Schließlich werden den Anbietern von Trainingsdaten niemals Kennzahlen auf Benutzerebene zur Verfügung gestellt, wodurch eine weitere Möglichkeit für einen Angriff auf Mitgliedschaftsabschlüsse ausgeschlossen wird.

AWS Clean Rooms Kennzahlen zur Bewertung von ML-Modellen

Clean Rooms ML berechnet den Erinnerungs - und den Relevanzwert, um festzustellen, wie gut Ihr Modell abschneidet. Recall vergleicht die Ähnlichkeit zwischen den Lookalike-Daten und den Trainingsdaten. Der Relevanzwert wird verwendet, um zu entscheiden, wie groß die Zielgruppe sein sollte, und nicht, ob das Modell gut abschneidet.

Der Recall ist ein unvoreingenommenes Maß dafür, wie ähnlich das Lookalike-Segment den Trainingsdaten ist. Die Rückrufaktion ist der Prozentsatz der Nutzer, die sich am ähnlichsten sind (standardmäßig die ähnlichsten 20%) aus einer Stichprobe von Trainingsdaten, die in der Startzielgruppe nach dem Job zur Zielgruppengenerierung enthalten sind. Die Werte liegen zwischen 0 und 1, größere Werte deuten auf eine bessere Zielgruppe hin. Ein Wiedererkennungswert, der in etwa dem maximalen Prozentsatz entspricht, gibt an, dass das Zielgruppenmodell einer zufälligen Auswahl entspricht.

Wir halten dies für eine bessere Bewertungsmetrik als Genauigkeit, Präzision und F1-Werte, da Clean Rooms ML bei der Erstellung seines Modells nicht genau als negativ eingestufte Nutzer eingestuft hat.

Der Relevanzwert auf Segmentebene ist ein Maß für die Ähnlichkeit mit Werten im Bereich von -1 (am wenigsten ähnlich) bis 1 (am ähnlichsten). Clean Rooms ML berechnet eine Reihe von Relevanzwerten für verschiedene Segmentgrößen, damit Sie die beste Segmentgröße für Ihre Daten ermitteln können. Die Relevanzwerte nehmen mit zunehmender Segmentgröße monoton ab, sodass sie mit zunehmender Segmentgröße den Ausgangsdaten weniger ähnlich sein können. Wenn der Relevanzwert auf Segmentebene 0 erreicht, prognostiziert das Modell, dass alle Benutzer im Lookalike-Segment aus derselben Verteilung stammen wie die Ausgangsdaten. Durch eine Erhöhung der Ausgabegröße werden wahrscheinlich auch Benutzer im Lookalike-Segment berücksichtigt, die nicht aus derselben Verteilung wie die Ausgangsdaten stammen.

Die Relevanzwerte werden innerhalb einer einzelnen Kampagne normalisiert und sollten nicht für Vergleiche zwischen Kampagnen verwendet werden. Relevanzwerte sollten nicht als Einzelnachweis für Geschäftsergebnisse verwendet werden, da diese neben der Relevanz auch von mehreren komplexen Faktoren beeinflusst werden, wie z. B. Bestandsqualität, Inventarart, Zeitpunkt der Werbung usw.

Relevanzwerte sollten nicht dazu verwendet werden, die Qualität des Saatguts zu beurteilen, sondern vielmehr, ob sie erhöht oder verringert werden kann. Betrachten Sie die folgenden Beispiele:

- Durchweg positive Werte — Dies deutet darauf hin, dass es mehr Output-Nutzer gibt, die als ähnlich prognostiziert werden, als dass sie im Lookalike-Segment enthalten sind. Dies ist bei Saatgutdaten üblich, die Teil eines großen Marktes sind, z. B. bei allen, die im letzten Monat Zahnpasta gekauft haben. Wir empfehlen, sich kleinere Samendaten anzusehen, z. B. alle Personen, die im letzten Monat mehr als einmal Zahnpasta gekauft haben.
- Alle Werte sind negativ oder negativ für Ihre gewünschte Lookalike-Segmentgröße — Dies deutet darauf hin, dass Clean Rooms ML davon ausgeht, dass es in der gewünschten Lookalike-Segmentgröße nicht genügend ähnliche Benutzer gibt. Das kann daran liegen, dass die Saatgutdaten zu spezifisch sind oder der Markt zu klein ist. Wir empfehlen, entweder weniger Filter auf die Saatgutdaten anzuwenden oder den Markt zu erweitern. Wenn es sich bei den ursprünglichen Ausgangsdaten beispielsweise um Kunden handelte, die einen Kinderwagen und einen Kindersitz gekauft haben, könnten Sie den Markt auf Kunden ausdehnen, die mehrere Babyartikel gekauft haben.

Die Anbieter von Schulungsdaten bestimmen, ob die Relevanzwerte veröffentlicht werden und welche Felder für die Berechnung der Relevanzwerte verwendet werden.

Mit AWS Clean Rooms ML arbeiten

Ein Lookalike-Modell ist ein Modell der Daten eines Trainingsdatenanbieters, das es einem Seed-Datenanbieter ermöglicht, ein ähnliches Segment der Daten eines Trainingsdatenanbieters zu erstellen, das seinen Ausgangsdaten am ähnlichsten ist. Um ein Lookalike-Modell zu erstellen, das in einer Zusammenarbeit verwendet werden kann, müssen Sie Ihre Trainingsdaten importieren, ein Lookalike-Modell erstellen, dieses Lookalike-Modell konfigurieren und es dann einer Kollaboration zuordnen.

Nachdem der Trainingsdatenanbieter das ML-Modell erstellt hat, kann der Seed-Datenprovider das Seed-Segment erstellen und exportieren.

Themen

Arbeiten mit Lookalike-Modellen (Trainingsdatenanbieter)

Trainingsdaten importieren

Bevor Sie ein Lookalike-Modell erstellen, müssen Sie die AWS Glue Tabelle angeben, die die Trainingsdaten enthält. Clean Rooms ML speichert keine Kopie dieser Daten, sondern lediglich Metadaten, die den Zugriff auf die Daten ermöglichen.

Um Trainingsdaten zu importieren AWS Clean Rooms

1. Melde dich bei der an AWS Management Console und öffne die AWS Clean Rooms Konsole mit deinem AWS-Konto (falls du das noch nicht getan hast).
2. Wählen Sie im linken Navigationsbereich ML Modeling aus.
3. Wählen Sie auf der Registerkarte Trainingsdatensätze die Option Trainingsdatensatz erstellen aus.
4. Geben Sie einen Namen und optional eine Beschreibung ein.
5. Wählen Sie als Datenquelle Ihre AWS Glue Tabelle aus:
    a. Wählen Sie die Datenbank, die Sie konfigurieren möchten, aus der Dropdownliste aus.
    b. Wählen Sie die Trainingsdatenquelle aus, indem Sie die Datenbank und die Tabelle, die Sie konfigurieren möchten, aus den Dropdownlisten auswählen.

> **Note**
>
> Um zu überprüfen, ob es sich um die richtige Tabelle handelt, führen Sie einen der folgenden Schritte aus:
>
> - Wählen Sie Anzeigen in AWS Glue.
> - Aktivieren Sie „Schema anzeigen“, um das Schema anzuzeigen.

6. Wählen Sie für Trainingsdetails die Spalten Benutzer-ID, Artikel-ID und Timestamp aus Ihren Daten aus. Die Trainingsdaten müssen diese drei Spalten enthalten. Sie können auch alle anderen Spalten auswählen, die Sie in die Trainingsdaten aufnehmen möchten.

   Die Daten in der Timestamp-Spalte müssen im Format Unix-Epochenzeit in Sekunden vorliegen.

7. Unter Dienstzugriff müssen Sie eine Servicerolle angeben, die auf Ihre Daten zugreifen kann, und einen KMS-Schlüssel angeben, falls Ihre Daten verschlüsselt sind. Wählen Sie Neue Servicerolle erstellen und verwenden aus. Clean Rooms ML erstellt dann automatisch eine Servicerolle und fügt die erforderlichen Berechtigungsrichtlinien hinzu. Wählen Sie Bestehende Servicerolle verwenden und geben Sie sie in das Feld Servicerollenname ein, wenn Sie über eine bestimmte Servicerolle verfügen, die Sie verwenden möchten.

   Wenn Ihre Daten verschlüsselt sind, geben Sie Ihren KMS-Schlüssel in das AWS KMS keyFeld ein oder klicken Sie auf Erstellen, AWS KMS key um einen neuen KMS-Schlüssel zu generieren.

8. Wenn Sie Tags für den Trainingsdatensatz aktivieren möchten, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel-Wert-Paar ein.
9. Wählen Sie Trainingsdatensatz erstellen aus.

Die entsprechende API-Aktion finden Sie unter CreateTrainingDatensatz.

Erstellen Sie ein Lookalike-Modell

Nachdem Sie einen Trainingsdatensatz erstellt haben, sind Sie bereit, ein Lookalike-Modell zu erstellen. Sie können viele Lookalike-Modelle aus einem einzigen Trainingsdatensatz erstellen.

Sie müssen eine Standarddatenbank in Ihrer Rolle erstellen AWS Glue Data Catalog oder die `glue:createDatabase` Berechtigung in der angegebenen Rolle angeben.

So erstellen Sie ein Lookalike-Modell in AWS Clean Rooms

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich ML Modeling aus.
3. Wählen Sie auf der Registerkarte Lookalike-Modelle die Option Lookalike-Modell erstellen aus.
4. Gehen Sie für Lookalike-Modell erstellen und für Details zum Lookalike-Modell wie folgt vor:

   a. Geben Sie einen Namen und optional eine Beschreibung ein.

b. Wählen Sie den Trainingsdatensatz, den Sie modellieren möchten, aus der Dropdownliste aus.

c. Geben Sie ein optionales Trainingsfenster ein.

5. Wenn Sie benutzerdefinierte Verschlüsselungseinstellungen für das Lookalike-Modell aktivieren möchten, wählen Sie Verschlüsselungseinstellungen anpassen und geben Sie dann den KMS-Schlüssel ein.
6. Wenn Sie Tags für das Lookalike-Modell aktivieren möchten, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel-Wert-Paar ein.
7. Wählen Sie Lookalike-Modell erstellen aus.

Die entsprechende API-Aktion finden Sie unter CreateAudienceModell.

Konfigurieren Sie ein Lookalike-Modell

Nachdem Sie ein Lookalike-Modell erstellt haben, können Sie es für die Verwendung in einer Zusammenarbeit konfigurieren. Sie können mehrere konfigurierte Lookalike-Modelle aus einem einzigen Lookalike-Modell erstellen.

So konfigurieren Sie ein Lookalike-Modell in AWS Clean Rooms

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich ML Modeling aus.
3. Wählen Sie auf der Registerkarte Konfigurierte Lookalike-Modelle die Option Lookalike-Modell konfigurieren aus.
4. Gehen Sie für „Lookalike-Modell konfigurieren“ und „Details zum konfigurierten Lookalike-Modell“ wie folgt vor:

   a. Geben Sie einen Namen und optional eine Beschreibung ein.

   b. Wählen Sie das Lookalike-Modell, das Sie konfigurieren möchten, aus der Dropdownliste aus.

   c. Wählen Sie die gewünschte Mindestgröße für die passende Samengröße aus. Dies ist die Mindestanzahl von Benutzern in den Daten des Seed-Datenanbieters, die sich mit den Benutzern in den Trainingsdaten überschneiden. Dieser Wert muss größer als 0 sein.

5. Damit Metriken mit anderen Mitgliedern geteilt werden können, wählen Sie aus, ob der Seed-Datenanbieter in Ihrer Zusammenarbeit Modellmetriken, einschließlich Relevanzbewertungen, erhalten soll.
6. Geben Sie für Zielort des Lookalike-Segments den Amazon S3 S3-Bucket ein, in den das Lookalike-Segment exportiert wird. Dieser Bucket muss sich in derselben Region befinden wie Ihre anderen Ressourcen.
7. Wählen Sie für Dienstzugriff den Namen der vorhandenen Servicerolle aus, der für den Zugriff auf diese Tabelle verwendet werden soll.
8. Wählen Sie Lookalike-Modell konfigurieren.
9. Wenn Sie Tags für die konfigurierte Tabellenressource aktivieren möchten, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

Die entsprechende API-Aktion finden Sie unter CreateConfiguredAudienceModel.

Ordnen Sie ein konfiguriertes Lookalike-Modell zu

Nachdem Sie ein Lookalike-Modell konfiguriert haben, können Sie es einer Kollaboration zuordnen.

Um ein konfiguriertes Lookalike-Modell zuzuordnen AWS Clean Rooms

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie auf der Registerkarte Mit aktiver Mitgliedschaft eine Kollaboration aus.
4. Wählen Sie auf der Registerkarte ML-Modellierung die Option Ähnliches Modell zuordnen aus.
5. Für „Konfiguriertes Lookalike-Modell zuordnen“ und für „Details zum Partner-Lookalike-Modell zuordnen“:

    a. Geben Sie einen Namen für das zugehörige konfigurierte Zielgruppenmodell ein.

    b. Geben Sie eine Beschreibung der Tabelle ein.

    Die Beschreibung hilft dabei, zwischen anderen zugehörigen konfigurierten Zielgruppenmodellen mit ähnlichen Namen zu unterscheiden.
6. Wählen Sie für Konfiguriertes Lookalike-Modell ein konfiguriertes Lookalike-Modell aus der Drop-down-Liste aus.
7. Wählen Sie Associate aus.

Informationen zur entsprechenden API-Aktion finden Sie unter Zuordnung. CreateConfigured AudienceModel

Aktualisieren Sie ein konfiguriertes Lookalike-Modell

Nachdem Sie ein konfiguriertes Lookalike-Modell zugeordnet haben, können Sie es aktualisieren, um Informationen wie den Namen, die zu teilenden Metriken oder den Amazon S3 S3-Ausgabeort zu ändern.

So aktualisieren Sie ein zugeordnetes konfiguriertes Lookalike-Modell in AWS Clean Rooms

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich ML-Modellierung aus.
3. Wählen Sie auf der Registerkarte Konfigurierte Lookalike-Modelle ein konfiguriertes Lookalike-Modell aus und klicken Sie auf Bearbeiten.
4. Für Lookalike-Modell konfigurieren für Details zum konfigurierten Lookalike-Modell:
    a. Wählen Sie das Lookalike-Modell, das Sie konfigurieren möchten, aus der Dropdownliste aus.
    b. Wählen Sie die gewünschte Mindestgröße für die passende Samengröße aus. Dies ist die Mindestanzahl von Benutzern in den Daten des Seed-Datenanbieters, die sich mit den Benutzern in den Trainingsdaten überschneiden. Dieser Wert muss größer als 0 sein.
5. Damit Metriken mit anderen Mitgliedern geteilt werden können, wählen Sie aus, ob der Seed-Datenanbieter in Ihrer Zusammenarbeit Modellmetriken, einschließlich Relevanzbewertungen, erhalten soll.
6. Geben Sie für Zielort des Lookalike-Segments den Amazon S3 S3-Bucket ein, in den das Lookalike-Segment exportiert wird. Dieser Bucket muss sich in derselben Region befinden wie Ihre anderen Ressourcen.
7. Wählen Sie für Dienstzugriff den Namen der vorhandenen Servicerolle aus, der für den Zugriff auf diese Tabelle verwendet werden soll.
8. Wählen Sie unter Erweiterte Konfiguration der Partitionsgröße aus, wie Sie die Zielgruppen-Bin-Größen konfigurieren möchten.
9. Wählen Sie Änderungen speichern aus.

Die entsprechende API-Aktion finden Sie unter UpdateConfiguredAudienceModel.

Mit Lookalike-Segmenten arbeiten (Seed-Datenanbieter)

Erstellen Sie ein Lookalike-Segment

Ein Lookalike-Segment ist eine Teilmenge der Trainingsdaten, die den Ausgangsdaten am ähnlichsten ist.

Um ein Lookalike-Segment zu erstellen AWS Clean Rooms

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie auf der Registerkarte Mit aktiver Mitgliedschaft eine Kollaboration aus.
4. Wählen Sie auf der Registerkarte ML Modeling die Option Lookalike-Segment erstellen aus.
5. Geben Sie für Lookalike-Segment erstellen für Lookalike-Segmentdetails einen Namen und optional eine Beschreibung ein.
6. Wählen Sie für Seed-Profile die Amazon S3 S3-Eingabequelle aus, in der Ihre Seed-Daten gespeichert sind.
7. Wählen Sie für den Servicezugriff den Namen der vorhandenen Servicerolle aus, die für den Zugriff auf diese Tabelle verwendet werden soll.
8. Wenn Sie Tags für den Trainingsdatensatz aktivieren möchten, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.
9. Wählen Sie Lookalike-Segment erstellen aus.

Die entsprechende API-Aktion finden Sie unter StartAudienceGenerationJob.

Exportieren Sie ein Lookalike-Segment

Nachdem Sie ein Lookalike-Segment erstellt haben, können Sie diese Daten in einen Amazon S3 S3-Bucket exportieren.

Um ein Lookalike-Segment zu exportieren in AWS Clean Rooms

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.

3. Wählen Sie auf der Registerkarte Mit aktiver Mitgliedschaft eine Kollaboration aus.
4. Wählen Sie auf der Registerkarte ML Modeling ein Lookalike-Segment aus und klicken Sie auf Exportieren.
5. Geben Sie für Lookalike-Modell exportieren unter Details des Lookalike-Modells exportieren einen Namen und optional eine Beschreibung ein.
6. Wählen Sie unter Segmentgröße die gewünschte Größe für das exportierte Segment aus.
7. Wählen Sie Export aus.

Die entsprechende API-Aktion finden Sie unter StartAudienceExportJob.

Nächste Schritte

Nachdem Sie nun ein Lookalike-Modell erstellt und ein Ausgangssegment exportiert haben, können Sie:

- Verwalten AWS Clean Rooms

Kryptografisches Rechnen für Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) ist eine Funktion AWS Clean Rooms , die zusätzlich zu Analyseregeln verwendet werden kann. Mit C3R können Unternehmen sensible Daten zusammenführen, um neue Erkenntnisse aus der Datenanalyse zu gewinnen, und gleichzeitig kryptografisch einschränken, was von jeder Partei im Prozess gelernt werden kann. C3R kann von zwei oder mehr Parteien verwendet werden, die mit ihren sensiblen Daten zusammenarbeiten möchten, aber nur verschlüsselte Daten in der Cloud verwenden müssen.

Der C3R-Verschlüsselungsclient ist ein clientseitiges Verschlüsselungstool, mit dem Sie Ihre Daten für die Verwendung mit verschlüsseln können. AWS Clean Rooms Wenn Sie den C3R-Verschlüsselungsclient verwenden, bleiben Daten während der Verwendung in einer Zusammenarbeit kryptografisch geschützt. AWS Clean Rooms Wie bei einer normalen AWS Clean Rooms Zusammenarbeit handelt es sich bei den Eingabedaten um relationale Datenbanktabellen, und die Berechnung wird als SQL-Abfrage ausgedrückt. C3R unterstützt jedoch nur eine begrenzte Teilmenge von SQL-Abfragen für verschlüsselte Daten.

Insbesondere unterstützt C3R SQL JOIN und SELECT Anweisungen zu kryptografisch geschützten Daten. Jede Spalte in der Eingabetabelle kann in genau einem der folgenden SQL-Anweisungstypen verwendet werden:

- Spalten, die für die Verwendung in JOIN Anweisungen kryptografisch geschützt sind, werden Spalten genanntfingerprint.
- Spalten, die für die Verwendung in SELECT Anweisungen kryptografisch geschützt sind, werden Spalten genannt. sealed
- Spalten, die nicht kryptografisch für die Verwendung in SELECT Oder-Anweisungen geschützt sind, werden als Spalten JOIN bezeichnet. cleartext

In einigen Fällen werden GROUP BY Anweisungen für Spalten unterstützt. fingerprint Weitere Informationen finden Sie unter FingerprintSpalten. Derzeit unterstützt C3R nicht die Verwendung anderer SQL-Konstrukte für verschlüsselte Daten, wie WHERE Klauseln oder Aggregatfunktionen wie SUM undAVERAGE, auch wenn sie sonst nach den entsprechenden Analyseregeln zulässig wären.

C3R wurde entwickelt, um Daten in einzelnen Zellen einer Tabelle zu schützen. Bei Verwendung der Standardkonfiguration für C3R bleiben die zugrunde liegenden Daten, die ein Kunde im Rahmen einer Zusammenarbeit Dritten zur Verfügung stellt, verschlüsselt, während der Inhalt darin verwendet wird. AWS Clean Rooms C3R verwendet die branchenübliche AES-GCM-Verschlüsselung für alle

sealed Spalten und eine dem Industriestandard entsprechende Pseudozufallsfunktion, bekannt als Hash-based Message Authentication Code (HMAC), zum Schutz von Spalten. fingerprint

Obwohl C3R die Daten in Ihren Tabellen verschlüsselt, können die folgenden Informationen möglicherweise dennoch abgeleitet werden:

- Informationen zu den Tabellen selbst, einschließlich der Anzahl der Spalten, der Spaltennamen und der Anzahl der Zeilen in Ihrer Tabelle.
- Wie bei den meisten Standardverschlüsselungsformen versucht C3R nicht, die Länge der verschlüsselten Werte zu verbergen. C3R bietet die Möglichkeit, verschlüsselte Werte aufzufüllen, um die genaue Länge von Klartexten zu verbergen. Eine Obergrenze für die Länge der Klartexte in jeder Spalte könnte jedoch immer noch einer anderen Partei offengelegt werden.
- Informationen auf Protokollebene, z. B. wann eine bestimmte Zeile zu einer verschlüsselten C3R-Tabelle hinzugefügt wurde.

Weitere Informationen zu C3R finden Sie in den folgenden Themen.

Themen

Überlegungen zur Verwendung von Cryptographic Computing für Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) zielt darauf ab, den Datenschutz zu maximieren. Einige Anwendungsfälle könnten jedoch von einem geringeren Datenschutzniveau im Austausch für zusätzliche Funktionen profitieren. Sie können diese spezifischen Kompromisse eingehen, indem Sie C3R von der sichersten Konfiguration aus ändern. Als Kunde sollten Sie sich dieser

Kompromisse bewusst sein und entscheiden, ob sie für Ihren Anwendungsfall geeignet sind. Zu den Kompromissen, die es zu berücksichtigen gilt, gehören:

Themen

Weitere Informationen zum Einstellen von Parametern für diese Szenarien finden Sie unter. Kryptografische Rechenparameter

Zulassen gemischter cleartext und verschlüsselter Daten in Ihren Tabellen

Die clientseitige Verschlüsselung aller Daten bietet maximalen Datenschutz. Dadurch werden jedoch bestimmte Arten von Abfragen eingeschränkt (z. B. die SUM Aggregatfunktion). Das Risiko, cleartext Daten zuzulassen, besteht darin, dass es möglich ist, dass jeder, der Zugriff auf die verschlüsselten Tabellen hat, Informationen über verschlüsselte Werte ableiten kann. Dies könnte durch eine statistische Analyse der Daten cleartext und der zugehörigen Daten geschehen.

Stellen Sie sich zum Beispiel vor, Sie hätten die Spalten `City` und`State`. Die `City` Spalte ist cleartext und die `State` Spalte ist verschlüsselt. Wenn Sie den Wert `Chicago` in der `City` Spalte sehen, können Sie mit hoher Wahrscheinlichkeit feststellen, `State` dass der`Illinois`. Im Gegensatz dazu, wenn eine Spalte `City` und die andere Spalte ist`EmailAddress`, ist es unwahrscheinlich, dass a cleartext `City` etwas über eine verschlüsselte Spalte aussagt`EmailAddress`.

Weitere Informationen zu dem Parameter für dieses Szenario finden Sie unterParameter „Spalten zulassencleartext“.

Wiederholte Werte in fingerprint Spalten zulassen

Für den sichersten Ansatz gehen wir davon aus, dass jede fingerprint Spalte genau eine Instanz einer Variablen enthält. Kein Element kann in einer fingerprint Spalte wiederholt werden. Der C3R-Verschlüsselungsclient ordnet diese cleartext Werte eindeutigen Werten zu, die nicht von Zufallswerten zu unterscheiden sind. Daher ist es unmöglich, aus diesen Zufallswerten Informationen über die abzuleiten. cleartext

Das Risiko wiederholter Werte in einer fingerprint Spalte besteht darin, dass wiederholte Werte zu wiederholten zufällig aussehenden Werten führen. Somit könnte theoretisch jeder, der Zugriff auf die verschlüsselten Tabellen hat, eine statistische Analyse der fingerprint Spalten durchführen, die Informationen über cleartext Werte liefern könnte.

Nehmen wir erneut an`State`, die fingerprint Spalte entspricht einem US-Haushalt und jede Zeile der Tabelle entspricht. Durch eine Frequenzanalyse könnte man ableiten, um welchen Bundesstaat es sich handelt `California` und welcher `Wyoming` mit hoher Wahrscheinlichkeit. Diese Schlussfolgerung ist möglich, weil es viel mehr Einwohner `California` hat als. `Wyoming` Nehmen wir dagegen an, die fingerprint Spalte bezieht sich auf eine Haushalts-ID und jeder Haushalt tauchte in der Datenbank ein- bis viermal in einer Datenbank mit Millionen von Einträgen auf. Es ist unwahrscheinlich, dass eine Frequenzanalyse nützliche Informationen liefern würde.

Weitere Informationen zu den Parametern für dieses Szenario finden Sie unterParameter „Duplikate zulassen“.

Lockerung der Beschränkungen für die Benennung von fingerprint Spalten

Standardmäßig gehen wir davon aus, dass, wenn zwei Tabellen mithilfe verschlüsselter fingerprint Spalten verknüpft werden, diese Spalten in jeder Tabelle denselben Namen haben. Der technische Grund für dieses Ergebnis ist, dass wir standardmäßig einen anderen kryptografischen Schlüssel für die Verschlüsselung jeder Spalte ableiten. fingerprint Dieser Schlüssel wird aus einer Kombination aus dem gemeinsamen geheimen Schlüssel für die Zusammenarbeit und dem Spaltennamen abgeleitet. Wenn wir versuchen, zwei Spalten mit unterschiedlichen Spaltennamen zu verbinden, leiten wir unterschiedliche Schlüssel ab und können keinen gültigen Join berechnen.

Um dieses Problem zu beheben, können Sie die Funktion deaktivieren, die Schlüssel aus jedem Spaltennamen ableitet. Anschließend verwendet der C3R-Verschlüsselungsclient einen einzigen abgeleiteten Schlüssel für alle fingerprint Spalten. Das Risiko besteht darin, dass eine andere Art der Frequenzanalyse durchgeführt werden kann, die Informationen preisgeben könnte.

Lassen Sie uns das `State` Beispiel `City` und noch einmal verwenden. Wenn wir für jede fingerprint Spalte dieselben Zufallswerte ableiten (indem wir den Spaltennamen nicht einbeziehen). `New York`hat den gleichen Zufallswert in den Spalten `City` und`State`. New York ist eine der wenigen Städte in den USA, in denen der `City` Name mit dem `State` Namen identisch ist. Wenn Ihr Datensatz dagegen in jeder Spalte völlig unterschiedliche Werte enthält, werden keine Informationen durchgesickert.

Weitere Informationen zum Parameter für dieses Szenario finden Sie unterParameter „Zulassen JOIN von Spalten mit unterschiedlichen Namen“.

Bestimmen, wie NULL Werte dargestellt werden

Sie haben die Wahl, ob Sie Werte wie alle anderen NULL Werte kryptografisch (verschlüsseln und HMAC) verarbeiten möchten. Wenn Sie Werte nicht wie alle anderen NULL Werte verarbeiten, können Informationen preisgegeben werden.

Nehmen wir zum Beispiel an, dass NULL in der `Middle Name` Spalte in der Personen ohne zweiten Vornamen cleartext angegeben werden. Wenn Sie diese Werte nicht verschlüsseln, können Sie durchsickern lassen, welche Zeilen in der verschlüsselten Tabelle für Personen ohne zweiten Vornamen verwendet werden. Diese Informationen könnten für einige Menschen in bestimmten Bevölkerungsgruppen ein Identifikationssignal sein. Wenn Sie NULL Werte jedoch kryptografisch verarbeiten, verhalten sich bestimmte SQL-Abfragen anders. Beispielsweise gruppieren GROUP BY Klauseln fingerprint NULL Werte in fingerprint Spalten nicht zusammen.

Weitere Informationen zum Parameter für dieses Szenario finden Sie unterParameter „NULLWerte beibehalten“.

Unterstützte Datei- und Datentypen in Cryptographic Computing für Clean Rooms

Der C3R-Verschlüsselungsclient erkennt die folgenden Dateitypen:

- CSV-Dateien
- ParquetDateien

Sie können das `--fileFormat` Flag im C3R-Verschlüsselungsclient verwenden, um ein Dateiformat explizit anzugeben. Wenn das Dateiformat explizit angegeben wird, wird es nicht durch die Dateierweiterung bestimmt.

Themen

- CSV-Dateien
- ParquetDateien
- Verschlüsseln von Werten, die keine Zeichenfolge sind

CSV-Dateien

Es wird davon ausgegangen, dass eine Datei mit der Erweiterung.csv im CSV-Format ist und UTF-8-codierten Text enthält. Der C3R-Verschlüsselungsclient behandelt alle Werte als Zeichenketten.

Unterstützte Eigenschaften in CSV-Dateien

Der C3R-Verschlüsselungsclient erfordert, dass CSV-Dateien die folgenden Eigenschaften haben:

- Kann eine erste Kopfzeile enthalten, die jede Spalte eindeutig benennt, oder auch nicht.
- Durch Kommas getrennt. (Derzeit werden benutzerdefinierte Trennzeichen nicht unterstützt.)
- UTF-8-codierter Text.

Löschen von Leerzeichen aus CSV-Einträgen

Sowohl führende als auch nachfolgende Leerzeichen werden aus CSV-Einträgen entfernt.

Benutzerdefinierte NULL Kodierung für eine CSV-Datei

Eine CSV-Datei kann eine benutzerdefinierte NULL Kodierung verwenden.

Mit dem C3R-Verschlüsselungsclient können Sie mithilfe des Flags benutzerdefinierte Kodierungen für NULL Einträge in den Eingabedaten angeben. `--csvInputNULLValue=<csv-input-null>` Der C3R-Verschlüsselungsclient kann mithilfe des Flags benutzerdefinierte Kodierungen in der generierten Ausgabedatei für NULL-Einträge verwenden. `--csvOutputNULLValue=<csv-output-null>`

> **Note**
>
> Es wird NULL davon ausgegangen, dass es einem Eintrag an Inhalt mangelt, insbesondere im Zusammenhang mit einem umfangreicheren Tabellenformat wie einer SQL-Tabelle. Obwohl .csv diese Charakterisierung aus historischen Gründen nicht ausdrücklich unterstützt, ist es üblich, einen leeren Eintrag, der nur Leerraum enthält, als solche zu betrachten. NULL Daher ist dies das Standardverhalten des C3R-Verschlüsselungsclients und kann nach Bedarf angepasst werden.

Wie werden CSV-Einträge von C3R interpretiert

Die folgende Tabelle enthält Beispiele dafür, wie .csv-Einträge auf der Grundlage der Werte (falls vorhanden)cleartext, die cleartext für die Flags und angegeben wurden, zusammengefasst werden (aus Gründen der Übersichtlichkeit). `--csvInputNULLValue=<csv-input-null> --csvOutputNULLValue=<csv-output-null>` Leerzeichen am Anfang und am Ende von Anführungszeichen werden gekürzt, bevor C3R die Bedeutung eines Werts interpretiert.

<csv-input-null>	**<csv-output-null>**	Eingabeeintrag	Ausgangseintrag
Keine	Keine	`,AnyProduct,`	`,AnyProduct,`
Keine	Keine	`, AnyProduct ,`	`,AnyProduct,`
Keine	Keine	`,"AnyProduct",`	`,AnyProduct,`
Keine	Keine	`, "AnyProduct" ,`	`,AnyProduct,`
Keine	Keine	`,,`	`,,`
Keine	Keine	`, ,`	`,,`
Keine	Keine	`,"",`	`,,`
Keine	Keine	`," ",`	`," ",`
Keine	Keine	`, " " ,`	`," ",`
`"AnyProduct"`	`"NULL"`	`,AnyProduct,`	`,NULL,`
`"AnyProduct"`	`"NULL"`	`, AnyProduct ,`	`,NULL,`
`"AnyProduct"`	`"NULL"`	`,"AnyProduct",`	`,NULL,`
`"AnyProduct"`	`"NULL"`	`, "AnyProduct" ,`	`,NULL,`
Keine	`"NULL"`	`,,`	`,NULL,`

<csv-input-null>	**<csv-output-null>**	Eingabeeintrag	Ausgangseintrag
Keine	"NULL"	, ,	,NULL,
Keine	"NULL"	,"",	,NULL,
Keine	"NULL"	," ",	," ",
None	"NULL"	, " " ,	," ",
""	"NULL"	,,	,NULL,
""	"NULL"	, ,	,NULL,
""	"NULL"	,"",	,"",
""	"NULL"	," ",	," ",
""	"NULL"	, " " ,	," ",
"\"\""	"NULL"	,,	,,
"\"\""	"NULL"	, ,	,,
"\"\""	"NULL"	,"",	,NULL,
"\"\""	"NULL"	," ",	," ",
"\"\""	"NULL"	, " " ,	," ",

CSV-Datei ohne Header

Die CSV-Quelldatei muss keine Kopfzeilen in der ersten Zeile haben, die jede Spalte eindeutig benennen. Für eine CSV-Datei ohne Kopfzeile ist jedoch ein positionsbezogenes Verschlüsselungsschema erforderlich. Das Positionsverschlüsselungsschema ist anstelle des typischen Mapping-Schemas erforderlich, das sowohl für CSV-Dateien mit einer Kopfzeile als auch für Dateien verwendet wird. Parquet

Ein positionsabhängiges Verschlüsselungsschema spezifiziert Ausgabespalten nach Position statt nach Namen. Ein zugeordnetes Verschlüsselungsschema ordnet Quellspaltennamen

Zielspaltennamen zu. Weitere Informationen, einschließlich einer ausführlichen Erläuterung und Beispielen für beide Schemaformate, finden Sie unterSchemas für zugeordnete und positionierte Tabellen.

ParquetDateien

Es wird davon ausgegangen, dass eine Datei mit einer .parquet Erweiterung das Apache Parquet Format hat.

Unterstützte Parquet Datentypen

Der C3R-Verschlüsselungsclient kann alle nicht komplexen (d. h. primitiven Datentypen) Daten in einer Parquet Datei verarbeiten, die einen Datentyp darstellt, der von unterstützt wird. AWS Clean Rooms

Für Spalten können jedoch nur Zeichenkettenspalten verwendet werden. sealed

Die folgenden Parquet-Datentypen werden unterstützt:

- `Binary`primitiver Typ mit den folgenden logischen Anmerkungen:
  - Keine, wenn der gesetzt `--parquetBinaryAsString` ist (`STRING`Datentyp)
  - `Decimal(scale, precision)`(`DECIMAL`Datentyp)
  - `String`(`STRING`Datentyp)
- `Boolean`primitiver Datentyp ohne logische Anmerkung (`BOOLEAN`Datentyp)
- `Double`primitiver Datentyp ohne logische Anmerkung (`DOUBLE`Datentyp)
- `Fixed_Len_Binary_Array`primitiver Typ mit der `Decimal(scale, precision)` logischen Anmerkung (`DECIMAL`Datentyp)
- `Float`primitiver Datentyp ohne logische Anmerkung (`FLOAT`Datentyp)
- `Int32`primitiver Typ mit den folgenden logischen Anmerkungen:
  - Keiner (`INT`Datentyp)
  - `Date`(`DATE`Datentyp)
  - `Decimal(scale, precision)`(`DECIMAL`Datentyp)
  - `Int(16, true)`(`SMALLINT`Datentyp)
  - `Int(32, true)`(`INT`Datentyp)
- `Int64`primitiver Datentyp mit den folgenden logischen Anmerkungen:

- Keiner (`BIGINT`Datentyp)
- `Decimal(scale, precision)`(`DECIMAL`Datentyp)
- `Int(64, true)`(`BIGINT`Datentyp)
- `Timestamp(isUTCAdjusted, TimeUnit.MILLIS)`(`TIMESTAMP`Datentyp)
- `Timestamp(isUTCAdjusted, TimeUnit.MICROS)`(`TIMESTAMP`Datentyp)
- `Timestamp(isUTCAdjusted, TimeUnit.NANOS)`(`TIMESTAMP`Datentyp)

Verschlüsseln von Werten, die keine Zeichenfolge sind

Derzeit werden nur Zeichenkettenwerte für sealed Spalten unterstützt.

Bei CSV-Dateien behandelt der C3R-Verschlüsselungsclient alle Werte als UTF-8-codierten Text und versucht nicht, sie vor der Verschlüsselung unterschiedlich zu interpretieren.

Bei Fingerabdruckspalten werden die Typen in Äquivalenzklassen eingeteilt. Eine Äquivalenzklasse ist ein Satz von Datentypen, deren Gleichheit anhand eines repräsentativen Datentyps eindeutig verglichen werden kann.

Äquivalenzklassen ermöglichen es, identische Fingerabdrücke demselben semantischen Wert zuzuweisen, unabhängig von der ursprünglichen Darstellung. Derselbe Wert in zwei Äquivalenzklassen führt jedoch nicht zu derselben Fingerabdruckspalte.

Beispielsweise `42` wird dem `INTEGRAL` Wert derselbe Fingerabdruck zugewiesen, unabhängig davon, ob es sich ursprünglich um ein `SMALLINTINT`, oder `BIGINT` handelte. Außerdem `0` wird der `INTEGRAL` Wert niemals mit dem `BOOLEAN` Wert `FALSE` (der durch den Wert repräsentiert wird`0`) übereinstimmen.

Die folgenden Äquivalenzklassen und die entsprechenden AWS Clean Rooms Datentypen werden von Fingerabdruckspalten unterstützt:

Äquivalenzklasse	Unterstützter AWS Clean Rooms Datentyp
`BOOLEAN`	`BOOLEAN`
`DATE`	`DATE`

Äquivalenzklasse	Unterstützter AWS Clean Rooms Datentyp
INTEGRAL	BIGINT, INT, SMALLINT
STRING	CHAR, STRING, VARCHAR

Spaltennamen in Cryptographic Computing für Clean Rooms

Standardmäßig sind die Namen von Spalten in Cryptographic Computing for wichtig. Clean Rooms

Wenn der Wert des Parameters Spalten mit unterschiedlichen Namen zulassen JOIN auf False gesetzt ist, werden bei der Verschlüsselung von fingerprint Spalten Spaltennamen verwendet. Aus diesem Grund müssen sich Mitarbeiter standardmäßig im Voraus abstimmen und dieselben Zielspaltennamen für Daten verwenden, für die JOIN Anweisungen in Abfragen verwendet werden. Standardmäßig können Spalten, für die unterschiedliche Namen verschlüsselt wurden, JOIN JOIN bei keinem Wert erfolgreich verwendet werden.

Wenn der Wert des Parameters Spalten mit unterschiedlichen Namen zulassen JOIN wahr ist, sind JOIN Anweisungen für alle als Spalten verschlüsselten fingerprint Spalten erfolgreich. Das Verschlüsseln von Daten mit diesem Parameter ermöglicht möglicherweise einige Rückschlüsse auf die cleartext Werte. Wenn eine Zeile beispielsweise denselben HMAC-Wert (Hash-Based Message Authentication Code) sowohl in der Spalte als auch in der `City` Spalte hat, könnte `State` der Wert lauten. `New York`

Normalisierung der Namen der Spaltenüberschriften

Die Namen der Spaltenüberschriften werden vom C3R-Verschlüsselungsclient normalisiert. Alle Leerzeichen am Anfang und Ende werden entfernt, und der Spaltenname wird für die transformierte Ausgabe in Kleinbuchstaben geschrieben.

Die Normalisierung wird vor allen anderen Berechnungen, Berechnungen oder anderen Operationen angewendet, die möglicherweise durch Spaltennamen beeinflusst werden könnten. Die ausgegebene Ausgabedatei enthält nur die normalisierten Namen.

Spaltentypen in Cryptographic Computing für Clean Rooms

Dieses Thema enthält Informationen zu Spaltentypen in Cryptographic Computing for. Clean Rooms

Themen

FingerprintSpalten

FingerprintSpalten sind Spalten, die kryptografisch für die Verwendung in JOIN Anweisungen geschützt sind.

Daten aus fingerprint Spalten können nicht entschlüsselt werden. Nur Daten aus versiegelten Spalten können entschlüsselt werden.

FingerprintSpalten dürfen nur in den folgenden SQL-Klauseln und Funktionen verwendet werden:

- JOIN (INNER, OUTER, LEFT, RIGHT, or FULL)gegen andere fingerprint Spalten:
  - Wenn der Wert des `allowJoinsOnColumnsWithDifferentNames` Parameters auf gesetzt ist`false`, JOIN müssen beide fingerprint Spalten von ebenfalls denselben Namen haben.
- `SELECT COUNT()`
- `SELECT COUNT(DISTINCT )`
- `GROUP BY`(Nur verwenden, wenn die Kollaboration den Wert des `preserveNulls` Parameters auf festgelegt hat`true`.)

Abfragen, die gegen diese Einschränkungen verstoßen, können zu falschen Ergebnissen führen.

Versiegelte Spalten

Versiegelte Spalten sind Spalten, die kryptografisch für die Verwendung in SELECT Anweisungen geschützt sind.

Versiegelte Spalten dürfen nur in den folgenden SQL-Klauseln und Funktionen verwendet werden:

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

> **Note**
>
> `SELECT COUNT(DISTINCT )` wird nicht unterstützt.

Abfragen, die gegen diese Einschränkungen verstoßen, können zu falschen Ergebnissen führen.

Daten für eine sealed Spalte vor der Verschlüsselung auffüllen

Wenn Sie angeben, dass eine Spalte eine Spalte sein soll, fragt C3R Sie, welche Art von Polsterung Sie wählen sollen. sealed Das Auffüllen von Daten vor der Verschlüsselung ist optional. Ohne Auffüllung (ein Pad-Typ von`none`) gibt die Länge der verschlüsselten Daten die Größe des an. cleartext Unter bestimmten Umständen cleartext könnte die Größe von den Klartext offenlegen. Bei Padding (ein Pad-Typ von `fixed` oder`max`) werden alle Werte zunächst auf eine gemeinsame Größe aufgefüllt und dann verschlüsselt. Beim Padding gibt die Länge der verschlüsselten Daten keine Auskunft über die ursprüngliche cleartext Länge, es sei denn, es wird eine Obergrenze für die Größe angegeben.

Wenn Sie für eine Spalte eine Auffüllung wünschen und die maximale Bytelänge der Daten in dieser Spalte bekannt ist, verwenden Sie `fixed` Padding. Verwenden Sie einen `length` Wert, der mindestens so groß ist wie die Bytelänge des längsten Werts in dieser Spalte.

> **Note**
>
> Wenn ein Wert länger als der angegebene Wert ist, tritt ein Fehler auf und die Verschlüsselung schlägt fehl. `length`

Wenn Sie für eine Spalte eine Auffüllung wünschen und die maximale Bytelänge der Daten in dieser Spalte nicht bekannt ist, verwenden Sie `max` Padding. In diesem Auffüllmodus werden alle Daten auf die Länge des längsten Werts zuzüglich zusätzlicher Byte aufgefüllt. `length`

> **Note**
>
> Möglicherweise möchten Sie Daten stapelweise verschlüsseln oder Ihre Tabellen regelmäßig mit neuen Daten aktualisieren. Beachten Sie, dass beim `max` Auffüllen die Einträge auf die Länge (plus `length` Byte) des längsten Klartexteintrags in einem bestimmten Stapel

aufgefüllt werden. Das bedeutet, dass die Länge des Chiffretextes von Stapel zu Stapel variieren kann. Wenn Sie also die maximale Bytelänge für eine Spalte kennen, sollten Sie stattdessen die Option verwenden. `fixed max`

CleartextSpalten

CleartextSpalten sind Spalten, die nicht kryptografisch für die Verwendung in JOIN Oder-Anweisungen geschützt sind. SELECT

CleartextSpalten können in jedem Teil der SQL-Abfrage verwendet werden.

Kryptografische Rechenparameter

Kryptografische Rechenparameter sind für Kollaborationen verfügbar, bei denen Cryptographic Computing for Clean Rooms (C3R) beim Erstellen einer Kollaboration verwendet wird. Sie können eine Kollaboration entweder mithilfe der AWS Clean Rooms Konsole oder mithilfe der API-Operation erstellen. `CreateCollaboration` In der Konsole können Sie Werte für die Parameter unter Verschlüsselungsparameter festlegen, nachdem Sie die Option Kryptografisches Rechnen Support aktiviert haben. Weitere Informationen finden Sie unter den folgenden Themen.

Themen

- Parameter „Spalten zulassencleartext“
- Parameter „Duplikate zulassen“
- Parameter „Zulassen JOIN von Spalten mit unterschiedlichen Namen“
- Parameter „NULLWerte beibehalten“

Parameter „Spalten zulassencleartext“

In der Konsole können Sie beim Erstellen einer Kollaboration den Parameter cleartextSpalten zulassen festlegen, um anzugeben, ob cleartext Daten in einer Tabelle mit verschlüsselten Daten zulässig sind.

In der folgenden Tabelle werden die Werte für den Parameter Allow cleartext columns beschrieben.

Parameterwert	Beschreibung
Nein	CleartextSpalten sind in der verschlüsselten Tabelle nicht zulässig. Alle Daten sind kryptografisch geschützt.
Ja	CleartextSpalten sind in der verschlüsselten Tabelle zulässig. CleartextSpalten sind nicht kryptografisch geschützt und werden als aufgenommen. cleartext Sie sollten sich notieren, was die Daten Ihrer Zeilen über die anderen cleartext Daten in der Tabelle aussagen könnten. Um SUM oder AVG für bestimmte Spalten ausführen zu können, müssen sich die Spalten in cleartext befinden.

Mithilfe der `CreateCollaboration` API-Operation können Sie für den `dataEncryptionMetadata` Parameter den Wert `allowCleartext` auf `true` oder festlegen`false`. Weitere Informationen zu API-Vorgängen finden Sie in der AWS Clean Rooms API-Referenz.

CleartextSpalten entsprechen Spalten, die cleartext im tabellenspezifischen Schema als Spalten klassifiziert sind. Die Daten in diesen Spalten sind nicht verschlüsselt und können auf beliebige Weise verwendet werden. CleartextSpalten können nützlich sein, wenn die Daten nicht sensibel sind und/oder wenn mehr Flexibilität erforderlich ist, als es eine verschlüsselte sealed Spalte oder fingerprint Spalte zulässt.

Parameter „Duplikate zulassen“

In der Konsole können Sie beim Erstellen einer Kollaboration den Parameter Duplikate zulassen festlegen, um anzugeben, ob für JOIN Abfragen verschlüsselte Spalten doppelte Nichtwerte enthalten können. NULL

> **Important**
>
> Die Parameter „Duplikate zulassenJOIN“, „Spalten mit unterschiedlichen Namen zulassen“ und „NULLWerte beibehalten“ haben unterschiedliche, aber verwandte Auswirkungen.

In der folgenden Tabelle werden die Werte für den Parameter Duplikate zulassen beschrieben.

Parameterwert	Beschreibung
Nein	Wiederholte Werte sind in einer fingerprint Spalte nicht zulässig. Alle Werte in einer einzelnen fingerprint Spalte müssen eindeutig sein.
Ja	Wiederholte Werte sind in einer fingerprint Spalte zulässig. Wenn Sie Spalten mit wiederholten Werten verbinden müssen, setzen Sie diesen Wert auf Ja. Wenn diese Option auf Ja gesetzt ist, können Häufigkeitsmuster, die in den fingerprint Spalten der C3R-Tabelle oder der Ergebnisse erscheinen, zusätzliche Informationen über die Struktur der cleartext Daten enthalten.

Mithilfe der `CreateCollaboration` API-Operation können Sie für den `dataEncryptionMetadata` Parameter den Wert `allowDuplicates` auf `true` oder `false` festlegen. Weitere Informationen zu API-Vorgängen finden Sie in der AWS Clean Rooms API-Referenz.

Wenn verschlüsselte Daten in JOIN Abfragen verwendet werden müssen, verlangt der C3R-Verschlüsselungsclient standardmäßig, dass diese Spalten keine doppelten Werte enthalten. Diese Anforderung ist ein Versuch, den Datenschutz zu verbessern. Dieses Verhalten kann dazu beitragen, dass wiederholte Muster in den Daten nicht beobachtbar sind. Wenn Sie jedoch mit verschlüsselten Daten in JOIN Abfragen arbeiten möchten und sich keine Gedanken über doppelte Werte machen, kann der Parameter Duplikate zulassen diese konservative Prüfung deaktivieren.

Parameter „Zulassen JOIN von Spalten mit unterschiedlichen Namen“

In der Konsole können Sie beim Erstellen einer Kollaboration den Parameter Spalten mit unterschiedlichen Namen zulassen JOIN festlegen, um anzugeben, ob JOIN Anweisungen zwischen Spalten mit unterschiedlichen Namen unterstützt werden.

Weitere Informationen finden Sie unter Normalisierung der Namen der Spaltenüberschriften .

In der folgenden Tabelle werden die Werte für den Parameter Zulassen JOIN von Spalten mit unterschiedlichen Namen beschrieben.

Parameterwert	Beschreibung
Nein	Verknüpfungen von fingerprint Spalten mit unterschiedlichen Namen werden nicht unterstützt. JOINAnweisungen liefern nur genaue Ergebnisse für Spalten, die denselben Namen haben. **Important** Der Wert „Nein“ erhöht die Informationssicherheit, erfordert jedoch, dass sich die Kollaborationsteilnehmer zuvor über die Spaltennamen einigen. Wenn zwei Spalten unterschiedliche Namen haben, wenn sie als fingerprint Spalten verschlüsselt sind und Spalten mit unterschiedlichen Namen zulassen JOIN auf Nein gesetzt ist, führen JOIN Anweisungen zu diesen Spalten zu keinen Ergebnissen. Das liegt daran, dass sie nach der Verschlüsselung keine Werte gemeinsam nutzen.
Ja	Verknüpfungen von fingerprint Spalten mit unterschiedlichen Namen werden unterstützt. Für zusätzliche Flexibilität können Benutzer diesen Wert auf Ja setzen, sodass JOIN Aussagen zu Spalten unabhängig von deren Spaltennamen möglich sind. Wenn dieser Wert auf Ja gesetzt ist, berücksichtigt der C3R-Verschlüsselungsclient den Spaltennamen beim Schutz von fingerprint Spalten nicht. Daher sind gemeinsame Werte in verschiedenen fingerprint Spalten in der C3R-Tabelle beobachtbar. Wenn eine Zeile beispielsweise denselben verschlüsselten JOIN Wert sowohl in einer Spalte als auch in einer `City` Spalte hat, kann es sinnvoll sein, daraus zu schließen, dass dieser Wert ist. `State` `New York`

Mithilfe der `CreateCollaboration` API-Operation können Sie für den `dataEncryptionMetadata` Parameter den Wert `allowJoinsOnColumnsWithDifferentNames` auf `true` oder `false` festlegen. Weitere Informationen zu API-Vorgängen finden Sie in der AWS Clean Rooms API-Referenz.

Standardmäßig wird die fingerprint Spaltenverschlüsselung durch die `targetHeader` für diese Spalte eingestellte Einstellung beeinflusstSchritt 4: Generieren Sie ein Verschlüsselungsschema für eine tabellarische Datei . Daher hat derselbe cleartext Wert in jeder fingerprint Spalte, für die er verschlüsselt ist, unterschiedliche verschlüsselte Darstellungen.

Dieser Parameter kann in einigen Fällen nützlich sein, um die Inferenz von cleartext Werten zu verhindern. `StateEs` kann beispielsweise verwendet werden, wenn derselbe verschlüsselte Wert in fingerprint Spalten angezeigt `City` wird, um vernünftigerweise auf den Wert schließen zu können. `New York` Die Verwendung dieses Parameters erfordert jedoch eine zusätzliche Abstimmung im Voraus, sodass alle Spalten, die in Abfragen verknüpft werden sollen, gemeinsame Namen haben.

Sie können den Parameter Zulassen JOIN von Spalten mit unterschiedlichen Namen verwenden, um diese Einschränkung zu lockern. Wenn der Parameterwert auf gesetzt ist`Yes`, können alle Spalten, für die verschlüsselt wurdeJOIN, unabhängig vom Namen zusammen verwendet werden.

Parameter „NULLWerte beibehalten“

In der Konsole können Sie beim Erstellen einer Kollaboration den Parameter NULLWerte beibehalten so einstellen, dass für diese Spalte kein Wert vorhanden ist.

In der folgenden Tabelle werden die Werte für den Parameter NULLWerte beibehalten beschrieben.

Parameterwert	Beschreibung
Nein	NULLWerte werden nicht beibehalten. NULLWerte werden nicht wie NULL in einer verschlüsselten Tabelle angezeigt . NULLWerte werden in einer C3R-Tabelle als eindeutige Zufallswerte angezeigt.
Ja	NULLWerte werden beibehalten. NULLWerte werden wie NULL in einer verschlüsselten Tabelle angezeigt. Wenn Sie eine SQL-Semantik für NULL Werte benötigen, können Sie diesen Wert auf Ja setzen. Daher werden NULL Einträge wie NULL in der C3R-Tabelle angezeigt, unabhängig davon, ob

Parameterwert	Beschreibung
	die Spalte verschlüsselt ist und unabhängig von der Parameter einstellung für Duplikate zulassen.

Mithilfe der `CreateCollaboration` API-Operation können Sie für den `dataEncryptionMetadata` Parameter den Wert auf oder festlegen. `preserveNulls` `true` `false` Weitere Informationen zu API-Vorgängen finden Sie in der AWS Clean Rooms API-Referenz.

Wenn der Parameter NULLWerte beibehalten für die Zusammenarbeit auf Nein gesetzt ist:

1. NULLEinträge in `cleartext` Spalten sind unverändert.
2. NULLEinträge in verschlüsselten `fingerprint` Spalten werden als Zufallswerte verschlüsselt, um ihren Inhalt zu verbergen. Bei der Verknüpfung zu einer verschlüsselten Spalte mit NULL Einträgen in der cleartext Spalte ergeben sich keine Treffer für einen der NULL Einträge. Es werden keine Treffer erzielt, da sie jeweils ihren eigenen, eindeutigen zufälligen Inhalt erhalten.
3. NULLEinträge in verschlüsselten `sealed` Spalten sind verschlüsselt.

Wenn der Wert des Parameters NULLWerte beibehalten für die Kollaboration auf Ja gesetzt ist, bleiben die NULL Einträge aus allen Spalten unverändert, NULL unabhängig davon, ob die Spalte verschlüsselt ist.

Der Parameter NULLWerte beibehalten ist nützlich in Szenarien wie der Datenanreicherung, in denen Sie fehlende Informationen weitergeben möchten, ausgedrückt alsNULL. Der Parameter NULLWerte beibehalten ist auch im fingerprint oder HMAC-Format nützlich, wenn Sie NULL Werte in der gewünschten Spalte haben oder. JOIN GROUP BY

Wenn der Wert der Parameter Duplikate zulassen und NULLWerte beibehalten auf Nein gesetzt ist, führt das Vorhandensein von mehr als einem NULL Eintrag in einer fingerprint Spalte zu einem Fehler und die Verschlüsselung wird gestoppt. Wenn der Wert eines der beiden Parameter auf Ja gesetzt ist, tritt kein solcher Fehler auf.

Optionale Flags in Cryptographic Computing für Clean Rooms

In den folgenden Abschnitten werden die optionalen Flags beschrieben, die Sie festlegen können, wenn Sie Daten mit dem C3R-Verschlüsselungsclient verschlüsseln, um tabellarische Dateien anzupassen und zu testen.

Themen

`--csvInputNULLValue`Flagge

Sie können das `--csvInputNULLValue` Flag verwenden, um benutzerdefinierte Kodierungen für NULL Einträge in den Eingabedaten anzugeben, wenn Sie Daten mit dem C3R-Verschlüsselungsclient verschlüsseln.

In der folgenden Tabelle werden die Verwendung und die Parameter dieses Flags zusammengefasst.

Verwendung	Parameter
Optional. Benutzer können benutzerdefinierte Kodierungen für NULL Einträge in den Eingabedaten angeben.	Benutzerdefinierte Kodierung von NULL Werten in der CSV-Eingabedatei

Ein NULL Eintrag ist ein Eintrag, der als inhaltslos angesehen wird, insbesondere im Zusammenhang mit einem umfangreicheren Tabellenformat wie einer SQL-Tabelle. Obwohl .csv diese Charakterisierung aus historischen Gründen nicht ausdrücklich unterstützt, ist es üblich, einen leeren Eintrag, der nur Leerraum enthält, als solche zu betrachten. NULL Daher ist dies das Standardverhalten des C3R-Verschlüsselungsclients und kann nach Bedarf angepasst werden.

`--csvOutputNULLValue`Flagge

Sie können das `--csvOutputNULLValue` Flag verwenden, um benutzerdefinierte Kodierungen für NULL Einträge in den Ausgabedaten anzugeben, wenn Sie Daten mit dem C3R-Verschlüsselungsclient verschlüsseln.

In der folgenden Tabelle werden die Verwendung und die Parameter dieses Flags zusammengefasst.

Verwendung	Parameter
Optional. Benutzer können in der generierten Ausgabedatei für NULL Einträge benutzerd efinierte Kodierungen angeben.	Benutzerdefinierte Kodierung von NULL Werten in der CSV-Ausgabedatei

Ein NULL Eintrag ist ein Eintrag, der als inhaltslos angesehen wird, insbesondere im Zusammenhang mit einem umfangreicheren Tabellenformat wie einer SQL-Tabelle. Obwohl .csv diese Charakterisierung aus historischen Gründen nicht ausdrücklich unterstützt, ist es üblich, einen leeren Eintrag, der nur Leerraum enthält, als solche zu betrachten. NULL Daher ist dies das Standardverhalten des C3R-Verschlüsselungsclients und kann nach Bedarf angepasst werden.

`--enableStackTraces`Flagge

Wenn Sie Daten mit dem C3R-Verschlüsselungsclient verschlüsseln, verwenden Sie das `--enableStackTraces` Flag, um zusätzliche Kontextinformationen für die Fehlerberichterstattung bereitzustellen, wenn C3R auf einen Fehler stößt.

AWS sammelt keine Fehler. Wenn Sie auf einen Fehler stoßen, verwenden Sie den Stack-Trace, um den Fehler selbst zu beheben, oder senden Sie den Stack-Trace an, um AWS Support Unterstützung zu erhalten.

In der folgenden Tabelle werden die Verwendung und die Parameter dieses Flags zusammengefasst.

Verwendung	Parameter
Optional. Wird verwendet, um zusätzliche Kontextinformationen für die Fehlerberichtersta ttung bereitzustellen, wenn der C3R-Versc hlüsselungsclient auf einen Fehler stößt.	None

`--dryRun`Flagge

Die Befehle zum Verschlüsseln und Entschlüsseln von C3R-Verschlüsselungsclients enthalten ein optionales Flag. `--dryRun` Das Flag verwendet alle vom Benutzer angegebenen Argumente und überprüft sie auf Gültigkeit und Konsistenz.

Sie können das `--dryRun` Flag verwenden, um zu überprüfen, ob Ihre Schemadatei gültig ist und mit der entsprechenden Eingabedatei konsistent ist.

In der folgenden Tabelle werden die Verwendung und die Parameter dieses Flags zusammengefasst.

Verwendung	Parameter
Optional. Bewirkt, dass der C3R-Versc hlüsselungsclient Parameter analysiert und Dateien überprüft, aber keine Verschlüsselung oder Entschlüsselung durchführt.	None

`--tempDir`Flagge

Möglicherweise möchten Sie ein temporäres Verzeichnis verwenden, da verschlüsselte Dateien je nach ihren Einstellungen manchmal größer sein können als unverschlüsselte Dateien. Datensätze müssen außerdem pro Kollaboration verschlüsselt werden, damit sie korrekt funktionieren.

Wenn Sie Daten mit C3R verschlüsseln, verwenden Sie das `--tempDir` Flag, um den Speicherort anzugeben, an dem temporäre Dateien während der Verarbeitung der Eingabe erstellt werden können.

In der folgenden Tabelle werden die Verwendung und die Parameter dieses Flags zusammengefasst.

Verwendung	Parameter
Benutzer können den Speicherort angeben, an dem temporäre Dateien während der Verarbeit ung der Eingabe erstellt werden können.	Standardmäßig wird das temporäre Systemver zeichnis verwendet.

Abfragen mit Cryptographic Computing für Clean Rooms

Dieses Thema enthält Informationen zum Schreiben von Abfragen, die Datentabellen verwenden, die mithilfe von Cryptographic Computing for verschlüsselt wurden. Clean Rooms

Themen

- Abfragen, die sich wie folgt verzweigen NULL

- Zuordnen einer Quellspalte zu mehreren Zielspalten
- Verwenden Sie dieselben Daten für beide JOINSELECT Abfragen

Abfragen, die sich wie folgt verzweigen NULL

Eine Abfrageverzweigung für eine NULL Anweisung zu haben, bedeutet, eine Syntax wie zu verwenden`IF x IS NULL THEN 0 ELSE 1`.

Abfragen können sich immer auf NULL Anweisungen in cleartext Spalten verzweigen.

Abfragen können sich nur dann auf NULL Anweisungen in sealed Spalten und fingerprint Spalten stützen, wenn der Wert des Parameters NULL-Werte beibehalten (`preserveNulls`) auf gesetzt ist`true`.

Abfragen, die gegen diese Einschränkungen verstoßen, können zu falschen Ergebnissen führen.

Zuordnen einer Quellspalte zu mehreren Zielspalten

Eine Quellspalte kann mehreren Zielspalten zugeordnet werden. Beispielsweise möchten Sie vielleicht beides JOIN und SELECT eine Spalte gleichzeitig verwenden.

Weitere Informationen finden Sie unter Verwenden Sie dieselben Daten für beide JOINSELECT Abfragen.

Verwenden Sie dieselben Daten für beide JOINSELECT Abfragen

Wenn die Daten in einer Spalte nicht vertraulich sind, können sie in einer cleartext Zielspalte erscheinen, sodass sie für jeden Zweck verwendet werden können.

Wenn Daten in einer Spalte vertraulich sind JOIN und sowohl für SELECT Abfragen als auch verwendet werden müssen, ordnen Sie diese Quellspalte zwei Zielspalten in der Ausgabedatei zu. Eine Spalte ist mit der `type` als fingerprint Spalte verschlüsselt, und eine Spalte ist mit der `type` als versiegelte Spalte verschlüsselt. Die interaktive Schemagenerierung des C3R-Verschlüsselungsclients schlägt Header-Suffixe von und vor. `_fingerprint` `_sealed` Diese Header-Suffixe können eine nützliche Konvention sein, um solche Spalten schnell zu unterscheiden.

Richtlinien für den C3R-Verschlüsselungsclient

Der C3R-Verschlüsselungsclient ist ein Tool, mit dem Unternehmen sensible Daten zusammenführen können, um aus Datenanalysen neue Erkenntnisse zu gewinnen. Das Tool schränkt kryptografisch

ein, was von jeder Partei und AWS während des Prozesses gelernt werden kann. Dies ist zwar von entscheidender Bedeutung, aber der Prozess der kryptografischen Sicherung von Daten kann zu einem erheblichen Mehraufwand sowohl in Bezug auf Rechen- als auch Speicherressourcen führen. Daher ist es wichtig, die Kompromisse bei der Verwendung der einzelnen Einstellungen zu verstehen und zu verstehen, wie die Einstellungen optimiert und gleichzeitig die gewünschten kryptografischen Garantien beibehalten werden können. Dieses Thema konzentriert sich auf die Auswirkungen verschiedener Einstellungen im C3R-Verschlüsselungsclient und in den Schemas auf die Leistung.

Alle Verschlüsselungseinstellungen des C3R-Verschlüsselungsclients bieten unterschiedliche kryptografische Garantien. Die Einstellungen auf Kollaborationsebene sind standardmäßig am sichersten. Durch die Aktivierung zusätzlicher Funktionen bei gleichzeitiger Schaffung einer Zusammenarbeit werden die Datenschutzgarantien geschwächt, sodass Aktivitäten wie Frequenzanalysen anhand des Chiffretextes durchgeführt werden können. Weitere Informationen darüber, wie diese Einstellungen verwendet werden und welche Auswirkungen sie haben, finden Sie unter. Kryptografisches Rechnen

Themen

- Auswirkungen auf die Leistung von Spaltentypen
- Behebung unerwarteter Zunahmen der Chiffretext-Größe

Auswirkungen auf die Leistung von Spaltentypen

C3R verwendet drei Spaltentypen: cleartextfingerprint, undsealed. Jeder dieser Spaltentypen bietet unterschiedliche kryptografische Garantien und hat unterschiedliche Verwendungszwecke. In den folgenden Abschnitten werden die Auswirkungen des Spaltentyps auf die Leistung sowie die Auswirkungen der einzelnen Einstellungen auf die Leistung erörtert.

Themen

- CleartextSpalten
- FingerprintSpalten
- SealedSpalten

CleartextSpalten

CleartextSpalten werden gegenüber ihrem ursprünglichen Format nicht verändert und in keiner Weise kryptografisch verarbeitet. Dieser Spaltentyp kann nicht konfiguriert werden und beeinträchtigt weder die Speicher- noch die Rechenleistung.

FingerprintSpalten

FingerprintSpalten sollen verwendet werden, um Daten aus mehreren Tabellen zu verbinden. Zu diesem Zweck muss die resultierende Chiffretextgröße immer dieselbe sein. Diese Spalten werden jedoch von den Einstellungen auf Kollaborationsebene beeinflusst. FingerprintSpalten können sich unterschiedlich stark auf die Größe der Ausgabedatei auswirken, je nachdem, was in der Eingabe cleartext enthalten ist.

Themen

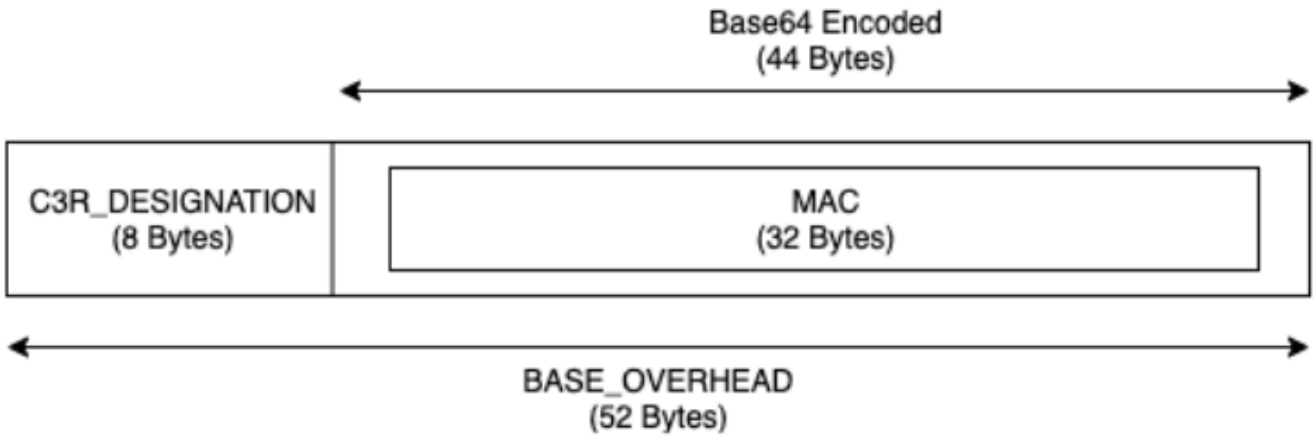
- Basis-Overhead für fingerprint Spalten
- Einstellungen für die Zusammenarbeit für fingerprint Spalten
- Beispieldaten für eine fingerprint Spalte
- Problembehandlung bei fingerprint Spalten

Basis-Overhead für fingerprint Spalten

Es gibt einen Basisgemeinkosten für fingerprint Spalten. Dieser Overhead ist konstant und ersetzt die Größe der cleartext Bytes.

Die Daten in den fingerprint Spalten werden mithilfe einer Hash-basierten HMAC-Funktion (Message Authentication Code) kryptografisch verarbeitet, die die Daten in einen 32-Byte-Nachrichtenauthentifizierungscode (MAC) umwandelt. Diese Daten werden dann über einen Base64-Encoder verarbeitet, wodurch die Bytegröße um etwa 33 Prozent erhöht wird. Ihm wird eine 8-Byte-C3R-Bezeichnung vorangestellt, um den Spaltentyp zu bezeichnen, zu dem die Daten gehören, und die Client-Version, die sie erzeugt hat. Das Endergebnis ist 52 Byte. Dieses Ergebnis wird dann mit der Zeilenanzahl multipliziert, um den gesamten Basis-Overhead zu erhalten (verwenden Sie die Anzahl der gesamten `null` Nichtwerte, wenn der Wert auf „true“ gesetzt `preserveNulls` ist).

Die folgende Abbildung zeigt, wie $BASE\_OVERHEAD = C3R\_DESIGNATION + (MAC * 1.33)$



Der ausgegebene Chiffretext in den fingerprint Spalten wird immer 52 Byte lang sein. Dies kann zu einer erheblichen Verringerung des Speicherplatzes führen, wenn die cleartext Eingabedaten im Durchschnitt mehr als 52 Byte umfassen (z. B. vollständige Straßenadressen). Dies kann eine erhebliche Speichererweiterung bedeuten, wenn die cleartext Eingabedaten im Durchschnitt weniger als 52 Byte enthalten (z. B. aufgrund des Alters des Kunden).

Einstellungen für die Zusammenarbeit für fingerprint Spalten

`preserveNulls`-Einstellung

Wenn die Einstellung `preserveNulls` auf Kollaborationsebene `false` (Standard) lautet, wird jeder `null` Wert durch eindeutige, zufällige 32 Byte ersetzt und so verarbeitet, als ob dies nicht der Fall wäre. `null` Das Ergebnis ist, dass jeder `null` Wert jetzt 52 Byte groß ist. Dies kann zu erheblichen Speicheranforderungen für Tabellen führen, die nur sehr wenige Daten enthalten, verglichen mit der Einstellung, bei der `null` Werte übergeben werden. `true` `null`

Wenn Sie die Datenschutzgarantien dieser Einstellung nicht benötigen und es vorziehen, `null` Werte in Ihren Datensätzen beizubehalten, aktivieren Sie die `preserveNulls` Einstellung bei der Erstellung der Kollaboration. Die `preserveNulls` Einstellung kann nach der Erstellung der Kollaboration nicht mehr geändert werden.

Beispieldaten für eine fingerprint Spalte

Im Folgenden finden Sie ein Beispiel für Eingabe- und Ausgabedaten für eine fingerprint Spalte mit Einstellungen zur Reproduktion. Andere Einstellungen auf Kollaborationsebene wirken sich wie `allowCleartext` und `allowDuplicates` nicht auf die Ergebnisse aus und können so eingestellt werden, als `true` `false` ob versucht wird, lokal zu reproduzieren.

Beispiel für ein geteiltes Geheimnis: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Beispiel für eine Kollaborations-ID: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

allowJoinsOnColumnsWithDifferentNames: `True` Diese Einstellung hat keinen Einfluss auf die Leistungs- oder Speicheranforderungen. Diese Einstellung macht die Wahl des Spaltennamens jedoch irrelevant, wenn die Werte in den folgenden Tabellen wiedergegeben werden.

Beispiel 1

Eingabe	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministisch	`Yes`
Eingabe-Bytes	0
Ausgabe-Bytes	0

Beispiel 2

Eingabe	`null`
`preserveNulls`	`FALSE`
Output	`01:hmac:3lkFjthvV3IUu6mMvFc1a +XAHwgw/ElmOq4p3Yg25kk=`
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	52

Beispiel 3

Eingabe	`empty string`
`preserveNulls`	-

Output	`01:hmac:oKTgi3Gba+eUb3JteSz 2EMgXUkF1WgM77UP0Ydw5kPQ=`
Deterministisch	`Yes`
Eingabe-Bytes	0
Ausgabe-Bytes	52

Beispiel 4

Eingabe	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:hmac:kU/IqwG7FMmzzshr0B9 scomE0UJUEE7j9keTctplGww=`
Deterministisch	`Yes`
Eingabe-Bytes	26
Ausgabe-Bytes	52

Beispiel 5

Eingabe	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Output	`01:hmac:ks3htnQbw2vdhCRFF6J NzW5LMndJaHG57uvE26mBtSs=`
Deterministisch	`Yes`
Eingabe-Bytes	62

Ausgabe-Bytes	52

Problembehandlung bei fingerprint Spalten

Warum ist der Chiffretext in meinen fingerprint Spalten um ein Vielfaches größer als cleartext der Inhalt?

Der Chiffretext in einer fingerprint Spalte ist immer 52 Byte lang. Wenn Ihre Eingabedaten klein waren (z. B. das Alter der Kunden), wurde sie deutlich größer. Dies kann auch passieren, wenn die `preserveNulls` Einstellung auf gesetzt ist`false`.

Warum ist der Chiffretext in meinen fingerprint Spalten um ein Vielfaches kleiner als cleartext der Inhalt?

Der Chiffretext in einer fingerprint Spalte ist immer 52 Byte lang. Wenn Ihre Eingabedaten umfangreich sind (z. B. die vollständigen Straßenadressen von Kunden), ist die Größe deutlich geringer.

Woher weiß ich, ob ich die kryptografischen Garantien von benötige? **`preserveNulls`**

Leider lautet die Antwort, dass es darauf ankommt. Zumindest the section called “Parameter” sollte überprüft werden, wie die `preserveNulls` Einstellung Ihre Daten schützt. Wir empfehlen Ihnen jedoch, die Datenverarbeitungsanforderungen Ihres Unternehmens und alle Verträge, die für die jeweilige Zusammenarbeit gelten, zu beachten.

Warum muss ich den Overhead von Base64 auf mich nehmen?

Um die Kompatibilität mit tabellarischen Dateiformaten wie CSV zu gewährleisten, ist eine Base64-Kodierung erforderlich. Zwar unterstützen einige Dateiformate wie z. Parquet B. binäre Darstellungen von Daten, es ist jedoch wichtig, dass alle Teilnehmer einer Zusammenarbeit Daten auf die gleiche Weise darstellen, um korrekte Abfrageergebnisse zu gewährleisten.

SealedSpalten

SealedSpalten sollen für die Übertragung von Daten zwischen Mitgliedern einer Kollaboration verwendet werden. Der Geheimtext in diesen Spalten ist nicht deterministisch und hat je nach Konfiguration der Spalten erhebliche Auswirkungen sowohl auf die Leistung als auch auf den Speicherplatz. Diese Spalten können individuell konfiguriert werden und haben oft den größten

Einfluss auf die Leistung des C3R-Verschlüsselungsclients und die daraus resultierende Größe der Ausgabedatei.

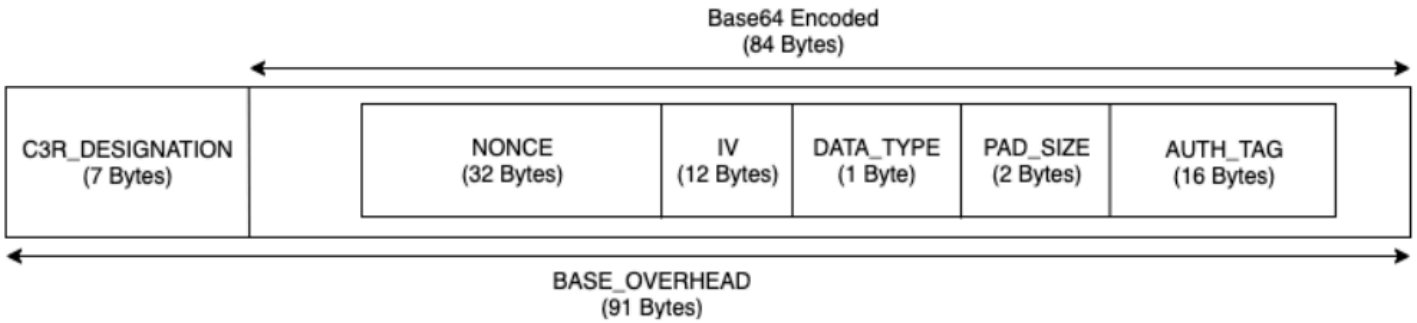
Themen

Basis-Overhead für Spalten sealed

Es gibt einen Basisgemeinkosten für sealed Spalten. Dieser Overhead ist konstant und kommt zu der Größe der Byte cleartext und der Füllmenge (falls vorhanden) hinzu.

Vor jeder Verschlüsselung wird den Daten in den sealed Spalten ein 1-Byte-Zeichen vorangestellt, das angibt, welcher Datentyp enthalten ist. Wenn Padding ausgewählt ist, werden die Daten aufgefüllt und mit 2 Byte angehängt, die die Pad-Größe angeben. Nachdem diese Byte hinzugefügt wurden, werden die Daten mithilfe von AES-GCM kryptografisch verarbeitet und mit IV (12 Byte), (32 Byte) und nonce (16 Byte) gespeichert. Auth Tag Diese Daten werden dann durch einen Base64-Encoder verarbeitet, wodurch die Bytegröße um etwa 33 Prozent erhöht wird. Den Daten wird eine 7-Byte-C3R-Bezeichnung vorangestellt, um anzugeben, zu welchem Spaltentyp die Daten gehören und welche Client-Version verwendet wurde, um sie zu erzeugen. Das Ergebnis ist ein endgültiger Basisaufwand von 91 Byte. Dieses Ergebnis kann dann mit der Zeilenanzahl multipliziert werden, um den gesamten Basis-Overhead zu erhalten (verwenden Sie die Anzahl der Gesamtwerte ungleich Null, wenn der Wert auf true gesetzt `preserveNulls` ist).

Die folgende Abbildung zeigt, wie *`BASE_OVERHEAD = C3R_DESIGNATION + ((NONCE + IV + DATA_TYPE + PAD_SIZE + AUTH_TAG) * 1.33)`*



Einstellungen für die Zusammenarbeit für sealed Spalten

`preserveNulls`-Einstellung

Wenn die Einstellung auf Kollaborationsebene auf `false` (Standard) gesetzt `preserveNulls` ist, ist jeder `null` Wert einmalig, hat 32 Byte Zufallswerte und wird so verarbeitet, als ob dies nicht der Fall wäre. `null` Das Ergebnis ist, dass jeder `null` Wert jetzt 91 Byte groß ist (mehr, wenn er aufgefüllt wird). Dies kann zu erheblichen Speicheranforderungen für Tabellen führen, die nur sehr wenige Daten enthalten, als wenn diese Einstellung aktiviert ist `true` und `null` Werte als `null` übergeben werden.

Wenn Sie die Datenschutzgarantien dieser Einstellung nicht benötigen und es vorziehen, `null` Werte in Ihren Datensätzen beizubehalten, aktivieren Sie die `preserveNulls` Einstellung bei der Erstellung der Kollaboration. Die `preserveNulls` Einstellung kann nach der Erstellung der Kollaboration nicht mehr geändert werden.

sealedSpalten mit Schemaeinstellungen: Polstertypen

Themen

- Pad-Typ von none
- Pad-Typ von fixed
- Pad-Typ von max

Pad-Typ von **`none`**

Durch die Auswahl des Padtyps von `none` wird dem zuvor beschriebenen Grund-Overhead keine Polsterung hinzugefügt cleartext und auch kein zusätzlicher Overhead hinzugefügt. Wenn keine Polsterung vorhanden ist, ergibt sich die platzsparendste Ausgabegröße. Es bietet jedoch nicht die gleichen Datenschutzgarantien wie die Polstertypen `fixed` und`max`. Das liegt daran, dass die Größe des Basistextes anhand der Größe des Chiffretextes erkennbar cleartext ist.

Pad-Typ von **`fixed`**

Die Auswahl des Pad-Typs von `fixed` dient dem Schutz der Privatsphäre, um die Länge der in einer Spalte enthaltenen Daten zu verbergen. Dies wird erreicht, indem das gesamte Feld mit dem angegebenen Feld ausgefüllt wirdcleartext, `pad_length` bevor es verschlüsselt wird. Alle Daten, die diese Größe überschreiten, führen dazu, dass der C3R-Verschlüsselungsclient fehlschlägt.

Da das Padding cleartext vor der Verschlüsselung hinzugefügt wird, hat AES-GCM eine 1-zu-1-Zuordnung von Chiffretext-Bytes. cleartext Durch die Base64-Kodierung werden 33 Prozent hinzukommen. Der zusätzliche Speicheraufwand des Padding kann berechnet werden, indem die durchschnittliche Länge von vom Wert von subtrahiert `pad_length` und mit 1,33 multipliziert wird. cleartext Das Ergebnis ist der durchschnittliche Mehraufwand für das Auffüllen pro Datensatz. Dieses Ergebnis kann dann mit der Anzahl der Zeilen multipliziert werden, um den gesamten Auffüllaufwand zu erhalten (verwenden Sie die Anzahl der gesamten `null` Nichtwerte, falls `preserveNulls` auf gesetzt). `true`

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

Es wird empfohlen, das Minimum auszuwählen`pad_length`, das den größten Wert in einer Spalte umfasst. Wenn der größte Wert beispielsweise 50 Byte beträgt, ist ein Wert `pad_length` von 50 ausreichend. Ein höherer Wert erhöht nur zusätzlichen Speicheraufwand.

Eine feste Polsterung erhöht keinen nennenswerten Rechenaufwand.

Pad-Typ von **`max`**

Die Auswahl des Pad-Typs von `max` dient dem Schutz der Privatsphäre, um die Länge der in einer Spalte enthaltenen Daten zu verbergen. Dies wird erreicht, indem der cleartext gesamte Wert mit dem größten Wert in der Spalte und dem zusätzlichen Wert aufgefüllt wird, `pad_length` bevor die Spalte verschlüsselt wird. Im Allgemeinen bietet `max` das Auffüllen die gleiche Sicherheit wie das Auffüllen `fixed` eines einzelnen Datensatzes, ermöglicht jedoch, dass der größte cleartext Wert in der Spalte nicht bekannt ist. Das Auffüllen `max` bietet jedoch möglicherweise nicht die gleichen Datenschutzgarantien wie `fixed` das Auffüllen bei Aktualisierungen, da der größte Wert in den einzelnen Datensätzen unterschiedlich sein kann.

Wir empfehlen, dass Sie bei der Verwendung von Padding einen zusätzlichen Wert `pad_length` von 0 wählen. `max` Bei dieser Länge werden alle Werte so aufgefüllt, dass sie dieselbe Größe wie der größte Wert in der Spalte haben. Ein höherer Wert erhöht nur zusätzlichen Speicheraufwand.

Wenn der größte cleartext Wert für eine bestimmte Spalte bekannt ist, empfehlen wir, stattdessen den `fixed` Pad-Typ zu verwenden. Die Verwendung von `fixed` Padding sorgt für Konsistenz zwischen aktualisierten Datensätzen. Die Verwendung `max` von Auffüllung führt dazu, dass jede Teilmenge der Daten mit dem größten Wert aufgefüllt wird, der in der Teilmenge enthalten war.

Beispieldaten für eine Spalte sealed

Im Folgenden finden Sie ein Beispiel für Eingabe- und Ausgabedaten für eine sealed Spalte mit Einstellungen zur Reproduktion. Andere Einstellungen auf Kollaborationsebene wie

`allowCleartext`allowJoinsOnColumnsWithDifferentNames, und wirken sich `allowDuplicates` nicht auf die Ergebnisse aus und können so eingestellt werden, als `true` `false` ob versucht wird, sich lokal zu reproduzieren. Dies sind zwar die Grundeinstellungen für die Reproduktion, aber die sealed Spalte ist nicht deterministisch und die Werte ändern sich jedes Mal. Das Ziel besteht darin, die eingehenden Byte im Vergleich zu den ausgehenden Bytes anzuzeigen. Die `pad_length` Beispielwerte wurden bewusst ausgewählt. Sie zeigen, dass beim `fixed` Auffüllen die gleichen Werte wie `max` beim Auffüllen mit den empfohlenen `pad_length` Mindesteinstellungen erzielt werden oder wenn zusätzliche Polsterung gewünscht wird.

Beispiel für einen gemeinsamen geheimen Schlüssel: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Beispiel für eine Kollaborations-ID: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

Themen

Pad-Typ von **none**

Beispiel 1

Eingabe	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministisch	`Yes`
Eingabe-Bytes	0
Ausgabe-Bytes	0

Beispiel 2

Eingabe	`null`
`preserveNulls`	`FALSE`
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSPbNIJfG3iXmu6cbCUrizuV`
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	91

Beispiel 3

Eingabe	`empty string`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSPEM6qR8DWC2PB2GMlX41YK`
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	91

Beispiel 4

Eingabe	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-

Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9sGL5VLDQeHzh6DmPpyWNuI=`
Deterministisch	No
Eingabe-Bytes	26
Ausgabe-Bytes	127

Beispiel 5

Eingabe	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Deterministisch	No
Eingabe-Bytes	62
Ausgabe-Bytes	175

Pad-Typ von **`fixed`** (Beispiel 1)

In diesem Beispiel `pad_length` ist es 62 und die größte Eingabe ist 62 Byte.

Beispiel 1

Eingabe	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministisch	`Yes`
Eingabe-Bytes	0
Ausgabe-Bytes	0

Beispiel 2

Eingabe	`null`
`preserveNulls`	`FALSE`
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=`
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	175

Beispiel 3

Eingabe	`empty string`
`preserveNulls`	-

Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=`
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	175

Beispiel 4

Eingabe	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`
Deterministisch	No
Eingabe-Bytes	26
Ausgabe-Bytes	175

Beispiel 5

Eingabe	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqdP4/ QOQ3cXb/pbvPcnnohrHIGSX54ua+1/ JfcVjc=`
Deterministisch	No
Eingabe-Bytes	62
Ausgabe-Bytes	175

Pad-Typ von **`fixed`** (Beispiel 2)

In diesem Beispiel `pad_length` ist es 162 und die größte Eingabe ist 62 Byte.

Beispiel 1

Eingabe	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministisch	`Yes`
Eingabe-Bytes	0
Ausgabe-Bytes	0

Beispiel 2

Eingabe	`null`
`preserveNulls`	`FALSE`
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb`
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	307

Beispiel 3

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

	pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	307

Beispiel 4

Eingabe	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf
Deterministisch	No
Eingabe-Bytes	26
Ausgabe-Bytes	307

Beispiel 5

Eingabe	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/QOQ3cXb/pbvPcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i``
Deterministisch	No
Eingabe-Bytes	62
Ausgabe-Bytes	307

Pad-Typ von **`max`** (Beispiel 1)

In diesem Beispiel `pad_length` ist der Wert 0 und die größte Eingabe ist 62 Byte.

Beispiel 1

Eingabe	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministisch	`Yes`

Eingabe-Bytes	0
Ausgangs-Bytes	0

Beispiel 2

Eingabe	`null`
`preserveNulls`	`FALSE`
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=`
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	175

Beispiel 3

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

Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	175

Beispiel 4

Eingabe	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`
Deterministisch	No
Eingabe-Bytes	26
Ausgabe-Bytes	175

Beispiel 5

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

	`RFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Deterministisch	`No`
Eingabe-Bytes	62
Ausgabe-Bytes	175

Pad-Typ von **`max`** (Beispiel 2)

In diesem Beispiel `pad_length` ist es 100 und die größte Eingabe ist 62 Byte.

Beispiel 1

Eingabe	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministisch	`Yes`
Eingabe-Bytes	0
Ausgabe-Bytes	0

Beispiel 2

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

	`NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb`
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	307

Beispiel 3

Eingabe	`empty string`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT`
Deterministisch	No
Eingabe-Bytes	0
Ausgabe-Bytes	307

Beispiel 4

Eingabe	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcnkB0xbLWD7zNdAqQGR0rXoSESdW0I0vpNoGcBfv4cJbG0A3h1DvtkSSVc2B80OOGppzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn+8o4WtG/ClipNcjDXvXVtK4vfCohcCA6uwrmwtX5Hnl+WyfO6ks3QMaRDGSf`
Deterministisch	No
Eingabe-Bytes	26
Ausgabe-Bytes	307

Beispiel 5

Eingabe	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnkB0xbLWD7z`

	`NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i`
Deterministisch	No
Eingabe-Bytes	62
Ausgabe-Bytes	307

sealedSpalten zur Problembehandlung

Warum ist der Chiffretext in meinen sealed Spalten um ein Vielfaches größer als cleartext der Inhalt?

Das hängt von mehreren Faktoren ab. Zum einen ist der Chiffretext in einer Cleartext Spalte immer mindestens 91 Byte lang. Wenn Ihre Eingabedaten klein wären (z. B. das Alter der Kunden), würden sie deutlich an Größe zunehmen. Zweitens, wenn `preserveNulls` wir auf eingestellt sind `false` und Ihre Eingabedaten viele `null` Werte enthielten, wurde jeder dieser `null` Werte in 91 Byte Chiffretext umgewandelt. Und wenn Sie Padding verwenden, werden den cleartext Daten per Definition Byte hinzugefügt, bevor sie verschlüsselt werden.

Die meisten meiner Daten in einer sealed Spalte sind sehr klein, und ich muss Padding verwenden. Kann ich einfach die großen Werte entfernen und sie separat verarbeiten, um Platz zu sparen?

Wir empfehlen nicht, große Werte zu entfernen und separat zu verarbeiten. Dadurch ändern sich die Datenschutzgarantien, die der C3R-Verschlüsselungsclient bietet. Gehen Sie als Bedrohungsmodell davon aus, dass ein Beobachter beide verschlüsselten Datensätze sehen kann. Wenn der Beobachter feststellt, dass bei einer Teilmenge von Daten eine Spalte deutlich mehr oder weniger aufgefüllt ist als bei einer anderen Teilmenge, kann er Rückschlüsse auf die Größe der Daten in jeder Teilmenge ziehen. Nehmen wir beispielsweise an, dass eine `fullName` Spalte in einer Datei auf insgesamt 40 Byte aufgefüllt ist und in einer anderen Datei auf 800 Byte aufgefüllt wird. Ein Beobachter könnte davon ausgehen, dass ein Datensatz den längsten Namen der Welt (747 Byte) enthält.

Muss ich zusätzliche Polsterung bereitstellen, wenn ich den **`max`** Padding-Typ verwende?

Nein. Bei der Verwendung `max` von Innenabständen empfehlen wir`pad_length`, die auch als zusätzliche Polsterung bezeichnet wird, die über den größten Wert in der Spalte hinausgeht, auf 0 zu setzen.

Kann ich **`pad_length`** bei der Verwendung von **`fixed`** Padding einfach einen Wert vom Typ L wählen, damit ich mir keine Gedanken darüber machen muss, ob der größte Wert passt?

Ja, aber die große Länge des Pads ist ineffizient und beansprucht mehr Speicherplatz als nötig. Wir empfehlen Ihnen, zu überprüfen, wie groß der größte Wert ist, und den Wert `pad_length` auf diesen Wert einzustellen.

Woher weiß ich, ob ich die kryptografischen Garantien von benötige? **`preserveNulls`**

Leider lautet die Antwort, dass es darauf ankommt. Zumindest Kryptografisches Rechnen für Clean Rooms sollte überprüft werden, wie die `preserveNulls` Einstellung Ihre Daten schützt. Wir empfehlen Ihnen jedoch, die Datenverarbeitungsanforderungen Ihres Unternehmens und alle Verträge, die für die jeweilige Zusammenarbeit gelten, zu beachten.

Warum muss ich den Overhead von Base64 auf mich nehmen?

Um die Kompatibilität mit tabellarischen Dateiformaten wie CSV zu gewährleisten, ist eine Base64-Kodierung erforderlich. Obwohl einige Dateiformate, wie z. Parquet B., binäre Darstellungen von Daten unterstützen, ist es wichtig, dass alle Teilnehmer einer Zusammenarbeit Daten auf die gleiche Weise darstellen, um korrekte Abfrageergebnisse zu gewährleisten.

Behebung unerwarteter Zunahmen der Chiffretext-Größe

Nehmen wir an, Sie haben Ihre Daten verschlüsselt und die Größe der resultierenden Daten ist überraschend groß. Mithilfe der folgenden Schritte können Sie ermitteln, wo der Größenzuwachs stattgefunden hat und welche Maßnahmen Sie gegebenenfalls ergreifen können.

Identifizieren Sie, wo die Größenzunahme stattgefunden hat

Bevor Sie herausfinden können, warum Ihre verschlüsselten Daten deutlich größer sind als Ihre cleartext Daten, müssen Sie zunächst herausfinden, wo die Zunahme liegt. CleartextSpalten können bedenkenlos ignoriert werden, da sie unverändert sind. Sehen Sie sich die verbleibenden sealed Spalten fingerprint und die anderen an und wählen Sie eine aus, die aussagekräftig erscheint.

Identifizieren Sie den Grund für die Größenzunahme

Eine fingerprint Spalte oder eine sealed Spalte könnte zur Größenzunahme beitragen.

Themen

Kommt die Größenzunahme von einer fingerprint Spalte?

Wenn es sich bei der Spalte, die am meisten zur Speichererweiterung beiträgt, um eine fingerprint Spalte handelt, liegt das wahrscheinlich daran, dass die cleartext Daten klein sind (z. B. das Alter des Kunden). Jeder resultierende fingerprint Chiffretext hat eine Länge von 52 Byte. Leider kann gegen dieses Problem nichts auf der Grundlage unternommen werden. column-by-column Weitere Informationen zu dieser Spalte, einschließlich der Auswirkungen auf die Speicheranforderungen, finden Sie unter. Basis-Overhead für fingerprint Spalten

Die andere mögliche Ursache für die Vergrößerung einer fingerprint Spalte ist die Einstellung für die Zusammenarbeit,`preserveNulls`. Wenn die Einstellung für die Zusammenarbeit deaktiviert `preserveNulls` ist (die Standardeinstellung), werden aus allen `null` Werten in fingerprint Spalten 52 Byte Chiffretext. In der aktuellen Zusammenarbeit kann dafür nichts unternommen werden.
Die `preserveNulls` Einstellung wird bei der Erstellung einer Kollaboration festgelegt, und alle Mitarbeiter müssen dieselbe Einstellung verwenden, um korrekte Abfrageergebnisse sicherzustellen. Weitere Informationen zu dieser `preserveNulls` Einstellung und dazu, wie sich ihre Aktivierung auf die Datenschutzgarantien Ihrer Daten auswirkt, finden Sie unter. Kryptografisches Rechnen

Ist die Größenzunahme auf eine sealed Spalte zurückzuführen?

Wenn es sich bei der Spalte, die am meisten zur Erhöhung des Speicherplatzes beiträgt, um eine sealed Spalte handelt, gibt es einige Details, die zur Vergrößerung beitragen könnten.

Wenn die cleartext Daten klein sind (z. B. das Alter des Kunden), ist jeder resultierende sealed Chiffretext mindestens 91 Byte lang. Leider kann nichts gegen dieses Problem unternommen werden. Weitere Informationen zu dieser Spalte, einschließlich der Auswirkungen auf die Speicheranforderungen, finden Sie unter. Basis-Overhead für Spalten sealed

Die zweite Hauptursache für die Erhöhung des Speicherplatzes in sealed Spalten ist die Polsterung. Beim Auffüllen werden zusätzliche Byte hinzugefügt, cleartext bevor es verschlüsselt wird, um die Größe einzelner Werte in einem Datensatz zu verbergen. Wir empfehlen Ihnen, das Padding auf den kleinstmöglichen Wert für Ihren Datensatz festzulegen. `pad_length`Für das `fixed` Padding muss mindestens so eingestellt werden, dass es den größtmöglichen Wert in der Spalte umfasst. Eine höhere Einstellung als diese bietet keine zusätzlichen Datenschutzgarantien. Wenn Sie

beispielsweise wissen, dass der größtmögliche Wert in einer Spalte 50 Byte sein kann, empfehlen wir, den Wert `pad_length` auf 50 Byte festzulegen. Wenn in der sealed Spalte jedoch `max` Padding verwendet wird, empfehlen wir, den Wert `pad_length` auf 0 Byte zu setzen. Dies liegt daran, dass `max` sich das Auffüllen auf das zusätzliche Auffüllen bezieht, das über den größten Wert in der Spalte hinausgeht.

Die letzte mögliche Ursache für die Vergrößerung einer sealed Spalte ist die Einstellung für die Zusammenarbeit,. `preserveNulls` Wenn die Einstellung für die Zusammenarbeit deaktiviert `preserveNulls` ist (die Standardeinstellung), werden aus allen `null` Werten in sealed Spalten 91 Byte Chiffretext. In der aktuellen Zusammenarbeit kann dafür nichts unternommen werden. Die `preserveNulls` Einstellung wird bei der Erstellung einer Kollaboration festgelegt, und alle Mitarbeiter müssen dieselbe Einstellung verwenden, um korrekte Abfrageergebnisse sicherzustellen. Weitere Informationen zu dieser Einstellung und zu den Auswirkungen ihrer Aktivierung auf die Datenschutzgarantien Ihrer Daten finden Sie unter. Kryptografisches Rechnen

Anmeldung abfragen AWS Clean Rooms

Die Abfrageprotokollierung ist eine Funktion in AWS Clean Rooms. Wenn Sie eine Kollaboration erstellen und die Abfrageprotokollierung aktivieren, können Mitglieder für sie relevante Abfrageprotokolle in Amazon CloudWatch Logs speichern.

Mithilfe von Abfrageprotokollen können Mitglieder feststellen, ob die Abfragen den Analyseregeln entsprechen und ob sie mit der Kooperationsvereinbarung übereinstimmen. Darüber hinaus unterstützen Abfrageprotokolle Audits.

Wenn die Option Abfrageprotokollierung in der AWS Clean Rooms Konsole aktiviert ist, enthalten die Abfrageprotokolle Folgendes:

- `analysisRule`— Die Analyseregel für die konfigurierte Tabelle.
- `analysisTemplateArn`— Die Analysevorlage, die ausgeführt wurde (wird je nach Analyseregel angezeigt).
- `collaborationId`— Die eindeutige Kennung für die Zusammenarbeit, in der die Abfrage ausgeführt wurde.
- `configuredTableID`— Die eindeutige Kennung für die konfigurierte Tabelle, auf die in der Abfrage verwiesen wird.
- `directQueryAnalysisRulePolicy.custom.allowedAnalysis`— Die Analysevorlage, die für die konfigurierte Tabelle ausgeführt werden darf (wird je nach Analyseregel angezeigt).
- `directQueryAnalysisRulePolicy.v1.custom.allowedAnalysisProviders`— Die Abfrageanbieter, die eine Abfrage erstellen dürfen (wird je nach Analyseregel angezeigt).
- `eventID`— Die eindeutige Kennung für den Abfragelauf. Nach dem 31. August 2023 ist der eindeutige Bezeichner derselbe wie der`protectedQueryID`.
- `eventTimestamp`— Die Laufzeit der Abfrage.
- `parameters.parametervalue`— Die Parameterwerte (erscheint je nach Abfragetext).
- `queryText`— Die SQL-Definition von Query Run. Wenn es Parameter gibt, werden sie als `:parametervalue` gekennzeichnet.
- `queryValidationErrors`— Die Abfragefehler bei der Abfragevalidierung.
- `schemaName`— Der Name der konfigurierten Tabellenverknüpfung, auf die in der Abfrage verwiesen wird.

Empfangen von Abfrageprotokollen

Sie müssen keine Aktionen außerhalb der Einrichtung von AWS Clean Rooms Abfrageprotokollen ausführen. AWS Clean Rooms erstellt Protokollgruppen für Kollaborationen, nachdem jedes Kollaborationsmitglied eine Mitgliedschaft erstellt hat.

Mitglieder, die Abfragen durchführen können, Mitglieder, die Ergebnisse empfangen können, und Mitglieder, auf deren Konfigurationstabellen in der Abfrage verwiesen wird, erhalten ein Abfrageprotokoll.

Das Mitglied, das Abfragen durchführen kann, und das Mitglied, das Ergebnisse empfangen kann, erhalten Abfrageprotokolle für jede konfigurierte Tabelle, auf die in der Abfrage verwiesen wird. Wenn sie nicht Eigentümer der konfigurierten Tabelle sind, können sie die konfigurierte Tabellen-ID (`configuredTableID`) nicht einsehen.

Wenn ein Mitglied über mehrere konfigurierte Tabellenzuordnungen verfügt, auf die in der Abfrage verwiesen wird, erhält es für jede konfigurierte Tabelle ein Abfrageprotokoll.

Protokolle werden für Abfragen erstellt, die nicht unterstütztes und unterstütztes SQL in AWS Clean Rooms enthalten. Weitere Informationen finden Sie in der AWS Clean Rooms SQL-Referenz.

Protokolle werden auch erstellt, wenn Abfragen auf konfigurierte Tabellen verweisen, die nicht mit der Kollaboration verknüpft sind.

Für eine falsche SQL-Eingabe werden keine Protokolle erstellt AWS Clean Rooms.

Abfrageprotokolle geben nicht an, dass eine Abfrage erfolgreich war und die Abfrageausgabe zugestellt wurde. Sie bestätigen, dass eine Anfrage von dem Mitglied eingereicht wurde, das Abfragen durchführen kann. Abfrageprotokolle bestätigen auch, dass die Abfrage unterstütztes SQL enthält AWS Clean Rooms und auf konfigurierte Tabellen verweist, die der Kollaboration zugeordnet sind.

Example

Beispielsweise wird kein Protokoll erstellt, wenn die Abfrage abgebrochen wurde, nachdem AWS Clean Rooms überprüft wurde, ob sie den Analyseregeln entspricht, und während der Abfrageverarbeitung.

Wenn Sie die Protokollgruppe löschen, müssen Sie die Protokollgruppe manuell mit demselben Protokollgruppennamen (Kollaborations-ID der Kollaboration) neu erstellen. Oder Sie können die Protokollierung in Ihrer Mitgliedschaft ein- und ausschalten.

Weitere Informationen zum Aktivieren der Abfrageprotokollierung finden Sie unterAufbau einer Zusammenarbeit in AWS Clean Rooms.

Weitere Informationen zu Amazon CloudWatch Logs finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

Verwenden von Abfrageprotokollen

Wir empfehlen Mitgliedern, regelmäßig die folgenden Maßnahmen zu ergreifen:

- Um sicherzustellen, dass die Abfragen den Anwendungsfällen oder Abfragen entsprechen, die für die Zusammenarbeit vereinbart wurden, überprüfen Sie die Abfragen, die in der Kollaboration ausgeführt werden.

  Weitere Informationen zum Anzeigen der letzten Abfragen finden Sie unter Aktuelle Abfragen anzeigen.
- Überprüfen Sie die konfigurierten Tabellenspalten, die in den Analyseregeln der Kollaborationsmitglieder und in Abfragen verwendet werden, um sicherzustellen, dass die konfigurierten Tabellenspalten mit den für die Kollaboration vereinbarten Werten übereinstimmen.

  Weitere Informationen zum Anzeigen der konfigurierten Spalten finden Sie unter Tabellen und Analyseregeln anzeigen.

Einrichten AWS Clean Rooms

In den folgenden Themen wird die Einrichtung erläutert AWS Clean Rooms.

Themen

Melden Sie sich an für AWS

Bevor Sie eines davon AWS-Service nutzen können AWS Clean Rooms, müssen Sie sich für registrieren AWS.

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.
3. Wenn Sie sich für einen anmelden AWS-Konto, wird ein AWS-Konto Root-Benutzer erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

Richten Sie Servicerollen ein für AWS Clean Rooms

Themen

- Erstellen Sie eine Servicerolle, um Ergebnisse zu erhalten

Erstellen Sie einen Administratorbenutzer

Zur Verwendung AWS Clean Rooms müssen Sie einen Administratorbenutzer für sich selbst erstellen und den Administratorbenutzer zu einer Administratorgruppe hinzufügen.

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
Im IAM Identity Center (Empfohlen)	Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS. Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.	Beachtung der Anweisungen unter Erste Schritte im AWS IAM Identity Center - Benutzerhandbuch.	Konfigurieren Sie den programmatischen Zugriff, indem Sie AWS CLI die Konfiguration für die Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch vornehmen.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
In IAM (Nicht empfohlen)	Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS.	Beachtung der Anweisungen unter Erstellen Ihres ersten IAM-Administratorbenutzers und Ihrer ersten Benutzergruppe im IAM-Benutzerhandbuch.	Programmgesteuerten Zugriff unter Verwendung der Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im IAM-Benutzerhandbuch konfigurieren.

Erstellen Sie eine IAM-Rolle für ein Kollaborationsmitglied

Ein Mitglied ist ein AWS Kunde, der an einer Kollaboration teilnimmt.

Um eine IAM-Rolle für ein Kollaborationsmitglied zu erstellen

1. Folgen Sie dem Verfahren Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer im AWS Identity and Access Management Benutzerhandbuch.
2. Wählen Sie für den Schritt Richtlinie erstellen im Richtlinien-Editor die Registerkarte JSON aus und fügen Sie dann je nach den Fähigkeiten, die dem Kollaborationsmitglied gewährt wurden, Richtlinien hinzu.

   AWS Clean Rooms bietet die folgenden verwalteten Richtlinien auf der Grundlage gängiger Anwendungsfälle:

Wenn Sie …	Dann benutze...
Sehen Sie sich die Ressourcen und Metadaten an	AWS verwaltete Richtlinie: `AWSCleanRoomsReadOnlyAccess`
Abfrage	AWS verwaltete Richtlinie: `AWSCleanRoomsFullAccess`
Ergebnisse abfragen und empfangen	AWS verwaltete Richtlinie: `AWSCleanRoomsFullAccess`
Ressourcen für die Zusammenarbeit verwalten, aber keine Abfragen durchführen	AWS verwaltete Richtlinie: `AWSCleanRoomsFullAccessNoQuerying`

Informationen zu den verschiedenen verwalteten Richtlinien, die von angeboten werden AWS Clean Rooms, finden Sie unter AWS verwaltete Richtlinien für AWS Clean Rooms

Erstellen Sie eine Servicerolle zum Lesen von Daten

AWS Clean Rooms verwendet eine Servicerolle, um die Daten zu lesen.

Es gibt zwei Möglichkeiten, diese Servicerolle zu erstellen:

Wenn...	Dann
Sie verfügen über die erforderlichen IAM-Berechtigungen, um eine Servicerolle zu erstellen	Verwenden Sie die AWS Clean Rooms Konsole, um eine Servicerolle zu erstellen.
Sie haben keine `iam:CreateRole` , `iam:CreatePolicy` und `iam:AttachRolePolicy` Berechtigungen	Führen Sie eine der folgenden Aktionen aus:

Wenn...	Dann
or Sie möchten die IAM-Rollen manuell erstellen	• Gehen Sie wie folgt vor, um eine Servicerolle zu erstellen. • Bitten Sie Ihren Administrator, die Servicerolle mithilfe des folgenden Verfahrens zu erstellen.

Um eine Servicerolle zum Lesen von Daten zu erstellen

> **Note**
>
> Sie oder Ihr IAM-Administrator sollten dieses Verfahren nur befolgen, wenn Sie nicht über die erforderlichen Berechtigungen zum Erstellen einer Servicerolle mithilfe der AWS Clean Rooms Konsole verfügen.

1. Folgen Sie dem Verfahren zum Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien (Konsole) im AWS Identity and Access Management Benutzerhandbuch.
2. Verwenden Sie die folgende benutzerdefinierte Vertrauensrichtlinie gemäß dem Verfahren Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien (Konsole).

   > **Note**
   >
   > Wenn Sie sicherstellen möchten, dass die Rolle nur im Rahmen einer bestimmten Kollaborationsmitgliedschaft verwendet werden kann, können Sie die Vertrauensrichtlinie weiter einschränken. Weitere Informationen finden Sie unter Serviceübergreifende Confused-Deputy-Prävention.

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

```
                "Service": "cleanrooms.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

3. Verwenden Sie die folgende Berechtigungsrichtlinie gemäß dem Verfahren Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien (Konsole).

> **Note**
>
> Die folgende Beispielrichtlinie unterstützt die Berechtigungen, die zum Lesen von AWS Glue Metadaten und den entsprechenden Amazon S3 S3-Daten erforderlich sind. Je nachdem, wie Sie Ihre S3-Daten eingerichtet haben, müssen Sie diese Richtlinie jedoch möglicherweise ändern. Wenn Sie beispielsweise einen benutzerdefinierten KMS-Schlüssel für Ihre S3-Daten eingerichtet haben, müssen Sie diese Richtlinie möglicherweise mit zusätzlichen AWS KMS Berechtigungen ändern.
> Ihre AWS Glue Ressourcen und die zugrunde liegenden Amazon S3 S3-Ressourcen müssen sich in derselben Weise AWS-Region wie die AWS Clean Rooms Zusammenarbeit befinden.

```
{
    "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. Ersetzen Sie jeden *`Platzhalter`* durch Ihre eigenen Informationen.
5. Folgen Sie weiterhin dem Verfahren Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien (Konsole), um die Rolle zu erstellen.

Erstellen Sie eine Servicerolle, um Ergebnisse zu erhalten

> **Note**
>
> Wenn Sie das Mitglied sind, das nur Ergebnisse erhalten kann (in der Konsole ist Ihre Mitgliederfähigkeit nur Ergebnisse erhalten aktiviert), gehen Sie wie folgt vor.
> Wenn Sie ein Mitglied sind, das Ergebnisse sowohl abfragen als auch empfangen kann (in der Konsole ist Ihre Fähigkeit als Mitglied sowohl Ergebnisse abfragen als auch Ergebnisse erhalten), können Sie dieses Verfahren überspringen.

AWS Clean Rooms Verwendet für Kollaborationsmitglieder, die nur Ergebnisse erhalten können, eine Servicerolle, um Ergebnisse der abgefragten Daten in der Kollaboration in den angegebenen Amazon S3 S3-Bucket zu schreiben.

Es gibt zwei Möglichkeiten, diese Servicerolle zu erstellen:

Wenn...	Dann
Sie verfügen über die erforderlichen IAM-Berechtigungen, um eine Servicerolle zu erstellen	Verwenden Sie die AWS Clean Rooms Konsole, um eine Servicerolle zu erstellen.
Sie haben keine`iam:CreateRole` , `iam:CreatePolicy` und `iam:AttachRolePolicy` Berechtigungen	Führen Sie eine der folgenden Aktionen aus:

Wenn...	Dann
or Sie möchten die IAM-Rollen manuell erstellen	• Gehen Sie wie folgt vor, um eine Servicerolle zu erstellen. • Bitten Sie Ihren Administrator, die Servicerolle mithilfe des folgenden Verfahrens zu erstellen.

Um eine Servicerolle zu erstellen, um Ergebnisse zu erhalten

> **Note**
>
> Sie oder Ihr IAM-Administrator sollten dieses Verfahren nur befolgen, wenn Sie nicht über die erforderlichen Berechtigungen verfügen, um mithilfe der AWS Clean Rooms Konsole eine Servicerolle zu erstellen.

1. Folgen Sie dem Verfahren zum Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien (Konsole) im AWS Identity and Access Management Benutzerhandbuch.
2. Verwenden Sie die folgende benutzerdefinierte Vertrauensrichtlinie gemäß dem Verfahren Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien (Konsole).

```
{
    "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. Verwenden Sie die folgende Berechtigungsrichtlinie gemäß dem Verfahren Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien (Konsole).

> **Note**
>
> Die folgende Beispielrichtlinie unterstützt die Berechtigungen, die zum Lesen von AWS Glue Metadaten und den entsprechenden Amazon S3 S3-Daten erforderlich sind. Je nachdem, wie Sie Ihre S3-Daten eingerichtet haben, müssen Sie diese Richtlinie jedoch möglicherweise ändern.
> Ihre AWS Glue Ressourcen und die zugrunde liegenden Amazon S3 S3-Ressourcen müssen sich in derselben Weise AWS-Region wie die AWS Clean Rooms Zusammenarbeit befinden.

```
{
    "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. Ersetzen Sie jeden *Platzhalter* durch Ihre eigenen Informationen:

   - *Region* — Der Name der AWS-Region. z. B. **us-east-1**.
   - *a1B2C3D4-5678-90AB-CDEF-exampleAAAAA* — Die Mitglieds-ID des Mitglieds, das Abfragen durchführen kann. Die Mitglieds-ID finden Sie auf der Registerkarte Details der Kollaboration. Dadurch AWS Clean Rooms wird sichergestellt, dass die Rolle nur übernommen wird, wenn dieses Mitglied die Analyse in dieser Kollaboration ausführt.
   - *arn:aws:cleanrooms:us-east- 1:555555555555:membership/ a1b2c3d4-5678-90ab-cdef-exampleAAAAA* – Der einzige Mitgliedschafts-ARN des Mitglieds, das Abfragen durchführen kann. Den Mitglieds-ARN finden Sie auf der Registerkarte Details der Kollaboration. Dadurch AWS Clean Rooms wird sichergestellt, dass die Rolle nur übernommen wird, wenn dieses Mitglied die Analyse in dieser Kollaboration ausführt.

- *bucket_name* — Der Amazon-Ressourcenname (ARN) des S3-Buckets. Den Amazon-Ressourcennamen (ARN) finden Sie auf der Registerkarte Eigenschaften des Buckets in Amazon S3.
- *accountId* — Die AWS-Konto ID, in der sich der S3-Bucket befindet.

  bucket_name/optional_key_prefix — Der Amazon-Ressourcenname (ARN) des Ergebnisziels in S3. Den Amazon-Ressourcennamen (ARN) finden Sie auf der Registerkarte Eigenschaften des Buckets in Amazon S3.

5. Folgen Sie weiterhin dem Verfahren zum Erstellen einer Rolle mithilfe benutzerdefinierter Vertrauensrichtlinien (Konsole), um die Rolle zu erstellen.

Richten Sie Servicerollen für AWS Clean Rooms ML ein

Themen

- Erstellen Sie eine Servicerolle zum Lesen von Trainingsdaten
- Erstellen Sie eine Servicerolle, um ein Lookalike-Segment zu schreiben
- Erstellen Sie eine Servicerolle zum Lesen von Startdaten

Erstellen Sie eine Servicerolle zum Lesen von Trainingsdaten

AWS Clean Rooms verwendet eine Servicerolle, um Trainingsdaten zu lesen. Sie können diese Rolle mithilfe der Konsole erstellen, wenn Sie über die erforderlichen IAM-Berechtigungen verfügen. Wenn Sie keine `CreateRole` Berechtigungen haben, bitten Sie Ihren Administrator, die Servicerolle zu erstellen.

Um eine Servicerolle zum Trainieren eines Datensatzes zu erstellen

1. Melden Sie sich mit Ihrem Administratorkonto bei der IAM-Konsole (https://console.aws.amazon.com/iam/) an.
2. Wählen Sie unter Access management (Zugriffsverwaltung) Policies (Richtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie im Policy-Editor die Registerkarte JSON aus und kopieren Sie dann die folgende Richtlinie und fügen Sie sie ein.

> **Note**
>
> Die folgende Beispielrichtlinie unterstützt die Berechtigungen, die zum Lesen von AWS Glue Metadaten und den entsprechenden Amazon S3 S3-Daten erforderlich sind.
> Je nachdem, wie Sie Ihre S3-Daten eingerichtet haben, müssen Sie diese Richtlinie jedoch möglicherweise ändern. Diese Richtlinie beinhaltet keinen KMS-Schlüssel zum Entschlüsseln von Daten.
> Ihre AWS Glue Ressourcen und die zugrunde liegenden Amazon S3 S3-Ressourcen müssen sich in derselben Weise AWS-Region wie die AWS Clean Rooms Zusammenarbeit befinden.

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

Wenn Sie einen KMS-Schlüssel zum Entschlüsseln von Daten verwenden müssen, fügen Sie diese AWS KMS Anweisung zur vorherigen Vorlage hinzu:

```
{
```

```
            "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. Wählen Sie Weiter aus.
6. Geben Sie unter Überprüfen und erstellen einen Richtliniennamen und eine Beschreibung ein, und überprüfen Sie die Zusammenfassung.
7. Wählen Sie Richtlinie erstellen aus.

   Sie haben eine Richtlinie für erstellt AWS Clean Rooms.
8. Wählen Sie unter Access management (Zugriffsverwaltung) Roles (Rollen) aus.

   Mit Rollen können Sie kurzfristige Anmeldeinformationen erstellen, was aus Sicherheitsgründen empfohlen wird. Sie können auch Benutzer auswählen, um langfristige Anmeldeinformationen zu erstellen.
9. Wählen Sie Rolle erstellen aus.
10. Wählen Sie im Assistenten zum Erstellen von Rollen unter Vertrauenswürdiger Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus.
11. Kopieren Sie die folgende benutzerdefinierte Vertrauensrichtlinie und fügen Sie sie in den JSON-Editor ein.

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

Das `SourceAccount` ist immer dein AWS Konto. Das `SourceArn` kann auf einen bestimmten Trainingsdatensatz beschränkt werden, jedoch erst, nachdem dieser Datensatz erstellt wurde. Da Sie den ARN des Trainingsdatensatzes nicht vorab kennen können, wird der Platzhalter hier angegeben.

12. Wählen Sie Weiter und geben Sie unter Berechtigungen hinzufügen den Namen der Richtlinie ein, die Sie gerade erstellt haben. (Möglicherweise müssen Sie die Seite neu laden.)
13. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die Sie erstellt haben, und klicken Sie dann auf Weiter.
14. Geben Sie unter Name, review and create den Rollennamen und die Beschreibung ein.

> **Note**
>
> Der Rollenname muss dem Muster in den `passRole` Berechtigungen entsprechen, die dem Mitglied erteilt wurden, das Ergebnisse abfragen und empfangen kann, und den Mitgliedsrollen.

a. Überprüfen Sie die Option Vertrauenswürdige Entitäten auswählen und bearbeiten Sie sie gegebenenfalls.
b. Überprüfen Sie die Berechtigungen unter Berechtigungen hinzufügen und bearbeiten Sie sie gegebenenfalls.

c. Überprüfen Sie die Tags und fügen Sie bei Bedarf Stichwörter hinzu.

d. Wählen Sie Rolle erstellen aus.

15. Die Servicerolle für AWS Clean Rooms wurde erstellt.

Erstellen Sie eine Servicerolle, um ein Lookalike-Segment zu schreiben

AWS Clean Rooms verwendet eine Servicerolle, um Lookalike-Segmente in einen Bucket zu schreiben. Sie können diese Rolle mithilfe der Konsole erstellen, wenn Sie über die erforderlichen IAM-Berechtigungen verfügen. Wenn Sie keine `CreateRole` Berechtigungen haben, bitten Sie Ihren Administrator, die Servicerolle zu erstellen.

Um eine Servicerolle zu erstellen, um ein Lookalike-Segment zu schreiben

1. Melden Sie sich mit Ihrem Administratorkonto bei der IAM-Konsole (https://console.aws.amazon.com/iam/) an.
2. Wählen Sie unter Access management (Zugriffsverwaltung) Policies (Richtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie im Policy-Editor die Registerkarte JSON aus und kopieren Sie dann die folgende Richtlinie und fügen Sie sie ein.

> **Note**
>
> Die folgende Beispielrichtlinie unterstützt die Berechtigungen, die zum Lesen von AWS Glue Metadaten und den entsprechenden Amazon S3 S3-Daten erforderlich sind.
> Je nachdem, wie Sie Ihre S3-Daten eingerichtet haben, müssen Sie diese Richtlinie jedoch möglicherweise ändern. Diese Richtlinie beinhaltet keinen KMS-Schlüssel zum Entschlüsseln von Daten.
> Ihre AWS Glue Ressourcen und die zugrunde liegenden Amazon S3 S3-Ressourcen müssen sich in derselben Weise AWS-Region wie die AWS Clean Rooms Zusammenarbeit befinden.

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

Wenn Sie einen KMS-Schlüssel zum Verschlüsseln von Daten verwenden müssen, fügen Sie der Vorlage diese AWS KMS Anweisung hinzu:

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

Wenn Sie einen KMS-Schlüssel zum Entschlüsseln von Daten verwenden müssen, fügen Sie der Vorlage diese AWS KMS Anweisung hinzu:

```
{
            "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. Wählen Sie Weiter aus.
6. Geben Sie unter Überprüfen und erstellen einen Richtliniennamen und eine Beschreibung ein, und überprüfen Sie die Zusammenfassung.
7. Wählen Sie Richtlinie erstellen aus.

Sie haben eine Richtlinie für erstellt AWS Clean Rooms.

8. Wählen Sie unter Access management (Zugriffsverwaltung) Roles (Rollen) aus.

   Mit Rollen können Sie kurzfristige Anmeldeinformationen erstellen, was aus Sicherheitsgründen empfohlen wird. Sie können auch Benutzer auswählen, um langfristige Anmeldeinformationen zu erstellen.

9. Wählen Sie Rolle erstellen aus.

10. Wählen Sie im Assistenten zum Erstellen von Rollen unter Vertrauenswürdiger Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus.

11. Kopieren Sie die folgende benutzerdefinierte Vertrauensrichtlinie und fügen Sie sie in den JSON-Editor ein.

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

   Das `SourceAccount` ist immer dein AWS Konto. Das `SourceArn` kann auf einen bestimmten Trainingsdatensatz beschränkt werden, jedoch erst, nachdem dieser Datensatz erstellt wurde.

Da Sie den ARN des Trainingsdatensatzes nicht vorab kennen können, wird der Platzhalter hier angegeben.

12. Wählen Sie Weiter aus.
13. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die Sie erstellt haben, und wählen Sie dann Weiter aus.
14. Geben Sie unter Name, review and create den Rollennamen und die Beschreibung ein.

> **Note**
>
> Der Rollenname muss dem Muster in den `passRole` Berechtigungen entsprechen, die dem Mitglied erteilt wurden, das Ergebnisse abfragen und empfangen kann, und den Mitgliedsrollen.

    a. Überprüfen Sie die Option Vertrauenswürdige Entitäten auswählen und bearbeiten Sie sie gegebenenfalls.
    b. Überprüfen Sie die Berechtigungen unter Berechtigungen hinzufügen und bearbeiten Sie sie gegebenenfalls.
    c. Überprüfen Sie die Tags und fügen Sie bei Bedarf Stichwörter hinzu.
    d. Wählen Sie Rolle erstellen aus.
15. Die Servicerolle für AWS Clean Rooms wurde erstellt.

Erstellen Sie eine Servicerolle zum Lesen von Startdaten

AWS Clean Rooms verwendet eine Servicerolle, um Seed-Daten zu lesen. Sie können diese Rolle mithilfe der Konsole erstellen, wenn Sie über die erforderlichen IAM-Berechtigungen verfügen. Wenn Sie keine `CreateRole` Berechtigungen haben, bitten Sie Ihren Administrator, die Servicerolle zu erstellen.

Um eine Servicerolle zum Lesen von Startdaten zu erstellen

1. Melden Sie sich mit Ihrem Administratorkonto bei der IAM-Konsole (https://console.aws.amazon.com/iam/) an.
2. Wählen Sie unter Access management (Zugriffsverwaltung) Policies (Richtlinien) aus.
3. Wählen Sie Richtlinie erstellen aus.

4. Wählen Sie im Policy-Editor die Registerkarte JSON aus und kopieren Sie dann die folgende Richtlinie und fügen Sie sie ein.

> **Note**
>
> Die folgende Beispielrichtlinie unterstützt die Berechtigungen, die zum Lesen von AWS Glue Metadaten und den entsprechenden Amazon S3 S3-Daten erforderlich sind.
> Je nachdem, wie Sie Ihre S3-Daten eingerichtet haben, müssen Sie diese Richtlinie jedoch möglicherweise ändern. Diese Richtlinie beinhaltet keinen KMS-Schlüssel zum Entschlüsseln von Daten.
> Ihre AWS Glue Ressourcen und die zugrunde liegenden Amazon S3 S3-Ressourcen müssen sich in derselben Weise AWS-Region wie die AWS Clean Rooms Zusammenarbeit befinden.

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

Wenn Sie einen KMS-Schlüssel zum Entschlüsseln von Daten verwenden müssen, fügen Sie der Vorlage diese AWS KMS Anweisung hinzu:

```
{
            "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. Wählen Sie Weiter aus.
6. Geben Sie unter Überprüfen und erstellen einen Richtliniennamen und eine Beschreibung ein, und überprüfen Sie die Zusammenfassung.
7. Wählen Sie Richtlinie erstellen aus.

   Sie haben eine Richtlinie für erstellt AWS Clean Rooms.
8. Wählen Sie unter Access management (Zugriffsverwaltung) Roles (Rollen) aus.

Mit Rollen können Sie kurzfristige Anmeldeinformationen erstellen, was aus Sicherheitsgründen empfohlen wird. Sie können auch Benutzer auswählen, um langfristige Anmeldeinformationen zu erstellen.

9. Wählen Sie Rolle erstellen aus.
10. Wählen Sie im Assistenten zum Erstellen von Rollen unter Vertrauenswürdiger Entitätstyp die Option Benutzerdefinierte Vertrauensrichtlinie aus.
11. Kopieren Sie die folgende benutzerdefinierte Vertrauensrichtlinie und fügen Sie sie in den JSON-Editor ein.

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

Das `SourceAccount` ist immer dein AWS Konto. Das `SourceArn` kann auf einen bestimmten Trainingsdatensatz beschränkt werden, jedoch erst, nachdem dieser Datensatz erstellt wurde. Da Sie den ARN des Trainingsdatensatzes nicht vorab kennen können, wird der Platzhalter hier angegeben.

12. Wählen Sie Weiter aus.

13. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die Sie erstellt haben, und wählen Sie dann Weiter aus.
14. Geben Sie unter Name, review and create den Rollennamen und die Beschreibung ein.

    > **Note**
    >
    > Der Rollenname muss dem Muster in den `passRole` Berechtigungen entsprechen, die dem Mitglied erteilt wurden, das Ergebnisse abfragen und empfangen kann, und den Mitgliedsrollen.

    a. Überprüfen Sie die Option Vertrauenswürdige Entitäten auswählen und bearbeiten Sie sie gegebenenfalls.
    b. Überprüfen Sie die Berechtigungen unter Berechtigungen hinzufügen und bearbeiten Sie sie gegebenenfalls.
    c. Überprüfen Sie die Tags und fügen Sie bei Bedarf Stichwörter hinzu.
    d. Wählen Sie Rolle erstellen aus.
15. Die Servicerolle für AWS Clean Rooms wurde erstellt.

Aufbau einer Zusammenarbeit in AWS Clean Rooms

Eine Kollaboration ist eine sichere logische Grenze, AWS Clean Rooms innerhalb derer Mitglieder SQL-Abfragen an konfigurierten Tabellen ausführen können.

Jedes Mitglied AWS Clean Rooms kann eine Kollaboration erstellen.

Der Ersteller der Kollaboration kann ein einzelnes Mitglied bestimmen, das Ergebnisse abfragt und empfängt. Der Ersteller der Kollaboration möchte jedoch möglicherweise verhindern, dass das Mitglied, das Abfragen durchführen kann, Zugriff auf die Abfrageergebnisse hat. In diesem Fall kann der Ersteller der Kollaboration ein Mitglied bestimmen, das Abfragen durchführen kann, und ein anderes Mitglied, das Ergebnisse erhalten kann.

In den meisten Fällen ist das Mitglied, das Abfragen durchführen kann, auch das Mitglied, das die Rechenkosten für Abfragen bezahlt. Der Ersteller der Kollaboration kann jedoch ein anderes Mitglied so konfigurieren, dass es für die Bezahlung der Abfrageberechnungskosten verantwortlich ist.

Informationen zum Erstellen einer Kollaboration mithilfe der AWS SDKs finden Sie in der AWS Clean RoomsAPI-Referenz.

Themen

Erstellen Sie eine Kollaboration

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllt haben:

- Sie haben den Namen und die AWS-Konto ID für jedes Mitglied, das Sie zur Kollaboration einladen möchten.
- Sie sind berechtigt, den Namen und die AWS-Konto ID jedes Mitglieds mit allen Mitgliedern der Kollaboration zu teilen.

> **Note**
>
> Sie können keine weiteren Mitglieder hinzufügen, nachdem die Kollaboration erstellt wurde.

Um eine Kollaboration mit der AWS Clean Rooms Konsole zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit derAWS-Konto, die als Ersteller der Kollaboration fungiert.
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie in der oberen rechten Ecke die Option Kollaboration erstellen aus.
4. Gehen Sie für Schritt 1: Zusammenarbeit definieren wie folgt vor:

   a. Geben Sie für Details den Namen und die Beschreibung der Zusammenarbeit ein.

      Diese Informationen sind für Mitglieder der Kollaboration sichtbar, die zur Teilnahme an der Kollaboration eingeladen wurden. Der Name und die Beschreibung helfen ihnen zu verstehen, worauf sich die Zusammenarbeit bezieht.

   b. Für Mitglieder:

      i. Für Mitglied 1: Sie geben den Anzeigenamen Ihres Mitglieds so ein, wie er für die Kollaboration angezeigt werden soll.

      > **Note**
      >
      > Ihre AWS-Konto ID ist automatisch in der AWS-KontoMitglieds-ID enthalten.

      ii. Geben Sie für Mitglied 2 den Anzeigenamen und die AWS-KontoMitglieds-ID des Mitglieds ein, das Sie zur Kollaboration einladen möchten.

      Der Anzeigename und die AWS-KontoMitglieds-ID des Mitglieds sind für alle zu der Kollaboration eingeladenen Personen sichtbar. Nachdem Sie die Werte für diese Felder eingegeben und gespeichert haben, können sie nicht bearbeitet werden.

      > **Note**
      >
      > Sie müssen das Mitglied der Kollaboration darüber informieren, dass seine AWS-KontoMitglieds-ID und sein Anzeigename für alle eingeladenen und aktiven Mitarbeiter in der Kollaboration sichtbar sind.

      iii. Wenn Sie ein weiteres Mitglied hinzufügen möchten, wählen Sie Weiteres Mitglied hinzufügen. Geben Sie dann den Anzeigenamen und die AWS-KontoMitglieds-ID

für jedes Mitglied ein, das Daten beitragen kann, die Sie zur Kollaboration einladen möchten.

c. Wählen Sie für die Fähigkeiten von Mitgliedern eine der folgenden Optionen aus:

Wenn Sie …	Dann...
Fragen Sie die Daten in der Zusammenarbeit ab und erhalten Sie die Ergebnisse	1. Wählen Sie sich selbst als das Mitglied aus, das Abfragen ausführen kann. 2. Lassen Sie die Standardeinstellung für das Mitglied, das Ergebnisse empfangen kann, dieselbe Einstellung wie das Mitglied, das Abfragen ausführt, unverändert.
Fragen Sie die Daten in der Kollaboration ab und weisen Sie ein anderes Mitglied dem Empfang von Ergebnissen zu	1. Wählen Sie sich selbst als das Mitglied aus, das Abfragen ausführen kann. 2. Wählen Sie aus der Drop-down-Liste das Mitglied aus, das Ergebnisse erhalten kann.
Empfangen Sie die Ergebnisse der Abfrage in der Kollaboration und weisen Sie ein anderes Mitglied mit der Abfrage der Daten zu	1. Wählen Sie aus der Dropdownliste das Mitglied aus, das Abfragen ausführen kann. 2. Wählen Sie sich selbst als Mitglied aus, das Ergebnisse aus der Drop-down-Liste erhalten kann.
Erstellen und verwalten Sie die Kollaboration, weisen Sie einem anderen Mitglied die Abfrage der Daten zu und weisen Sie ein anderes Mitglied dem Empfang von Ergebnissen zu	1. Wählen Sie aus der Dropdownliste das Mitglied aus, das Abfragen ausführen kann. 2. Wählen Sie aus der Drop-down-Liste das Mitglied aus, das Ergebnisse erhalten kann.

d. Wählen Sie für die Zahlungskonfiguration eine der folgenden Optionen aus:

Wenn Sie …	Dann...
Weisen Sie dem Mitglied, das Abfragen ausführen kann, das Mitglied zu sein, das die Kosten für die Berechnung der Abfrage bezahlt	Behalten Sie die Standardeinstellung für das Mitglied, das für Abfragen bezahlt, dieselbe Einstellung wie das Mitglied, das Abfragen ausführt, bei.
Weisen Sie einem anderen Mitglied die Kosten für die Berechnung der Abfrage zu	Wählen Sie aus der Drop-down-Liste das Mitglied aus, das für Abfragen bezahlt.

e. Wenn Sie die Abfrageprotokollierung aktivieren möchten, aktivieren Sie das Kontrollkästchen Abfrageprotokollierung für diese Zusammenarbeit Support.

f. Wenn Sie die kryptografische Rechenfunktion aktivieren möchten, aktivieren Sie das Kontrollkästchen Kryptografisches Rechnen in dieser Zusammenarbeit Support und wählen Sie die folgenden kryptografischen Berechnungsparameter aus:

- Spalten zulassen cleartext

  Wählen Sie Nein, wenn Sie nicht möchten, dass cleartext Spalten in der verschlüsselten Tabelle zulässig sind.

  Wählen Sie Ja, wenn Sie möchten, dass cleartext Spalten in der verschlüsselten Tabelle zulässig sind.

  Damit SUM oder AVG für bestimmte Spalten ausgeführt werden kann, müssen sich die Spalten in befindencleartext.

- Duplikate zulassen

  Wählen Sie Nein, wenn Sie nicht möchten, dass doppelte Einträge in einer fingerprint Spalte zulässig sind.

  Wählen Sie Ja, wenn doppelte Einträge in einer fingerprint Spalte zulässig sein sollen.

- Zulassen JOIN von Spalten mit unterschiedlichen Namen

  Wählen Sie Nein, wenn Sie fingerprint Spalten mit unterschiedlichen Namen nicht verbinden möchten.

Wählen Sie Ja, wenn Sie fingerprint Spalten mit unterschiedlichen Namen verbinden möchten.

- NULLWerte beibehalten

  Wählen Sie Nein, wenn Sie NULL Werte nicht beibehalten möchten. NULLWerte werden nicht wie NULL in einer verschlüsselten Tabelle angezeigt.

  Wählen Sie Ja, wenn Sie NULL Werte beibehalten möchten. NULLWerte werden wie NULL in einer verschlüsselten Tabelle angezeigt.

Weitere Hinweise zu kryptografischen Rechenparametern finden Sie unterKryptografische Rechenparameter.

Weitere Hinweise zur Verschlüsselung Ihrer Daten für die Verwendung in finden Sie AWS Clean Rooms unter. Vorbereiten verschlüsselter Datentabellen mit Cryptographic Computing für Clean Rooms

> **Note**
>
> Überprüfen Sie diese Konfigurationen sorgfältig, bevor Sie den nächsten Schritt ausführen. Nachdem Sie die Kollaboration erstellt haben, können Sie nur den Namen und die Beschreibung der Kollaboration bearbeiten und angeben, ob die Abfrage-Logs in Amazon CloudWatch Logs gespeichert sind.

g. Wenn Sie Tags für die Kollaborationsressource aktivieren möchten, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

h. Wählen Sie Weiter.

5. Gehen Sie für Schritt 2: Mitgliedschaft konfigurieren wie folgt vor:

   a. Wählen Sie eine Option aus:

Wenn Sie folgendes auswählen …	Dann...
Ja, treten Sie bei, indem Sie jetzt eine Mitgliedschaft erstellen	Sowohl die Zusammenarbeit als auch Ihre Mitgliedschaft werden erstellt. Ihr Status in der Kollaboration ist aktiv.

Wenn Sie folgendes auswählen …	Dann...
Nein, ich werde später eine Mitgliedschaft erstellen	Nur die Kollaboration wird erstellt. Ihr Status in der Kollaboration ist inaktiv.

b. Wenn Sie das Mitglied sind, das Ergebnisse empfangen kann, wählen Sie unter Standardeinstellungen für Abfrageergebnisse eine Option aus:

Wenn du...	Dann...
Lassen Sie das Kontrollkästchen Jetzt Standardeinstellungen festlegen aktiviert. (Es ist standardmäßig ausgewählt.)	1. Geben Sie für das Ergebnisziel in Amazon S3 das Amazon S3 S3-Ziel ein. 2. Wählen Sie für das Abfrageergebnisformat entweder CSV oder PARQUET.
Deaktivieren Sie das Kontrollkästchen Jetzt Standardeinstellungen festlegen	Nur die Kollaboration wird erstellt. Ihr Status in der Kollaboration ist inaktiv.

c. Wenn Sie sich in Schritt 4.e dafür entschieden haben, die Abfrageprotokollierung zu aktivieren, wählen Sie eine der folgenden Optionen für die Protokollspeicherung in Amazon CloudWatch Logs:

Wenn Sie folgendes auswählen …	Dann...
Einschalten	Die für Sie relevanten Abfrageprotokolle werden in Amazon CloudWatch Logs gespeichert. Jedes Mitglied kann nur Protokolle für Anfragen erhalten, die es initiiert hat oder die seine Daten enthalten. Das Mitglied, das Ergebnisse erhalten kann, erhält auch Protokolle für alle Abfragen, die in einer Kollaboration ausgeführt werden, auch wenn in einer Abfrage nicht auf seine Daten zugegriffen wird.
Ausschalten	Die für Sie relevanten Abfrageprotokolle werden nicht in Ihrem Amazon CloudWatch Logs-Konto gespeichert.

> **Note**
>
> Nachdem Sie die Abfrageprotokollierung aktiviert haben, kann es einige Minuten dauern, bis der Protokollspeicher eingerichtet ist und Protokolle in Amazon CloudWatch Logs empfangen werden. Während dieser kurzen Zeit führt das Mitglied, das Abfragen durchführen kann, möglicherweise Abfragen durch, ohne dass tatsächlich Protokolle gesendet werden.

d. Wenn Sie Tags für die Mitgliedschaftsressource aktivieren möchten, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

e. Wenn Sie das Mitglied sind, das für Anfragen bezahlt, geben Sie Ihre Zustimmung an, indem Sie das Kontrollkästchen Ich stimme zu, für die Kosten der Query-Berechnung in dieser Zusammenarbeit zu zahlen, aktivieren.

> **Note**
>
> Sie müssen dieses Kontrollkästchen aktivieren, um fortzufahren.
> Weitere Informationen zur Preisberechnung finden Sie unterPreisgestaltung für AWS Clean Rooms.

Wenn Sie das Mitglied sind, das die Kosten für die Berechnung von Abfragen bezahlt, aber nicht das Mitglied, das Abfragen durchführen kann, empfiehlt es sich, ein Budget AWS Budgets zu konfigurieren AWS Clean Rooms und Benachrichtigungen zu erhalten, sobald das maximale Budget erreicht ist. Weitere Informationen zur Einrichtung eines Budgets finden Sie AWS Budgets im AWS Cost ManagementBenutzerhandbuch unter Ihre Kosten verwalten mit. Weitere Informationen zum Einrichten von Benachrichtigungen finden Sie unter Erstellen eines Amazon SNS SNS-Themas für Budgetbenachrichtigungen im AWS Cost ManagementBenutzerhandbuch. Wenn das maximale Budget erreicht wurde, können Sie sich an das Mitglied wenden, das Anfragen stellen oder die Kollaboration verlassen kann. Wenn Sie die Kollaboration verlassen, dürfen keine Abfragen mehr ausgeführt werden, sodass Ihnen auch keine Kosten für die Berechnung von Abfragen mehr in Rechnung gestellt werden.

f. Wählen Sie Weiter.

6. Gehen Sie für Schritt 3: Überprüfen und erstellen wie folgt vor:

   a. Überprüfen Sie die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, und bearbeiten Sie sie gegebenenfalls.

   b. Wählen Sie eine der folgenden Optionen aus:

Wenn Sie sich dafür entschieden haben...	Dann wähle...
Erstellen Sie eine Mitgliedschaft mit der Kollaboration (Ja, treten Sie bei, indem Sie jetzt eine Mitgliedschaft erstellen)	Erstellen Sie eine Zusammenarbeit und Mitgliedschaft
Erstellen Sie die Kollaboration und legen Sie zu diesem Zeitpunkt noch keine	Kollaboration erstellen

Wenn Sie sich dafür entschieden haben...	Dann wähle...
Mitgliedschaft an (Nein, ich werde später eine Mitgliedschaft erstellen)	

Nachdem Ihre Kollaboration erfolgreich erstellt wurde, können Sie die Seite mit den Kollaborationsdetails unter Kollaborationen einsehen.

Nächste Schritte

Sie sind jetzt bereit für:

- Bereiten Sie Ihre Datentabelle für die Abfrage vor. AWS Clean Rooms (Optional, wenn Sie Ihre eigenen Daten abfragen möchten.)
- Ordnen Sie die konfigurierte Tabelle Ihrer Kollaboration zu. (Optional, wenn Sie Ihre eigenen Daten abfragen möchten.)
- Konfigurieren Sie eine Analyseregel für die konfigurierte Tabelle. (Optional, wenn Sie Ihre eigenen Daten abfragen möchten.)
- Erstellen Sie eine Mitgliedschaft und treten Sie einer Kollaboration bei.
- Verwalte deine Zusammenarbeit.

Eine Mitgliedschaft erstellen und einer Kollaboration beitreten

Eine Mitgliedschaft ist eine Ressource, die erstellt wird, wenn ein Mitglied einer Kollaboration in beitritt AWS Clean Rooms.

Sie können einer Kollaboration als Mitglied beitreten, das Daten abfragen kann, als Mitglied, das Ergebnisse einer Abfrage empfangen kann, oder als Mitglied, das Ergebnisse einer Abfrage empfangen kann, oder als beides. Sie können einer Kollaboration auch als Mitglied beitreten, das die Kosten für die Berechnung von Abfragen bezahlt. Alle Mitglieder können Daten beisteuern.

Informationen dazu, wie Sie mithilfe der AWS SDKs eine Mitgliedschaft erstellen und einer Kollaboration beitreten können, finden Sie in der AWS Clean Rooms API-Referenz.

Themen

Erstellen Sie eine Mitgliedschaft und treten Sie einer Kollaboration bei

Um eine Mitgliedschaft zu erstellen und einer Kollaboration beizutreten

1. Melden Sie sich bei Ihrem Mitglied an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole AWS-Konto.
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie auf der Registerkarte „Zum Beitritt verfügbar“ für Kollaborationen, die zum Beitritt verfügbar sind, den Namen der Kollaboration aus.
4. Sehen Sie sich auf der Seite mit den Kollaborationsdetails die Kollaborationsdetails an, einschließlich Ihrer Mitgliedsdetails und einer Liste der anderen Mitglieder.

   Vergewissern Sie sich, dass es sich bei den AWS-Konto IDs für jedes Mitglied der Kollaboration um die IDs handelt, mit denen Sie an der Kollaboration teilnehmen möchten.
5. Wählen Sie Mitgliedschaft erstellen aus.

6. Sehen Sie sich auf der Seite Mitgliedschaft erstellen in der Übersicht den Namen der Kollaboration, die Beschreibung der Kollaboration, die AWS-Konto ID des Erstellers der Kollaboration, Ihre Fähigkeiten als Mitglied und die AWS-Konto ID des Mitglieds an, das für Anfragen bezahlt.
7. Wenn der Ersteller der Kollaboration die Abfrageprotokollierung aktiviert hat, wählen Sie eine der folgenden Optionen für die Protokollspeicherung in Amazon CloudWatch Logs:

Wenn Sie folgendes auswählen …	Dann...
Einschalten	Die für Sie relevanten Abfrageprotokolle werden in Amazon CloudWatch Logs gespeichert. Jedes Mitglied kann nur Protokolle für Anfragen erhalten, die es initiiert hat oder die seine Daten enthalten. Das Mitglied, das Ergebnisse erhalten kann, erhält auch Protokolle für alle Abfragen, die in einer Kollaboration ausgeführt werden, auch wenn in einer Abfrage nicht auf seine Daten zugegriffen wird.
Ausschalten	Die für Sie relevanten Abfrageprotokolle werden nicht in Ihrem Amazon CloudWatch Logs-Konto gespeichert.

> **Note**
>
> Nachdem Sie die Abfrageprotokollierung aktiviert haben, kann es einige Minuten dauern, bis der Protokollspeicher eingerichtet ist und Protokolle in Amazon CloudWatch Logs empfangen werden. Während dieser kurzen Zeit führt das Mitglied, das Abfragen durchführen kann, möglicherweise Abfragen durch, ohne dass tatsächlich Protokolle gesendet werden.

8. Wenn zu Ihren Fähigkeiten als Mitglied das Empfangen von Ergebnissen gehört:

a. Für die Einstellungen „Ergebnisse abfragen“

   i. Geben Sie das Ergebnisziel in Amazon S3 an, indem Sie das S3-Ziel eingeben, oder wählen Sie Browse S3, um aus einer Liste verfügbarer S3-Buckets auszuwählen.

      Example

      Beispiel: **`s3://bucket/prefix`**

   ii. Wählen Sie das Ergebnisformat (entweder CSV oder PARQUET).

b. Wählen Sie für den Dienstzugriff entweder eine neue Servicerolle erstellen und verwenden oder Eine vorhandene Servicerolle verwenden.

> **Note**
>
> Sie müssen entweder eine vorhandene Servicerolle auswählen oder über die erforderlichen Berechtigungen verfügen, um eine neue zu erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Servicerolle, um Ergebnisse zu erhalten.

9. Wenn Sie Tags für die Mitgliedschaftsressource aktivieren möchten, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.
10. Wenn der Ersteller der Kollaboration Sie als das Mitglied benannt hat, das für Anfragen bezahlt, geben Sie Ihre Zustimmung an, indem Sie das Kontrollkästchen Ich stimme zu, für die Berechnung der Abfragekosten in dieser Zusammenarbeit zu zahlen, aktivieren.

> **Note**
>
> Sie müssen dieses Kontrollkästchen aktivieren, um fortzufahren.
> Weitere Informationen zur Preisberechnung finden Sie unterPreisgestaltung für AWS Clean Rooms.

Wenn Sie das Mitglied sind, das die Kosten für die Berechnung von Abfragen bezahlt, aber nicht das Mitglied, das Abfragen durchführen kann, empfiehlt es sich, ein Budget AWS Budgets zu konfigurieren AWS Clean Rooms und Benachrichtigungen zu erhalten, sobald das maximale Budget erreicht ist. Weitere Informationen zur Einrichtung eines Budgets finden Sie AWS Budgets im AWS Cost Management Benutzerhandbuch unter Ihre Kosten verwalten mit.

Weitere Informationen zum Einrichten von Benachrichtigungen finden Sie unter Erstellen eines Amazon SNS SNS-Themas für Budgetbenachrichtigungen im AWS Cost Management Benutzerhandbuch. Wenn das maximale Budget erreicht wurde, können Sie sich an das Mitglied wenden, das Anfragen stellen oder die Kollaboration verlassen kann. Wenn Sie die Kollaboration verlassen, dürfen keine Abfragen mehr ausgeführt werden, sodass Ihnen auch keine Kosten für die Berechnung von Abfragen mehr in Rechnung gestellt werden.

11. Wenn Sie sicher sind, dass Sie eine Mitgliedschaft erstellen und der Kollaboration beitreten möchten, wählen Sie Mitgliedschaft erstellen aus.

Sie haben Lesezugriff auf die Metadaten der Kollaboration. Dazu gehören Informationen wie der Anzeigename und die Beschreibung der Kollaboration sowie alle Namen und AWS-Konto IDs anderer Mitglieder.

Informationen darüber, wie Sie eine Kollaboration verlassen können, finden Sie unterVerlassen einer Kollaboration.

Nächste Schritte

Sie sind jetzt bereit für:

- Bereiten Sie Ihre Datentabelle für die Abfrage vor. AWS Clean Rooms (Optional, wenn Sie Ihre eigenen Daten abfragen möchten.)
- Ordnen Sie die konfigurierte Tabelle Ihrer Kollaboration zu.
- Konfigurieren Sie eine Analyseregel für die konfigurierte Tabelle.

Vorbereiten von Datentabellen für Abfragen in AWS Clean Rooms

> **Note**
>
> Die Vorbereitung von Datentabellen kann vor oder nach dem Beitritt zu einer Kollaboration erfolgen. Nachdem eine Tabelle vorbereitet wurde, können Sie sie in mehreren Kollaborationen wiederverwenden, sofern Ihre Datenschutzanforderungen für diese Tabelle dieselben sind.

Als Mitglied der Kollaboration müssen Sie Ihre Datentabellen vorbereiten, bevor sie AWS Clean Rooms von dem Mitglied der Kollaboration, das Abfragen durchführen kann, abgefragt werden können.

Wenn Ihr Anwendungsfall nicht erfordert, dass Sie Ihre eigenen Daten mitbringen, können Sie dieses Verfahren überspringen.

Wenn Ihre Datentabellen bereits katalogisiert sind AWS Glue, fahren Sie mit Erstellen einer konfigurierten Tabelle in AWS Clean Rooms fort.

Die Vorbereitung Ihrer Datentabellen umfasst die folgenden Schritte:

- Schritt 1: Erfüllen der Voraussetzungen
- Schritt 2: (Optional) Bereiten Sie Ihre Daten für kryptografische Berechnungen vor
- Schritt 3: Laden Sie Ihre Datentabelle auf Amazon S3 hoch
- Schritt 4: Erstellen Sie eine AWS Glue Tabelle
- Nächste Schritte

Weitere Informationen zu den Datenformaten, die Sie für Abfragen verwenden können, finden Sie unterDatenformate für AWS Clean Rooms.

Schritt 1: Erfüllen der Voraussetzungen

Um Ihre Datentabellen für die Verwendung mit vorzubereiten AWS Clean Rooms, müssen Sie die folgenden Voraussetzungen erfüllen:

- Ihre Datensätze müssen in einem der unterstützten Datenformate für AWS Clean Rooms gespeichert werden.
- Ihre Datentabellen müssen katalogisiert sein AWS Glue und die unterstützten Datentypen für verwenden. AWS Clean Rooms
- Alle Ihre Datentabellen müssen in Amazon Simple Storage Service (Amazon S3) in derselben Datei gespeichert werden, AWS-Region in der die Zusammenarbeit erstellt wurde.
- Sie AWS Glue Data Catalog müssen sich in derselben Region befinden, in der die Kollaboration erstellt wurde.
- Sie AWS Glue Data Catalog müssen sich in derselben Region befinden AWS-Konto wie die Mitgliedschaft.
- Der Amazon S3 S3-Bucket kann nicht registriert werden AWS Lake Formation.
- Der Ersteller der Kollaboration hat eine Kollaboration in eingerichtet AWS Clean Rooms. Weitere Informationen finden Sie unter Aufbau einer Zusammenarbeit in AWS Clean Rooms.
- Der Ersteller der Kollaboration hat die Kollaborations-ID an Sie als Teilnehmer der Kollaboration gesendet.

Schritt 2: (Optional) Bereiten Sie Ihre Daten für kryptografische Berechnungen vor

(Optional) Wenn Sie kryptografische Berechnungen verwenden und Ihre Datentabelle vertrauliche Informationen enthält, die Sie verschlüsseln möchten, müssen Sie die Datentabelle mit dem C3R-Verschlüsselungsclient verschlüsseln.

Gehen Sie wie unter beschrieben vor, um Ihre Daten für die kryptografische Datenverarbeitung vorzubereiten. Vorbereiten verschlüsselter Datentabellen mit Cryptographic Computing für Clean Rooms

Schritt 3: Laden Sie Ihre Datentabelle auf Amazon S3 hoch

> **Note**
>
> Wenn Sie beabsichtigen, verschlüsselte Datentabellen in der Zusammenarbeit zu verwenden, müssen Sie zuerst die Daten für kryptografische Berechnungen verschlüsseln, bevor Sie Ihre

Datentabelle auf Amazon S3 hochladen. Weitere Informationen finden Sie unter Vorbereiten verschlüsselter Datentabellen mit Cryptographic Computing für Clean Rooms.

So laden Sie Ihre Datentabelle auf Amazon S3 hoch

1. Melden Sie sich bei der Amazon S3 S3-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Buckets und dann einen Bucket aus, in dem Sie Ihre Datentabelle speichern möchten.
3. Wählen Sie Hochladen und folgen Sie dann den Anweisungen.
4. Wählen Sie die Registerkarte Objekte, um das Präfix anzuzeigen, in dem Ihre Daten gespeichert sind. Notieren Sie sich den Namen des Ordners.

   Sie können den Ordner auswählen, um die Daten anzuzeigen.

Schritt 4: Erstellen Sie eine AWS Glue Tabelle

Wenn Sie bereits über eine AWS Glue Datentabelle verfügen, können Sie diesen Schritt überspringen.

In diesem Schritt richten Sie einen Crawler ein AWS Glue , der alle Dateien in Ihrem S3-Bucket crawlt und eine AWS Glue Tabelle erstellt. Weitere Informationen finden Sie im AWS Glue Benutzerhandbuch unter Definieren von Crawlern.AWS Glue

Weitere Informationen zu unterstützten AWS Glue Data Catalog Datentypen finden Sie unterUnterstützte Datentypen.

> **Note**
>
> AWS Clean Rooms unterstützt derzeit keine S3-Buckets, bei AWS Lake Formation denen registriert ist.

Das folgende Verfahren beschreibt, wie Sie eine AWS Glue Tabelle erstellen. Wenn Sie ein AWS Glue Data Catalog verschlüsseltes Objekt mit einem Schlüssel AWS Key Management Service (AWS KMS) verwenden möchten, müssen Sie die KMS-Schlüsselberechtigungsrichtlinie so konfigurieren,

dass der Zugriff auf diese verschlüsselte Tabelle möglich ist. Weitere Informationen finden Sie unter Verschlüsselung in AWS Glue einrichten im AWS Glue Entwicklerhandbuch.

Um eine AWS Glue Tabelle zu erstellen

1. Folgen Sie dem Verfahren Arbeiten mit Crawlern auf der AWS Glue Konsole im AWS Glue Benutzerhandbuch.
2. Notieren Sie sich den AWS Glue Datenbanknamen und den AWS Glue Tabellennamen.

Nächste Schritte

Nachdem Sie Ihre Datentabellen vorbereitet haben, können Sie:

- Erstellen Sie eine konfigurierte Tabelle
- Erstellen Sie ein ML-Modell

Datenformate für AWS Clean Rooms

Bei den Datensätzen, die Sie für Abfragen verwenden, AWS Clean Rooms handelt es sich in der Regel um dieselben Datasetypen, die Sie für andere Anwendungen verwenden. Beispielsweise werden dieselben Datasetypen mit Amazon Athena, Amazon EMR, Amazon Redshift Spectrum und Amazon verwendet. QuickSight Sie können die Daten im Originalformat direkt von Amazon Simple Storage Service (Amazon S3) abfragen.

Um Daten abzufragen, müssen die Datensätze in einem Format vorliegen, das dies AWS Clean Rooms unterstützt. Der Amazon S3 S3-Bucket mit den Datensätzen und der AWS Clean Rooms Cluster müssen sich im selben AWS-Region befinden.

Unterstützte Datumsformate

AWS Clean Rooms unterstützt die folgenden strukturierten Formate:

- Apache Iceberg-Tabellen
- Parquet
- RCFile
- TextFile
- SequenceFile

- RegexSerde
- OpenCSV
- AVRO
- JSON

> **Note**
>
> Ein `timestamp` Wert in einer Textdatei muss das folgende Format `yyyy-MM-dd HH:mm:ss.SSSSSS` haben. Zum Beispiel:`2017-05-01 11:30:59.000000`.

Wir empfehlen die Verwendung eines spaltenförmigen Speicherdateiformats wieApache Parquet. Mit einem solchen Format minimieren Sie die Datenübertragung aus Amazon S3, indem Sie nur die benötigten Spalten auswählen. Für eine optimale Leistung sollten große Objekte in Objekte mit einer Größe von 100 MB bis 1 GB aufgeteilt werden.

Unterstützte Datentypen

Für eine optimale Benutzererfahrung müssen alle Ihre Daten katalogisiert werden. AWS Clean Rooms AWS Glue Weitere Informationen finden Sie im Abschnitt Erste Schritte mit dem AWS Glue Data Catalog im AWS Glue Entwicklerhandbuch.

AWS Clean Rooms unterstützt die folgenden AWS Glue Data Catalog Datentypen:

- bigint
- boolean
- char
- date
- decimal
- double
- float
- int
- Verschachtelte Datentypen wie:
  - array
  - map

  - struct
- smallint
- string
- timestamp
- varchar

AWS Clean Rooms unterstützt nicht:

- Binary
- Intervall

Arten der Dateikomprimierung für AWS Clean Rooms

Um Speicherplatz zu reduzieren, die Leistung zu verbessern und die Kosten zu minimieren, empfehlen wir dringend, Ihre Datensätze zu komprimieren.

AWS Clean Rooms erkennt Dateikomprimierungstypen anhand der Dateierweiterung und unterstützt die in der folgenden Tabelle aufgeführten Komprimierungstypen und -erweiterungen.

Komprimierungsalgorithmus	Dateierweiterung
GZIP	.gz
Bzip2	.bz2
Snappy	.snappy

Sie können die Komprimierung auf verschiedenen Ebenen anwenden. Zumeist komprimieren Sie eine ganze Datei oder einzelne Blöcke innerhalb einer Datei. Das Komprimieren von Spaltenformaten auf Dateiebene bringt keine Leistungsvorteile.

Serverseitige Verschlüsselung für AWS Clean Rooms

> **Note**
>
> Die serverseitige Verschlüsselung ersetzt nicht die kryptografische Datenverarbeitung in den Anwendungsfällen, in denen sie erforderlich ist.

AWS Clean Rooms entschlüsselt transparent Datensätze, die mit den folgenden Verschlüsselungsoptionen verschlüsselt wurden:

- SSE-S3 — Serverseitige Verschlüsselung mit einem AES-256-Verschlüsselungsschlüssel, der von Amazon S3 verwaltet wird
- SSE-KMS — Serverseitige Verschlüsselung mit Schlüsseln, die verwaltet werden von AWS Key Management Service

Um SSE-S3 verwenden zu können, muss die AWS Clean Rooms Servicerolle, die verwendet wird, um die konfigurierte Tabelle der Kollaboration zuzuordnen, über KMS-Decrypt-Berechtigungen verfügen. Um SSE-KMS verwenden zu können, muss die KMS-Schlüsselrichtlinie auch die Entschlüsselung der Servicerolle zulassen. AWS Clean Rooms

AWS Clean Rooms unterstützt keine clientseitige Amazon S3 S3-Verschlüsselung. Weitere Informationen zur serverseitigen Verschlüsselung finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung im Amazon Simple Storage Service-Benutzerhandbuch.

Verwenden von Apache Iceberg Tabellen in AWS Clean Rooms

Apache Icebergist ein Open-Source-Tabellenformat für Data Lakes. AWS Clean Rooms kann die in Apache Iceberg Metadaten gespeicherten Statistiken verwenden, um Abfragepläne zu optimieren und die Anzahl der Dateiscans bei der Verarbeitung von Abfragen im Reinraum zu reduzieren. Weitere Informationen finden Sie in der Apache Iceberg-Dokumentation.

Beachten Sie bei der Verwendung AWS Clean Rooms mit Iceberg-Tabellen Folgendes:

- Tabellen innerhalb des AWS Glue Data Catalog einzigen — Apache Iceberg Tabellen müssen in der auf dem Open-Source-Glue-Katalog AWS Glue Data Catalog basierenden Implementierung definiert werden.

- Parquet-Dateiformat — unterstützt AWS Clean Rooms nur Iceberg-Tabellen im Parquet-Datendateiformat.
- GZIP- und Snappy-Komprimierung — AWS Clean Rooms unterstützt Parquet mit GZIP und Komprimierung. Snappy
- Iceberg-Versionen — AWS Clean Rooms unterstützt das Ausführen von Abfragen für Iceberg-Tabellen der Versionen 1 und 2.
- Partitionen — Sie müssen Partitionen für Ihre Apache Iceberg Tabellen nicht manuell hinzufügen. AWS Glue AWS Clean Rooms erkennt neue Partitionen in Apache Iceberg Tabellen automatisch und es ist kein manueller Vorgang erforderlich, um Partitionen in der Tabellendefinition zu aktualisieren. Iceberg-Partitionen erscheinen als reguläre Spalten im AWS Clean Rooms Tabellenschema und nicht separat als Partitionsschlüssel im konfigurierten Tabellenschema.
- Einschränkungen
  - Nur neue Iceberg-Tabellen

    Apache IcebergAus Tabellen konvertierte Apache Parquet Tabellen werden nicht unterstützt.
  - Zeitreiseabfragen

    AWS Clean Rooms unterstützt keine Zeitreiseabfragen mit Apache Iceberg Tabellen.
  - Athena-Engine-Version 2

    IcebergTabellen, die mit der Athena-Engine Version 2 erstellt wurden, werden nicht unterstützt.
  - Dateiformate

    Avround ORC-Dateiformate (Optimized Row Columnar) werden nicht unterstützt.
  - Komprimierung

    ZstandardDie (Zstd) -Komprimierung für Parquet wird nicht unterstützt.

Unterstützte Datentypen für Iceberg-Tabellen

AWS Clean Rooms kann Iceberg Tabellen abfragen, die die folgenden Datentypen enthalten:

- boolean
- date
- decimal
- double

- float
- int
- list
- long
- map
- string
- struct
- timestamp without time zone

Weitere Informationen zu Iceberg-Datentypen finden Sie unter Schemata für Iceberg in der Apache-Iceberg-Dokumentation.

Vorbereiten verschlüsselter Datentabellen mit Cryptographic Computing für Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) ist eine Fähigkeit in. AWS Clean Rooms Sie können C3R verwenden, um kryptografisch einzuschränken, was von jeder Partei und in einer Zusammenarbeit gelernt werden kann. AWS AWS Clean Rooms

Sie können die Datentabelle mit dem C3R-Verschlüsselungsclient, einem clientseitigen Verschlüsselungstool, verschlüsseln, bevor Sie die Datentabelle auf Amazon Simple Storage Service (Amazon S3) hochladen.

Weitere Informationen finden Sie unter Kryptografisches Rechnen für Clean Rooms.

Die Vorbereitung verschlüsselter Datentabellen mit C3R umfasst die folgenden Schritte:

Schritte

Schritt 1: Erfüllen der Voraussetzungen

Um Ihre Datentabellen für die Verwendung mit C3R vorzubereiten, müssen Sie die folgenden Voraussetzungen erfüllen:

- Sie können auf das Clean Rooms Repository Cryptographic Computing for zugreifen unter: GitHub

  https://github.com/aws/c3r

- Sie haben AWS Anmeldeinformationen für die Verwendung des C3R-Verschlüsselungsclients eingerichtet. Diese Anmeldeinformationen werden vom C3R-Verschlüsselungsclient für schreibgeschützte API-Aufrufe zum Abrufen von Metadaten für die Zusammenarbeit AWS Clean Rooms verwendet. Weitere Informationen finden Sie unter Konfiguration von AWS CLI im AWS Command Line Interface Benutzerhandbuch für Version 2.
- Sie haben Java Runtime Environment (JRE) 11 oder höher auf Ihrem Computer installiert.
  - Die empfohlene VersionJava Runtime Environment, Amazon Corretto 11 oder höher, kann von https://aws.amazon.com/corretto heruntergeladen werden.
  - Das Java Development Kit (JDK) enthält eine entsprechende JRE Version derselben Version. Die zusätzlichen Funktionen von JDK werden jedoch nicht benötigt, um den Verschlüsselungsclient Cryptographic Computing for Clean Rooms (C3R) auszuführen.
- Ihre tabellarischen Datendateien (.csv) oder Dateien (. Parquet parquet) werden lokal gespeichert.
- Sie oder ein anderes Mitglied der Kollaboration haben die Möglichkeit, einen gemeinsamen geheimen Schlüssel zu erstellen. Weitere Informationen finden Sie unter Schritt 5: Erstellen Sie einen gemeinsamen geheimen Schlüssel.
- Der Ersteller der Kollaboration hat eine Kollaboration erstellt, in der AWS Clean Rooms Cryptographic Computing für die Zusammenarbeit aktiviert ist. Weitere Informationen finden Sie unter Aufbau einer Zusammenarbeit in AWS Clean Rooms.
- Der Kollaborationsersteller hat die Kollaborations-ID an Sie als Teilnehmer der Kollaboration gesendet. Der Amazon Resource Name (ARN) der Kollaboration ist in der gesendeten Einladung enthalten, die die Kollaborations-ID enthält.

Schritt 2: Laden Sie den C3R-Verschlüsselungsclient herunter

Um den C3R-Verschlüsselungsclient herunterzuladen von GitHub

1. Gehen Sie zum Clean RoomsAWSGitHub Repository Cryptographic Computing for: https://github.com/aws/c3r
2. Wählen Sie die Dateien aus und laden Sie sie herunter.

   Der Quellcode, die Lizenzen und das zugehörige Material können geklont oder als heruntergeladen werden. zipDatei von der Landingpage des GitHub Repositorys. (Siehe die Code-Schaltfläche oben rechts in der Inhaltsliste des Repositorys).

Der zuletzt signierte C3R-Verschlüsselungsclient Java Executable File (d. h. die Anwendung mit der Befehlszeilenschnittstelle) befindet sich auf der Releases-Seite des GitHub Repositorys.

Das C3R-Verschlüsselungsclientpaket für Apache Spark (`c3r-cli-spark`) ist eine Version der c3r-cli, die als Job an einen laufenden Apache Spark-Server gesendet werden muss. Weitere Informationen finden Sie unter C3R auf Apache Spark ausführen.

(Optional) Schritt 3: Verfügbare Befehle im C3R-Verschlüsselungsclient anzeigen

Gehen Sie wie folgt vor, um sich mit den verfügbaren Befehlen im C3R-Verschlüsselungsclient vertraut zu machen.

Um alle verfügbaren Befehle im C3R-Verschlüsselungsclient anzuzeigen

1. Navigieren Sie über eine Befehlszeilenschnittstelle (CLI) zu dem Ordner, der die heruntergeladene c3r-cli.jar Datei enthält.
2. Führen Sie den folgenden Befehl aus: `java -jar c3r-cli.jar`
3. Sehen Sie sich die Liste der verfügbaren Befehle und Optionen an.

Schritt 4: Generieren Sie ein Verschlüsselungsschema für eine tabellarische Datei

Um Daten zu verschlüsseln, ist ein Verschlüsselungsschema erforderlich, das beschreibt, wie die Daten verwendet werden. In diesem Abschnitt wird beschrieben, wie der C3R-Verschlüsselungsclient bei der Generierung eines Verschlüsselungsschemas für eine CSV-Datei mit einer Kopfzeile oder einer Parquet Datei hilft.

Sie müssen dies nur einmal pro Datei tun. Sobald das Schema existiert, kann es wiederverwendet werden, um dieselbe Datei (oder eine beliebige Datei mit identischen Spaltennamen) zu verschlüsseln. Wenn sich die Spaltennamen oder das gewünschte Verschlüsselungsschema ändern, müssen Sie die Schemadatei aktualisieren. Weitere Informationen finden Sie unter (Optional) Erstellen Sie ein Schema (fortgeschrittene Benutzer).

> **Important**
>
> Es ist von größter Bedeutung, dass alle beteiligten Parteien denselben gemeinsamen geheimen Schlüssel verwenden. Die beteiligten Parteien sollten auch die Spaltennamen so koordinieren, dass sie übereinstimmen, ob sie bei Abfragen JOIN bearbeitet oder auf andere Weise auf Gleichheit verglichen werden. Andernfalls könnten die SQL-Abfragen zu unerwarteten oder falschen Ergebnissen führen. Dies ist jedoch nicht erforderlich, wenn der Kollaborationsersteller die `allowJoinsOnColumnsWithDifferentNames` Verschlüsselungseinstellung bei der Erstellung der Kollaboration aktiviert hat. Weitere Informationen zu verschlüsselungsrelevanten Einstellungen finden Sie unter. Kryptografische Rechenparameter

Wenn der C3R-Verschlüsselungsclient im Schemamodus ausgeführt wird, durchsucht er die Eingabedatei spaltenweise und fragt Sie, ob und wie diese Spalte behandelt werden soll. Wenn die Datei viele Spalten enthält, die für die verschlüsselte Ausgabe nicht benötigt werden, kann die interaktive Schemagenerierung mühsam werden, da Sie jede unerwünschte Spalte überspringen müssen. Um dies zu vermeiden, könnten Sie manuell ein Schema schreiben oder eine vereinfachte Version der Eingabedatei erstellen, die nur die gewünschten Spalten enthält. Dann könnte der interaktive Schema-Generator für diese reduzierte Datei ausgeführt werden. Der C3R-Verschlüsselungsclient gibt Informationen über die Schemadatei aus und fragt Sie, wie die Quellspalten (wenn überhaupt) in der Zielausgabe enthalten oder verschlüsselt werden sollen.

Für jede Quellspalte in der Eingabedatei werden Sie aufgefordert, Folgendes einzugeben:

1. Wie viele Zielspalten sollen generiert werden
2. Wie soll jede Zielspalte verschlüsselt werden (wenn überhaupt)
3. Der Name jeder Zielspalte
4. Wie Daten vor der Verschlüsselung aufgefüllt werden sollen, wenn die Spalte als sealed Spalte verschlüsselt wird

> **Note**
>
> Wenn Sie Daten für eine Spalte verschlüsseln, die als Spalte verschlüsselt wurde, müssen Sie festlegen, welche Daten aufgefüllt werden müssen. sealed Der C3R-Verschlüsselungsclient schlägt bei der Schemagenerierung ein Standard-Padding vor, bei dem alle Einträge in einer Spalte auf dieselbe Länge aufgefüllt werden.

Beachten Sie bei der Bestimmung der Länge für`fixed`, dass das Auffüllen in Byte und nicht in Bits erfolgt.

Im Folgenden finden Sie eine Entscheidungstabelle für die Erstellung des Schemas.

Schema-Entscheidungstabelle

Entscheidung	Anzahl der Zielspalten aus der Quellspalte <' name-of-column '>?	Zielspaltentyp: [c]cleartext, [f] fingerprint oder [s]? sealed	Headername der Zielspalte <default 'name-of-column'>	Fügen Sie der <suffix>Kopfzeile ein Suffix hinzu, um anzugeben, wie sie verschlüsselt wurde, [y] ja oder [n] nein <default 'yes'>	<' name-of-column _sealed'> Polstertyp: [n] eins, [f] fest oder [m] max <default 'max'>
Lassen Sie die Spalte unverschlüsselt.	1	c	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Verschlüsseln Sie die Spalte als fingerprint Spalte.	1	f	Wählen Sie Standard oder geben Sie einen neuen Header-Namen ein.	Geben Sie einy, um Standard (`_fingerprint `) zu wählen, oder geben Sie die Eingabetaste einn.	Nicht zutreffend

Entscheidung	Anzahl der Zielspalten aus der Quellspalte <' name-of-column '>?	Zielspaltentyp: [c]cleartext, [f] fingerprint oder [s]? sealed	Headername der Zielspalte <default 'name-of-column'>	Fügen Sie der <suffix>Kopfzeile ein Suffix hinzu, um anzugeben, wie sie verschlüsselt wurde, [y] ja oder [n] nein <default 'yes'>	<' name-of-column _sealed'> Polstertyp: [n] eins, [f] fest oder [m] max <default 'max'>
Verschlüsseln Sie die Spalte als sealed Spalte.	1	S	Wählen Sie Standard oder geben Sie einen neuen Header-Namen ein.	Geben Sie einy, um Standard (`_sealed`) zu wählen, oder geben Sie die Eingabetaste einn.	Wählen Sie den Polstertyp. Weitere Informationen finden Sie unter (Optional) Erstellen Sie ein Schema (fortgeschrittene Benutzer).

Entscheidung	Anzahl der Zielspalten aus der Quellspalte <' name-of-column '>?	Zielspaltentyp: [c]cleartext, [f] fingerprint oder [s]? sealed	Headername der Zielspalte <default 'name-of-column'>	Fügen Sie der <suffix>Kopfzeile ein Suffix hinzu, um anzugeben, wie sie verschlüsselt wurde, [y] ja oder [n] nein <default 'yes'>	<' name-of-column _sealed'> Polstertyp: [n] eins, [f] fest oder [m] max <default 'max'>
Verschlüsseln Sie die Spalte sowohl als auchfingerprint. sealed	2	Geben Sie die erste Zielspalte ein: f. Geben Sie die zweite Zielspalte ein: s.	Wählen Sie die Zielüberschriften für jede Zielspalte aus.	Geben Sie einy, um Standard zu wählen, oder geben Sie ein n.	Wählen Sie den Fülltyp (nur für sealed Spalten). Weitere Informationen finden Sie unter (Optional) Erstellen Sie ein Schema (fortgeschrittene Benutzer).

Im Folgenden finden Sie zwei Beispiele für die Erstellung von Verschlüsselungsschemas. Der genaue Inhalt Ihrer Interaktion hängt von der Eingabedatei und den Antworten ab, die Sie geben.

Beispiele

- Beispiel: Generieren Sie ein Verschlüsselungsschema für eine fingerprint Spalte und eine cleartext Spalte

Beispiel: Generieren Sie ein Verschlüsselungsschema für eine fingerprint Spalte und eine cleartext Spalte

In diesem Beispiel gibt `ads.csv` es für nur zwei Spalten: `username` und`ad_variant`. Für diese Spalten wollen wir Folgendes:

- Damit die `username` Spalte als `fingerprint` Spalte verschlüsselt wird
- Damit die `ad_variant` Spalte eine `cleartext` Spalte ist

Um ein Verschlüsselungsschema für eine fingerprint Spalte und eine cleartext Spalte zu generieren

1. (Optional) Um sicherzustellen, dass die c3r-cli.jar Datei und die zu verschlüsselnde Datei vorhanden sind:

   a. Navigieren Sie zum gewünschten Verzeichnis und führen Sie es aus `ls` (falls Sie ein Mac oderUnix/verwendenLinux) oder `dir` wenn SieWindows) verwenden.

   b. Sehen Sie sich die Liste der tabellarischen Datendateien an (z. B. CSV) und wählen Sie eine zu verschlüsselnde Datei aus.

      In diesem Beispiel `ads.csv` ist das die Datei, die wir verschlüsseln möchten.

2. Führen Sie in der CLI den folgenden Befehl aus, um interaktiv ein Schema zu erstellen.

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

   > **Note**
   >
   > - Sie können ausführen`java --jar PATH/TO/c3r-cli.jar`. Oder, wenn Sie `PATH/TO/c3r-cli.jar` zu Ihrer CLASSPATH-Umgebungsvariablen etwas hinzugefügt haben, können Sie auch den Klassennamen ausführen. Der C3R-Verschlüsselungsclient sucht im CLASSPATH danach (z. B.). `java com.amazon.psion.cli.Main`
   > - Das `--interactive` Flag wählt den interaktiven Modus für die Entwicklung des Schemas aus. Dadurch wird der Benutzer durch einen Assistenten zum Erstellen des Schemas geführt. Benutzer mit fortgeschrittenen Kenntnissen können ihr eigenes

Schema-JSON erstellen, ohne den Assistenten zu verwenden. Weitere Informationen finden Sie unter (Optional) Erstellen Sie ein Schema (fortgeschrittene Benutzer).

- Das `--output` Flag legt einen Ausgabenamen fest. Wenn Sie das `--output` Flag nicht angeben, versucht der C3R-Verschlüsselungsclient, einen Standardausgabenamen zu wählen (z. B. `<input>.out.csv` oder für das Schema`<input>.json`).

3. Geben Sie für `Number of target columns from source column ‘username’?` die Eingabe ein **1** und drücken Sie dann die Eingabetaste.
4. Geben Sie für `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?` ein **f** und drücken Sie dann die Eingabetaste.
5. Drücken Sie für `Target column headername <default 'username'>` die Eingabetaste.

   Der Standardname '`username`' wird verwendet.
6. Geben Sie für `Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>` ein **y** und drücken Sie dann die Eingabetaste.

> **Note**
>
> Der interaktive Modus schlägt Suffixe vor, die zu den verschlüsselten Spaltenüberschriften hinzugefügt werden sollen (`_fingerprint`für fingerprint Spalten und `_sealed` für sealed Spalten). Die Suffixe können hilfreich sein, wenn Sie Aufgaben wie das Hochladen von Daten in Kollaborationen oder das Erstellen von Kollaborationen ausführen. AWS-Services AWS Clean Rooms Anhand dieser Suffixe kann angegeben werden, was mit den verschlüsselten Daten in den einzelnen Spalten geschehen kann. Zum Beispiel funktionieren Dinge nicht, wenn Sie eine Spalte als sealed Spalte (`_sealed`) verschlüsseln und versuchen, dies zu JOIN tun, oder wenn Sie es umgekehrt versuchen.

7. Geben Sie für `Number of target columns from source column ‘ad_variant’?` die Eingabe ein **1** und drücken Sie dann die Eingabetaste.
8. Geben Sie für `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?` ein **c** und drücken Sie dann die Eingabetaste.
9. Drücken Sie für `Target column headername <default 'username'>` die Eingabetaste.

Der Standardname '`ad_variant`' wird verwendet.

Das Schema wird in eine neue Datei mit dem Namen geschriebe`ads.json`.

> **Note**
>
> Sie können das Schema anzeigen, indem Sie es in einem beliebigen Texteditor öffnen, z. B. Notepad on Windows oder TextEdit onmacOS.

10. Sie sind jetzt bereit, Daten zu verschlüsseln.

Beispiel: Generieren Sie ein Verschlüsselungsschema mit sealed Spaltenfingerprint, und cleartext

In diesem Beispiel gibt `sales.csv` es für drei Spalten: `username``purchased`, und`product`. Für diese Spalten wollen wir Folgendes:

- Damit die `product` Spalte eine `sealed` Spalte ist
- Damit die `username` Spalte als `fingerprint` Spalte verschlüsselt wird
- Damit die `purchased` Spalte eine `cleartext` Spalte ist

Um ein Verschlüsselungsschema mit sealedfingerprint, und cleartext Spalten zu generieren

1. (Optional) Um sicherzustellen, dass die c3r-cli.jar Datei und die zu verschlüsselnde Datei vorhanden sind:

   a. Navigieren Sie zum gewünschten Verzeichnis und führen Sie es aus `ls` (falls Sie ein Mac oder`Unix/verwenden`Linux) oder `dir` wenn Sie`Windows`) verwenden.

   b. Sehen Sie sich die Liste der tabellarischen Datendateien (.csv) an und wählen Sie eine zu verschlüsselnde Datei aus.

      In diesem Beispiel `sales.csv` ist das die Datei, die wir verschlüsseln möchten.

2. Führen Sie in der CLI den folgenden Befehl aus, um interaktiv ein Schema zu erstellen.

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

> **Note**
>
> - Das `--interactive` Flag wählt den interaktiven Modus für die Entwicklung des Schemas aus. Dadurch wird der Benutzer durch einen geführten Arbeitsablauf zur Erstellung des Schemas geführt.
> - Wenn Sie ein erfahrener Benutzer sind, können Sie Ihr eigenes JSON-Schema erstellen, ohne den geführten Workflow zu verwenden. Weitere Informationen finden Sie unter (Optional) Erstellen Sie ein Schema (fortgeschrittene Benutzer).
> - Informationen zu CSV-Dateien ohne Spaltenüberschriften finden Sie im `--noHeaders` Flag für den Schemabefehl, der in der CLI verfügbar ist.
> - Das `--output` Flag legt einen Ausgabenamen fest. Wenn Sie das `--output` Flag nicht angeben, versucht der C3R-Verschlüsselungsclient, einen Standardausgabenamen zu wählen (z. B. `<input>.out` oder für das Schema`<input>.json`).

3. Geben Sie für `Number of target columns from source column ‘username’?` die Eingabe ein **1** und drücken Sie dann die Eingabetaste.
4. Geben Sie für `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?` ein **f** und drücken Sie dann die Eingabetaste.
5. Drücken Sie für `Target column headername <default 'username'>` die Eingabetaste.

   Der Standardname '`username`' wird verwendet.
6. Geben Sie für `Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>` ein **y** und drücken Sie dann die Eingabetaste.
7. Geben Sie für `Number of target columns from source column ‘purchased’?` ein **1** und drücken Sie dann die Eingabetaste.
8. Geben Sie für `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?` ein **c** und drücken Sie dann die Eingabetaste.
9. Drücken Sie für `Target column headername <default 'purchased'>` die Eingabetaste.

   Der Standardname '`purchased`' wird verwendet.
10. Geben Sie für `Number of target columns from source column ‘product’?` ein **1** und drücken Sie dann die Eingabetaste.

11. Geben Sie für `Target column type: [c]leartext, [f]ingerprint, or [s]ealed?` ein **`s`** und drücken Sie dann die Eingabetaste.
12. Drücken Sie für `Target column headername <default 'product'>` die Eingabetaste.

    Der Standardname '`product`' wird verwendet.
13. Drücken Sie für die Eingabetaste **`‘product_sealed’ padding type: [n]one, [f]ixed, or [m]ax <default ’max’?>`**, um die Standardeinstellung auszuwählen.
14. `Byte-length beyond max length to pad cleartext to in ‘product_sealed’ <default ‘0’>?`Drücken Sie die Eingabetaste, um die Standardeinstellung auszuwählen.

    Das Schema wird in eine neue Datei mit dem Namen geschrieben`sales.json`.
15. Sie sind jetzt bereit, Daten zu verschlüsseln.

Schritt 5: Erstellen Sie einen gemeinsamen geheimen Schlüssel

Um die Datentabellen zu verschlüsseln, müssen sich die Teilnehmer der Zusammenarbeit auf einen gemeinsamen geheimen Schlüssel einigen und diesen auf sichere Weise gemeinsam nutzen.

Der gemeinsame geheime Schlüssel muss mindestens 256 Bit (32 Byte) lang sein. Sie können einen größeren Schlüssel angeben, der Ihnen jedoch keine zusätzliche Sicherheit bietet.

> **Important**
>
> Denken Sie daran, dass der Schlüssel und die Kollaborations-ID, die für die Verschlüsselung und Entschlüsselung verwendet werden, für alle Kollaborationsteilnehmer identisch sein müssen.

Die folgenden Abschnitte enthalten Beispiele für Konsolenbefehle zum Generieren eines gemeinsamen geheimen Schlüssels, der `secret.key` im aktuellen Arbeitsverzeichnis des jeweiligen Terminals gespeichert wird.

Themen

- Beispiel: Schlüsselgenerierung mit OpenSSL
- Beispiel: Schlüsselgenerierung bei der Windows Verwendung PowerShell

Beispiel: Schlüsselgenerierung mit OpenSSL

Führen Sie für eine allgemeine Kryptografiebibliothek den folgenden Befehl aus, um einen gemeinsamen geheimen Schlüssel zu erstellen.

```
openssl rand 32 > secret.key
```

Wenn Sie sie verwenden Windows und noch nicht OpenSSL installiert haben, können Sie Schlüssel anhand des Beispiels generieren, das unter Beispiel: Schlüsselgenerierung bei Windows Verwendung PowerShell beschrieben ist.

Beispiel: Schlüsselgenerierung bei der Windows Verwendung PowerShell

Führen Sie für eine TerminalanwendungPowerShell, die auf verfügbar istWindows, den folgenden Befehl aus, um einen gemeinsamen geheimen Schlüssel zu erstellen.

```
$bs = New-Object Byte[](32);
[Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($bs); Set-
Content 'secret.key' -Encoding Byte -Value $bs
```

Schritt 6: Speichern Sie den gemeinsamen geheimen Schlüssel in einer Umgebungsvariablen

Eine Umgebungsvariable ist eine bequeme und erweiterbare Möglichkeit für Benutzer, einen geheimen Schlüssel aus verschiedenen Schlüsselspeichern bereitzustellen AWS Secrets Manager und ihn an den C3R-Verschlüsselungsclient weiterzuleiten.

Der C3R-Verschlüsselungsclient kann Schlüssel verwenden, die in gespeichert sind, AWS-Services wenn Sie die verwenden AWS CLI , um diese Schlüssel in der entsprechenden Umgebungsvariablen zu speichern. Der C3R-Verschlüsselungsclient kann beispielsweise einen Schlüssel von verwenden. AWS Secrets Manager Weitere Informationen finden Sie unter Geheimnisse erstellen und verwalten mit AWS Secrets Manager im AWS Secrets Manager Benutzerhandbuch.

> **Note**
>
> Bevor Sie jedoch ein AWS-Service solches als AWS Secrets Manager Aufbewahrung Ihrer C3R-Schlüssel verwenden, stellen Sie sicher, dass Ihr Anwendungsfall dies zulässt. In bestimmten Anwendungsfällen muss der Schlüssel möglicherweise vorenthalten werden.

AWS Dadurch soll sichergestellt werden, dass die verschlüsselten Daten und der Schlüssel niemals von derselben dritten Partei verwaltet werden.

Die einzigen Voraussetzungen für einen gemeinsamen geheimen Schlüssel sind, dass der gemeinsame geheime Schlüssel base64 -kodiert und in der Umgebungsvariablen gespeichert ist. `C3R_SHARED_SECRET`

In den folgenden Abschnitten werden die Konsolenbefehle zum Konvertieren einer `secret.key` Datei in eine Umgebungsvariable base64 und zum Speichern dieser Datei als Umgebungsvariable beschrieben. Die `secret.key` Datei könnte aus jedem der unter aufgeführten Befehle generiert worden sein Schritt 5: Erstellen Sie einen gemeinsamen geheimen Schlüssel und ist nur eine Beispielquelle.

Speichern Sie den Schlüssel in einer Umgebungsvariablen, wenn Windows Sie PowerShell

Führen Sie den folgenden Befehl ausPowerShell, um bei der Windows Verwendung in die Umgebungsvariable zu konvertieren base64 und sie festzulegen.

```
$Bytes=[IO.File]::ReadAllBytes((Get-Location).ToString()+'\secret.key');
 $env:C3R_SHARED_SECRET=[Convert]::ToBase64String($Bytes)
```

Speichern Sie den Schlüssel in einer Umgebungsvariablen auf Linux oder macOS

Führen Sie den folgenden Befehl ausmacOS, um in Linux oder zu konvertieren base64 und die Umgebungsvariable auf oder zu setzen.

```
export C3R_SHARED_SECRET="$(cat secret.key | base64)"
```

Schritt 7: Daten verschlüsseln

Um diesen Schritt auszuführen, müssen Sie die AWS Clean Rooms Kollaborations-ID und den gemeinsamen geheimen Schlüssel erwerben. Weitere Informationen finden Sie unter Voraussetzungen.

Im folgenden Beispiel führen wir die Verschlüsselung unter `ads.csv` Verwendung des von uns erstellten Schemas namens aus`ads.json`.

Um Daten zu verschlüsseln

1. Speichern Sie den gemeinsamen geheimen Schlüssel für die Zusammenarbeit in[Schritt 6: Speichern Sie den gemeinsamen geheimen Schlüssel in einer Umgebungsvariablen](#).
2. Geben Sie in der Befehlszeile den folgenden Befehl ein.

   ```
   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. <name of input .csv file>Geben Sie für den Namen der CSV-Eingabedatei ein.
4. Geben Sie für `schema=` den Namen der JSON-Verschlüsselungsschemadatei ein.
5. Geben Sie für `id=` die Kollaborations-ID ein.
6. Geben Sie für `output=` den Namen der Ausgabedatei ein (z. B.`ads-output.csv`).
7. Fügen Sie alle Befehlszeilen-Flags ein, die unter [Kryptografische Rechenparameter](#) und beschrieben sind[Optionale Flags in Cryptographic Computing für Clean Rooms](#).
8. Führen Sie den Befehl aus.

Im Beispiel für `ads.csv` führen wir den folgenden Befehl aus.

java -jar c3r-cli.jar encrypt ***ads.csv*** --schema=***ads.json*** --id=***123e4567-e89b-42d3-a456-556642440000*** --output=***ads-output.csv***

Im Beispiel für sales.csv führen wir den folgenden Befehl aus.

java -jar c3r-cli.jar encrypt ***sales.csv*** --schema=***sales.json*** --id=***123e4567-e89b-42d3-a456-556642440000***

> **Note**
>
> In diesem Beispiel geben wir keinen Namen für die Ausgabedatei (`--output=`*`sales-output.csv`*) an. Infolgedessen `name-of-file.out.csv` wurde der Standardname der Ausgabedatei generiert.

Sie sind jetzt bereit, die verschlüsselten Daten zu überprüfen.

Schritt 8: Überprüfen Sie die Datenverschlüsselung

Um zu überprüfen, ob die Daten verschlüsselt wurden

1. Zeigen Sie die verschlüsselte Datendatei an (z. B.`sales-output.csv`).
2. Überprüfen Sie die folgenden Spalten:

   a. Spalte 1 — Verschlüsselt (z. B.`username_fingerprint`).

      Für die fingerprint Spalten (HMAC) gibt es nach dem Versions- und Typpräfix (z. B.`01:hmac:`) 44 Zeichen mit Base64-codierten Daten.

   b. Spalte 2 — Nicht verschlüsselt (zum Beispiel). `purchased`

   c. Spalte 3 — Verschlüsselt (zum Beispiel`product_sealed`).

      Bei verschlüsselten (SELECT) Spalten ist die Länge der Spalte cleartext plus jegliches Auffüllen nach dem Versions- und Typpräfix (z. B.`01:enc:`) direkt proportional zur Länge der cleartext verschlüsselten Spalte. Das heißt, die Länge entspricht der Größe der Eingabe plus etwa 33 Prozent Mehraufwand aufgrund der Kodierung.

Sie sind jetzt bereit für:

1. Laden Sie die verschlüsselten Daten auf S3 hoch.
2. Erstellen Sie eine AWS Glue Tabelle.
3. Erstellen Sie eine konfigurierte Tabelle in AWS Clean Rooms.

Der C3R-Verschlüsselungsclient erstellt temporäre Dateien, die keine unverschlüsselten Daten enthalten (es sei denn, diese Daten würden auch in der endgültigen Ausgabe unverschlüsselt sein). Einige verschlüsselte Werte werden jedoch möglicherweise nicht richtig aufgefüllt. Fingerabdruckspalten können doppelte Werte enthalten, auch wenn die Einstellung für die Zusammenarbeit `allowRepeatedFingerprintValue` aktiviert ist`false`. Dieses Problem tritt auf, weil die temporäre Datei geschrieben wurde, bevor die richtigen Fülllängen und Eigenschaften zum Entfernen von Duplikaten überprüft wurden.

Wenn der C3R-Verschlüsselungsclient ausfällt oder während der Verschlüsselung unterbrochen wird, stoppt er möglicherweise, nachdem die temporäre Datei geschrieben wurde, aber bevor diese Eigenschaften überprüft und die temporären Dateien gelöscht wurden. Daher befinden sich diese temporären Dateien möglicherweise immer noch auf der Festplatte. Wenn dies der Fall ist,

schützt der Inhalt dieser Dateien die Klartextdaten nicht auf demselben Niveau wie die Ausgabe. Insbesondere könnten diese temporären Dateien Klartextdaten für statistische Analysen preisgeben, die sich nicht auf die endgültige Ausgabe auswirken würden. Der Benutzer sollte diese Dateien (insbesondere eine SQLite Datenbank) löschen, um zu verhindern, dass diese Dateien in unbefugte Hände gelangen.

(Optional) Erstellen Sie ein Schema (fortgeschrittene Benutzer)

Das manuelle Erstellen eines Schemas ist für fortgeschrittene Benutzer vorgesehen.

Im Folgenden finden Sie eine Beschreibung des JSON-Schemadateiformats für Eingabedateien mit oder ohne Spaltenüberschriften. Fortgeschrittene Benutzer können das Schema bei Bedarf direkt schreiben oder ändern.

> **Note**
>
> Der C3R-Verschlüsselungsclient kann Sie bei der Erstellung eines Schemas entweder durch den unter beschriebenen interaktiven Prozess Beispiel: Generieren Sie ein Verschlüsselungsschema mit sealed Spaltenfingerprint, und cleartext oder durch die Erstellung einer Stub-Vorlage unterstützen.

Schemas für zugeordnete und positionierte Tabellen

Im folgenden Abschnitt werden zwei Arten von Tabellenschemas beschrieben:

- Zugeordnetes Tabellenschema — Dieses Schema wird für die Verschlüsselung von CSV-Dateien mit einer Kopfzeile und Dateien verwendet. Apache Parquet
- Positionstabellenschema — Dieses Schema wird zum Verschlüsseln von CSV-Dateien ohne Kopfzeile verwendet.

Der C3R-Verschlüsselungsclient kann eine tabellarische Datei für eine Zusammenarbeit verschlüsseln. Dazu muss er über eine entsprechende Schemadatei verfügen, die angibt, wie die verschlüsselte Ausgabe aus der Eingabe abgeleitet werden soll.

Der C3R-Verschlüsselungsclient kann helfen, ein Schema für eine `INPUT` Datei zu generieren, indem er den Befehl C3R-Verschlüsselungsclient Schema in der Befehlszeile ausführt. Ein Beispiel für einen Befehl ist. `java -jar c3r-cli.jar schema --interactive INPUT`

Das Schema spezifiziert die folgenden Informationen:

1. Welche Quellspalten werden anhand ihrer Header-Namen (zugeordnete Schemas) oder ihrer Position (Positionsschemas) welchen transformierten Spalten in der Ausgabedatei zugeordnet
2. Welche Zielspalten sollen erhalten bleiben cleartext
3. Welche Zielspalten sollen für SELECT Abfragen verschlüsselt werden
4. Welche Zielspalten sollen für JOIN Abfragen verschlüsselt werden

Diese Informationen sind in einer tabellenspezifischen JSON-Schemadatei kodiert, die aus einem einzigen Objekt besteht, dessen `headerRow` Feld ein boolescher Wert ist. Der Wert muss `true` für Parquet Dateien und CSV-Dateien mit einer Kopfzeile gelten, andernfalls. `false`

Zugeordnetes Tabellenschema

Das zugeordnete Schema hat die folgende Form.

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": STRING,
      "targetHeader": STRING,
      "type": TYPE,
      "pad": PAD
    },
    ...
  ]
}
```

Falls `headerRow` ja`true`, ist das nächste Feld im Objekt`columns`, das eine Reihe von Spaltenschemas enthält, die Quellkopfzeilen Zielüberschriften zuordnen (d. h. JSON-Objekte, die beschreiben, was die Ausgabespalten enthalten sollen).

- `sourceHeader`— Der `STRING` Header-Name der Quellspalte, aus der die Daten abgeleitet wurden.

> **Note**
>
> Dieselbe Quellspalte kann für mehrere Zielspalten verwendet werden.

Eine Spalte aus der Eingabedatei, die nicht `sourceHeader` irgendwo im Schema aufgeführt ist, erscheint nicht in der Ausgabedatei.

- `targetHeader`— Der `STRING` Header-Name der entsprechenden Spalte in der Ausgabedatei.

> **Note**
>
> Dieses Feld ist für zugeordnete Schemas optional. Wenn dieses Feld weggelassen wird, `sourceHeader` wird das für den Header-Namen in der Ausgabe wiederverwendet. Entweder `_fingerprint` oder `_sealed` wird angehängt, wenn es sich bei der Ausgabespalte um eine fingerprint Spalte bzw. sealed Spalte handelt.

- `type`— Die `TYPE` der Zielspalte in der Ausgabedatei. Das heißt, eine von `cleartext`, `sealed`, oder `fingerprint` hängt davon ab, wie die Spalte in der Kollaboration verwendet wird.
- `pad`— Ein Feld eines Spaltenschemaobjekts, das nur vorhanden ist, wenn es vorhanden `TYPE` ist`sealed`. Sein entsprechender Wert von `PAD` ist ein Objekt, das beschreibt, wie die Daten aufgefüllt werden sollen, bevor sie verschlüsselt werden.

```
{
  "type": PAD_TYPE,
  "length": INT
}
```

Sie geben die Auffüllung vor der Verschlüsselung an `type` und `length` werden wie folgt verwendet:

- `PAD_TYPE`as `none` — Auf die Daten der Spalte wird kein Auffüllen angewendet, und das `length` Feld ist nicht zutreffend (d. h. es wird weggelassen).
- `PAD_TYPE`as `fixed` — Die Daten der Spalte werden auf die angegebene Anzahl `length` von Byte aufgefüllt.
- `PAD_TYPE`as `max` — Die Daten der Spalte werden auf die Größe der Bytelänge des längsten Werts zuzüglich weiterer `length` Byte aufgefüllt.

Im Folgenden finden Sie ein Beispiel für ein zugeordnetes Schema mit einer Spalte für jeden Typ.

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

Als komplexeres Beispiel finden Sie im Folgenden eine CSV-Beispieldatei mit Headern.

```
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
```

Im folgenden Beispiel für ein zugeordnetes Schema sind die Spalten `FirstName` und `LastName` Spalten. `cleartext` Die `State` Spalte ist als `fingerprint` Spalte und als `sealed` Spalte mit einer Auffüllung von verschlüsselt. `none` Die übrigen Spalten werden weggelassen.

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

Im Folgenden finden Sie die CSV-Datei, die sich aus dem zugewiesenen Schema ergibt.

```
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=
```

Positionstabellenschema

Das Positionsschema hat die folgende Form.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      },
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      }
    ],
    [],
    ...
  ]
}
```

Falls `headerRow` ja`false`, ist das nächste Feld im Objekt`columns`, das eine Reihe von Einträgen enthält. Jeder Eintrag ist selbst ein Array von null oder mehr positionellen Spaltenschemas (kein `sourceHeader` Feld). Dabei handelt es sich um JSON-Objekte, die beschreiben, was die Ausgabe enthalten soll.

- `sourceHeader`— Der `STRING` Header-Name der Quellspalte, aus der die Daten abgeleitet werden.

> **Note**
>
> Dieses Feld muss in Positionsschemas weggelassen werden. In Positionsschemas wird die Quellspalte aus dem entsprechenden Index der Spalte in der Schemadatei abgeleitet.

- `targetHeader`— Der `STRING` Header-Name der entsprechenden Spalte in der Ausgabedatei.

> **Note**
>
> Dieses Feld ist für Positionsschemas erforderlich.

- `type`— Die `TYPE` der Zielspalte in der Ausgabedatei. Das heißt, eine von `cleartext`, `sealed`, oder `fingerprint` hängt davon ab, wie die Spalte in der Kollaboration verwendet wird.
- `pad`— Ein Feld eines Spaltenschemaobjekts, das nur vorhanden ist, wenn es vorhanden `TYPE` ist`sealed`. Sein entsprechender Wert von `PAD` ist ein Objekt, das beschreibt, wie die Daten aufgefüllt werden sollen, bevor sie verschlüsselt werden.

```
{
  "type": PAD_TYPE,
  "length": INT
}
```

Sie geben die Auffüllung vor der Verschlüsselung an `type` und `length` werden wie folgt verwendet:

- `PAD_TYPE`as `none` — Auf die Daten der Spalte wird kein Auffüllen angewendet, und das `length` Feld ist nicht zutreffend (d. h. es wird weggelassen).
- `PAD_TYPE`as `fixed` — Die Daten der Spalte werden auf die angegebene Anzahl `length` von Byte aufgefüllt.
- `PAD_TYPE`as `max` — Die Daten der Spalte werden auf die Größe der Bytelänge des längsten Werts zuzüglich weiterer `length` Byte aufgefüllt.

> **Note**
>
> `fixed`ist nützlich, wenn Sie im Voraus eine Obergrenze für die Bytegröße der Spaltendaten kennen. Ein Fehler wird ausgelöst, wenn Daten in dieser Spalte länger als angegeben sind`length`.

`max`ist praktisch, wenn die genaue Größe der Eingabedaten unbekannt ist, da es unabhängig von der Größe der Daten funktioniert. `max`Erfordert jedoch zusätzliche Verarbeitungszeit, da die Daten zweimal verschlüsselt werden. `max`verschlüsselt die Daten einmal, wenn sie in die temporäre Datei eingelesen werden, und einmal, nachdem der längste Dateneintrag in der Spalte bekannt ist.
Außerdem wird die Länge des längsten Werts zwischen Aufrufen des Clients nicht gespeichert. Wenn Sie planen, Ihre Daten stapelweise oder regelmäßig neue Daten zu verschlüsseln, beachten Sie, dass die daraus resultierenden Chiffretext-Längen je nach Batch variieren können.

Im Folgenden finden Sie ein Beispiel für ein Positionsschema.

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

Im Folgenden finden Sie ein Beispiel für eine CSV-Beispieldatei, falls sie nicht die erste Zeile mit den Überschriften hatte.

```
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
```

Das Positionsschema hat die folgende Form.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": "GivenName",
        "type": "cleartext"
      }
    ],
    [
      {
        "targetHeader": "Surname",
        "type": "cleartext"
      }
    ],
    [],
    [],
    [
      {
        "targetHeader": "State_Join",
        "type": "fingerprint"
```

```
      },
      {
        "targetHeader": "State",
        "type": "sealed",
        "pad": {
          "type": "none"
        }
      }
    ],
    [],
    [],
    [],
    []
  ]
}
```

Das vorherige Schema erzeugt die folgende Ausgabedatei mit einer Kopfzeile, die die angegebenen Ziel-Header enthält.

```
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=
```

Erstellen einer konfigurierten Tabelle in AWS Clean Rooms

Eine konfigurierte Tabelle ist ein Verweis auf eine vorhandene Tabelle in der AWS Glue Data Catalog. Sie enthält eine Analyseregel, die festlegt, wie die Daten abgefragt werden können. AWS Clean Rooms Konfigurierte Tabellen können einer oder mehreren Kollaborationen zugeordnet werden. Weitere Informationen AWS Glue dazu finden Sie im AWS Glue Developer Guide.

Verwenden Sie die von bereitgestellte Statistikgenerierung AWS Glue , um Statistiken auf Spaltenebene für Tabellen zu berechnen. AWS Glue Data Catalog Sobald Statistiken für Tabellen im Datenkatalog AWS Glue generiert wurden, verwendet Amazon Redshift Spectrum diese Statistiken automatisch, um den Abfrageplan zu optimieren. Weitere Informationen zur Berechnung von Statistiken auf Spaltenebene mithilfe von Informationen finden Sie im AWS Glue Leitfaden Arbeiten mit Spaltenstatistiken.

Erstellen Sie eine konfigurierte Tabelle

In diesem Schritt erstellen Sie eine konfigurierte Tabelle, AWS Clean Rooms die in der Zusammenarbeit verwendet werden soll.

Um eine konfigurierte Tabelle zu erstellen in AWS Clean Rooms

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie in der oberen rechten Ecke die Option Neue Tabelle konfigurieren aus.
4. Für Neue Tabelle konfigurieren, für AWS Glue Tabelle auswählen:

    a. Wählen Sie die Datenbank, die Sie konfigurieren möchten, aus der Dropdownliste aus.

    b. Wählen Sie die Tabelle, die Sie konfigurieren möchten, aus der Dropdownliste aus.

> **Note**
>
> Um zu überprüfen, ob es sich um die richtige Tabelle handelt, führen Sie einen der folgenden Schritte aus:
>
> - Wählen Sie Anzeigen in AWS Glue.

- Aktivieren Sie „Schema anzeigen“, um das Schema anzuzeigen.

5. Wählen Sie für Spalten, die in Kollaborationen zulässig sind, entweder Alle Spalten oder Benutzerdefinierte Liste aus.

Wenn Sie folgendes auswählen …	Dann...
Alle Spalten	Alle Spalten dürfen in verwendet werden AWS Clean Rooms (vorbehaltlich der Analyseregeln).
Benutzerdefinierte Liste	Wählen Sie aus der Dropdownliste Zulässige Spalten angeben eine oder mehrere Spalten aus, die Sie zulassen möchten.

6. Einzelheiten zur konfigurierten Tabelle finden Sie unter

   a. Geben Sie einen Namen für die konfigurierte Tabelle ein.

      Sie können den Standardnamen verwenden oder diese Tabelle umbenennen.

   b. Geben Sie eine Beschreibung der Tabelle ein.

      Die Beschreibung hilft dabei, zwischen anderen konfigurierten Tabellen mit ähnlichen Namen zu unterscheiden.

   c. Wenn Sie Tags für die konfigurierte Tabellenressource aktivieren möchten, wählen Sie Neues Tag hinzufügen und geben Sie dann das Schlüssel - und Wertepaar ein.

7. Wählen Sie Neue Tabelle konfigurieren.

Nächste Schritte

Nachdem Sie eine konfigurierte Tabelle erstellt haben, können Sie:

- Konfigurieren Sie eine Analyseregel für die konfigurierte Tabelle
- Ordnen Sie die konfigurierte Tabelle einer Kollaboration zu

Konfiguration einer Analyseregel für eine konfigurierte Tabelle

In den folgenden Abschnitten wird beschrieben, wie Sie eine Analyseregel für Ihre konfigurierte Tabelle konfigurieren. Durch die Definition der Analyseregeln können Sie das Mitglied, das Abfragen durchführen kann, autorisieren, Abfragen auszuführen, die einer bestimmten Analyseregel entsprechen, die von unterstützt wird. AWS Clean Rooms

AWS Clean Roomsunterstützt die folgenden Arten von Analyseregeln: Aggregations -, Listen- und benutzerdefinierte Regeln.

Pro konfigurierter Tabelle kann es nur eine Analyseregel geben.

> **Important**
>
> Wenn Sie Cryptographic Computing für verwenden Clean Rooms und in der Zusammenarbeit verschlüsselte Datentabellen verwenden, sollte die Analyseregel, die Sie der verschlüsselten konfigurierten Tabelle hinzufügen, mit der Art der Verschlüsselung der Daten übereinstimmen. Wenn Sie beispielsweise die Daten für SELECT (Aggregationsanalyseregel) verschlüsselt haben, sollten Sie die Analyseregel für JOIN (Listenanalyseregel) nicht hinzufügen.

Informationen zu den Typen von Analyseregeln, die in verfügbar sindAWS Clean Rooms, finden Sie unterAnalyseregeln in AWS Clean Rooms.

Weitere Informationen zur Regel für die Aggregationsanalyse finden Sie unterRegel für die Aggregationsanalyse.

Weitere Informationen zur Regel für die Listenanalyse finden Sie unterAnalyseregel auflisten.

Weitere Informationen zur benutzerdefinierten Analyseregel finden Sie unterBenutzerdefinierte Analyseregel in AWS Clean Rooms.

Nachdem Sie diese Abschnitte gelesen und verstanden haben, können Sie die folgenden Verfahren ausführen:

Themen

- Konfiguration einer Aggregationsanalyseregel für eine Tabelle (geführter Ablauf)

Konfiguration einer Aggregationsanalyseregel für eine Tabelle (geführter Ablauf)

Die Aggregationsanalyseregel ermöglicht Abfragen, die Statistiken aggregieren, ohne Informationen auf Zeilenebene mithilfe von COUNTSUM, und AVG Funktionen entlang optionaler Dimensionen preiszugeben.

In diesem Verfahren wird beschrieben, wie Sie Ihrer konfigurierten Tabelle mithilfe der Option Guided Flow in der Konsole eine Aggregationsanalyseregel hinzufügen. AWS Clean Rooms

So fügen Sie die Aggregationsanalyseregel zu einer Tabelle hinzu (Guided Flow)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie die konfigurierte Tabelle aus.
4. Wählen Sie auf der Detailseite der konfigurierten Tabelle die Option Analyseregel konfigurieren aus.
5. Lassen Sie unter Schritt 1: Typ auswählen unter Typ die Option Aggregation standardmäßig ausgewählt.
6. Wählen Sie unter Erstellungsmethode die Option Geführter Flow und dann Weiter aus.
7. Gehen Sie unter Schritt 2: Abfragesteuerelemente angeben für Aggregatfunktionen wie folgt vor:

    a. Wählen Sie eine Aggregatfunktion aus der Dropdownliste aus:

    - ZÄHLEN
    - ZÄHLE UNTERSCHIEDLICH
    - SUM
    - DIFFERENZIERTE SUMME
    - AVG

b. Wählen Sie aus der Dropdownliste „Spalten“ aus, welche Spalten in der Aggregatfunktion verwendet werden können.

c. (Optional) Wählen Sie Weitere Funktion hinzufügen, um eine weitere Aggregatfunktion hinzuzufügen und dieser Funktion eine oder mehrere Spalten zuzuordnen.

> **Note**
>
> Es ist mindestens eine Aggregatfunktion erforderlich.

d. (Optional) Wählen Sie Entfernen, um eine Aggregatfunktion zu entfernen.

8. Für Join-Steuerelemente

a. Wählen Sie eine Option für die automatische Abfrage der Tabelle zulassen aus:

Wenn Sie folgendes auswählen …	Dann...
Nein, es können nur Überschneidungen abgefragt werden	Die Tabelle kann nur abgefragt werden, wenn sie mit einer Tabelle verknüpft ist, die dem Mitglied gehört, das Abfragen ausführen kann.
Ja	Die Tabelle kann eigenständig oder wenn sie mit anderen Tabellen verknüpft ist, abgefragt werden.

b. Wählen Sie unter Verbindungsspalten angeben die Spalten aus, deren Verwendung in der INNER JOIN Anweisung zulässig sein soll.

Dies ist optional, wenn Sie im vorherigen Schritt Ja ausgewählt haben.

c. Wählen Sie unter Zulässige Operatoren für den Abgleich angeben aus, welche Operatoren gegebenenfalls für den Abgleich mehrerer Join-Spalten verwendet werden können. Wenn Sie zwei oder mehr JOIN Spalten auswählen, ist einer dieser Operatoren erforderlich.

Wenn Sie folgendes auswählen …	Dann...
UND	Sie können `AND` in das `INNER JOIN` Spiel Bedingungen einbeziehen, um eine

Wenn Sie folgendes auswählen …	Dann...
	Spalte mit einer anderen Spalte zwischen Tabellen zu verbinden.
ODER	Sie können `OR` in die `INNER JOIN` Abgleichsbedingungen aufnehmen, um mehrere Spaltenübereinstimmungen zwischen Tabellen zu kombinieren. Dieser logische Operator ist nützlich, um eine höhere Trefferquote zu erzielen.

9. (Optional) Wählen Sie für Dimensionssteuerelemente in der Dropdownliste Dimensionsspalten angeben aus, welche Spalten Sie in der SELECT-Anweisung sowie in den ORDER BY Teilen WHERE GROUPBY, und der Abfrage verwenden lassen möchten.

> **Note**
>
> Aggregatfunktion oder Join-Spalten können nicht als Dimensionsspalten verwendet werden.

10. Wählen Sie für Skalarfunktionen eine Option für Welche Skalarfunktionen möchten Sie zulassen?

Wenn Sie folgendes auswählen …	Dann...
Alle werden derzeit unterstützt von AWS Clean Rooms	Sie erlauben alle Skalarfunktionen, die derzeit von AWS Clean Rooms unterstützt werden. • Sie können „Liste anzeigen“ wählen, um die gesamte Liste der unterstützten Skalarfunktionen von anzuzeigen. AWS Clean Rooms
Eine benutzerdefinierte Liste	Sie können anpassen, welche Skalarfun ktionen zulässig sind.

Wenn Sie folgendes auswählen …	Dann...
	• Wählen Sie eine oder mehrere Optionen aus der Dropdownliste Zulässige Skalarfunktionen angeben aus.
Keine	Sie möchten keine Skalarfunktionen zulassen.

Weitere Informationen finden Sie unter Skalarfunktionen.

11. Wählen Sie Weiter.
12. Gehen Sie unter Schritt 3: Steuerelemente für Abfrageergebnisse angeben für Aggregationseinschränkungen wie folgt vor:
    a. Wählen Sie die Dropdownliste für jeden Spaltennamen aus.
    b. Wählen Sie die Dropdownliste für jede Mindestanzahl unterschiedlicher Werte aus, die erfüllt sein müssen, damit jede Ausgabezeile zurückgegeben wird, nachdem die COUNT DISTINCT Funktion darauf angewendet wurde.
    c. Wählen Sie Einschränkung hinzufügen, um weitere Aggregationseinschränkungen hinzuzufügen.
    d. (Optional) Wählen Sie Entfernen, um eine Aggregationsbeschränkung zu entfernen.
13. Wählen Sie Weiter.
14. Überprüfen Sie unter Schritt 4: Überprüfen und konfigurieren die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, bearbeiten Sie sie gegebenenfalls und wählen Sie dann Analyseregel konfigurieren aus.

Es wird eine Bestätigungsmeldung angezeigt, dass Sie erfolgreich eine Aggregationsanalyseregel für die Tabelle konfiguriert haben.

Konfiguration einer Listenanalyseregel für eine Tabelle (geführter Ablauf)

Die Listenanalyseregel ermöglicht Abfragen, die Listen auf Zeilenebene ausgeben, in denen die Überschneidung zwischen der zugehörigen Tabelle und einer Tabelle des Mitglieds, das Abfragen durchführen kann, dargestellt wird.

Dieses Verfahren beschreibt den Vorgang des Hinzufügens der Listenanalyseregel zu Ihrer konfigurierten Tabelle mithilfe der Option Geführter Ablauf in der AWS Clean Rooms Konsole.

So fügen Sie einer Tabelle eine Listenanalyseregel hinzu (geführter Ablauf)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie die konfigurierte Tabelle aus.
4. Wählen Sie auf der Detailseite der konfigurierten Tabelle die Option Analyseregel konfigurieren aus.
5. Wählen Sie unter Schritt 1: Typ auswählen und unter Typ die Option Liste aus.
6. Wählen Sie unter Erstellungsmethode die Option Geführter Ablauf und dann Weiter aus.
7. Gehen Sie unter Schritt 2: Abfragesteuerelemente angeben für Join-Steuerelemente wie folgt vor:

    a. Wählen Sie unter Join-Spalten angeben die Spalten aus, deren Verwendung in der INNER JOIN Anweisung zulässig sein soll.

    b. Wählen Sie unter Zulässige Operatoren für den Abgleich angeben aus, welche Operatoren gegebenenfalls für den Abgleich mehrerer Join-Spalten verwendet werden können. Wenn Sie zwei oder mehr JOIN Spalten auswählen, ist einer dieser Operatoren erforderlich.

Wenn Sie folgendes auswählen …	Dann...
UND	Sie können `AND` in das `INNER JOIN` Spiel Bedingungen einbeziehen, um eine Spalte mit einer anderen Spalte zwischen Tabellen zu verbinden.

Wenn Sie folgendes auswählen …	Dann...
ODER	Sie können `OR` in die `INNER JOIN` Abgleichsbedingungen aufnehmen, um mehrere Spaltenübereinstimmungen zwischen Tabellen zu kombinieren. Dieser logische Operator ist nützlich, um eine höhere Trefferquote zu erzielen.

8. (Optional) Wählen Sie für Listensteuerelemente in der Dropdownliste „Listenspalten angeben“ aus, welche Spalten in der Abfrageausgabe (d. h. in der SELECT Anweisung) oder zum Filtern von Ergebnissen (d. h. in der WHERE Anweisung) verwendet werden sollen.
9. Wählen Sie Weiter.
10. Überprüfen Sie unter Schritt 3: Überprüfen und konfigurieren die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, bearbeiten Sie sie gegebenenfalls und wählen Sie dann Analyseregel konfigurieren aus.

Es wird eine Bestätigungsmeldung angezeigt, dass Sie eine Listenanalyseregel für die Tabelle erfolgreich konfiguriert haben.

Konfiguration einer benutzerdefinierten Analyseregel für eine Tabelle (geführter Ablauf)

Die benutzerdefinierte Analyseregel ermöglicht benutzerdefinierte SQL-Abfragen für eine konfigurierte Tabelle. Die benutzerdefinierte Analyseregel ist erforderlich, wenn Analysevorlagen oder Differential Privacy verwendet werden.

In diesem Verfahren wird beschrieben, wie Sie die benutzerdefinierte Analyseregel mithilfe der Option Guided Flow in der AWS Clean Rooms Konsole zu Ihrer konfigurierten Tabelle hinzufügen.

So fügen Sie einer Tabelle eine benutzerdefinierte Analyseregel hinzu (geführter Ablauf)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie die konfigurierte Tabelle aus.

4. Wählen Sie auf der Detailseite der konfigurierten Tabelle die Option Analyseregel konfigurieren aus.
5. Wählen Sie unter Schritt 1: Typ auswählen und unter Typ die Option Benutzerdefiniert aus.
6. Wählen Sie unter Erstellungsmethode die Option Geführter Ablauf und dann Weiter aus.
7. Legen Sie unter Schritt 2: Differentiellen Datenschutz einrichten fest, ob Sie den differenziellen Datenschutz ein- oder ausschalten möchten. Differential Privacy ist eine mathematisch erprobte Technik, mit der Sie Ihre Daten vor Reidentifikationsangriffen schützen können.

   a. Für differenziellen Datenschutz:

Wenn du...	Dann wähle...
Sie verfügen über Daten auf Benutzere bene und möchten sich vor Versuchen zur erneuten Identifizierung schützen	Einschalten
Sie verfügen nicht über Daten auf Benutzerebene oder benötigen keinen Schutz vor Versuchen zur erneuten Identifizierung	Ausschalten

   b. Wenn Sie sich für die Aktivierung des differenzierten Datenschutzes entschieden haben, wählen Sie die Spalte Benutzer-ID aus, die die eindeutige Kennung Ihrer Benutzer enthält, z. B. die `user_id` Spalte, deren Privatsphäre Sie schützen möchten. Wenn Sie den differenziellen Datenschutz für zwei oder mehr Tabellen in einer Kollaboration aktivieren möchten, müssen Sie in beiden Analyseregeln dieselbe Spalte wie die Benutzer-ID-Spalte konfigurieren, um eine konsistente Definition von Benutzern in allen Tabellen zu gewährleisten. Im Falle einer Fehlkonfiguration erhält das Mitglied, das Abfragen durchführen kann, eine Fehlermeldung, dass zwei Spalten zur Auswahl stehen, um die Anzahl der Benutzerbeiträge (z. B. die Anzahl der von einem Nutzer getätigten Anzeigenimpressionen) während der Ausführung der Abfrage zu berechnen.

   c. Wählen Sie Weiter.
8. Unter Schritt 3: Abfragesteuerelemente angeben

   a. Geben Sie als Steuerelement Folgendes ein:

Wenn Sie …	Dann wähle...
Überprüfen Sie jede neue Analysevorlage, bevor sie in Ihrer konfigurierten Tabelle ausgeführt wird	Überprüfen Sie jede neue Analyse, bevor sie in dieser Tabelle ausgeführt werden darf
Lassen Sie jede Analysevorlage oder direkte Abfrage an Ihrer konfigurierten Tabelle durchführen	Erlauben Sie, dass alle Abfragen, die von bestimmten Mitarbeitern erstellt wurden, ohne Überprüfung in dieser Tabelle ausgeführt werden

b. Wählen Sie eine der folgenden Optionen aus:

Wenn du gewählt hast...	Dann...
Prüfen Sie jede neue Analyse, bevor sie auf dieser Tabelle ausgeführt werden darf	Wählen Sie unter Analysevorlagen, die ausgeführt werden dürfen, die Option Analysevorlage hinzufügen aus und wählen Sie dann die entsprechende Vorlage für Zusammenarbeit und Analyse aus den Dropdownlisten aus.
Lassen Sie zu, dass alle Abfragen, die von bestimmten Mitarbeitern erstellt wurden, in dieser Tabelle ohne Überprüfung ausgeführt werden	Wählen Sie unter AWS-KontenZulässig zum Erstellen beliebiger Abfragen die Option Hinzufügen AWS-Konto und dann die entsprechende AWS-KontoID aus.

9. Wählen Sie Weiter.
10. Überprüfen Sie unter Schritt 4: Überprüfen und konfigurieren die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, bearbeiten Sie sie gegebenenfalls und wählen Sie dann Analyseregel konfigurieren aus.

Es wird eine Bestätigungsmeldung angezeigt, dass Sie erfolgreich eine benutzerdefinierte Analyseregel für die Tabelle konfiguriert haben.

Analyseregel für eine Tabelle konfigurieren (JSON-Editor)

Das folgende Verfahren zeigt, wie Sie mithilfe der JSON-Editor-Option in der AWS Clean Rooms Konsole eine Analyseregel zu einer Tabelle hinzufügen.

So konfigurieren Sie eine Aggregations-, Liste- oder benutzerdefinierte Analyseregel zu einer Tabelle (JSON-Editor)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie die konfigurierte Tabelle aus.
4. Wählen Sie auf der Detailseite der konfigurierten Tabelle die Option Analyseregel konfigurieren aus.
5. Wählen Sie unter Schritt 1: Typ auswählen unter Typ entweder die Option Aggregation, Liste oder Benutzerdefiniert aus.
6. Wählen Sie unter Erstellungsmethode die Option JSON-Editor und dann Weiter aus.
7. Unter Schritt 2: Steuerelemente angeben können Sie wählen, ob Sie eine Abfragestruktur (Vorlage einfügen) oder eine Datei einfügen möchten (Aus Datei importieren).

Wenn Sie folgendes auswählen …	Dann...
Vorlage einfügen	1. Geben Sie die Parameter für die ausgewählte Analyseregel in der Definition der Analyseregel an. 2. Sie können Strg + Leertaste drücken, um die automatische Vervollständigung zu aktivieren. Weitere Informationen zu den Regelpara metern für die Aggregationsanalyse finden Sie unter. Aggregationsanalyseregel – Abfragesteuerungen

Wenn Sie folgendes auswählen …	Dann...
	Weitere Informationen zu Regelparametern für Listenanalysen finden Sie unterAnalyseregel auflisten – Abfragesteuerungen.
Aus einer Datei importieren	1. Wählen Sie Ihre JSON-Datei von Ihrem lokalen Laufwerk aus. 2. Klicken Sie auf Open. In der Analyseregeldefinition wird die Analyseregel aus der hochgeladenen Datei angezeigt.

8. Wählen Sie Weiter.
9. Überprüfen Sie unter Schritt 3: Überprüfen und konfigurieren die Auswahlen, die Sie für die vorherigen Schritte getroffen haben, bearbeiten Sie sie gegebenenfalls und wählen Sie dann Analyseregel konfigurieren aus.

Sie erhalten eine Bestätigungsnachricht, dass Sie eine Analyseregel für die Tabelle erfolgreich konfiguriert haben.

Nächste Schritte

Nachdem Sie eine Analyseregel für Ihre konfigurierte Tabelle konfiguriert haben, können Sie:

- Ordnen Sie eine konfigurierte Tabelle einer Kollaboration zu
- Fragen Sie die Datentabellen ab (als Mitglied, das Abfragen durchführen kann)

Eine konfigurierte Tabelle einer Kollaboration zuordnen

Nachdem Sie eine konfigurierte Tabelle erstellt und ihr eine Analyseregel hinzugefügt haben, können Sie sie einer Kollaboration zuordnen.

Important

Bevor Sie die konfigurierten AWS Glue Tabellen der Kollaboration zuordnen, muss der Speicherort der AWS Glue Tabelle auf einen Amazon Simple Storage Service (Amazon S3) -Ordner und nicht auf eine einzelne Datei verweisen. Sie können diesen Speicherort überprüfen, indem Sie sich die Tabelle in der AWS Glue Konsole unter https://console.aws.amazon.com/glue/ ansehen.

Note

Wenn Sie die Verschlüsselung in konfiguriert AWS Glue und eine Servicerolle erstellt haben, müssen Sie dieser Rolle Zugriff gewähren, damit AWS KMS keys sie AWS Glue Tabellen entschlüsseln kann.
Wenn Sie eine konfigurierte Tabelle verknüpft haben, die von einem AWS KMS-verschlüsselten Amazon S3 S3-Datensatz unterstützt wird, müssen Sie der Rolle Zugriff gewähren, damit sie den KMS-Schlüssel zum Entschlüsseln von Amazon S3 S3-Daten verwenden kann.
Weitere Informationen finden Sie unter Verschlüsselung einrichten AWS Glue im AWS Glue Entwicklerhandbuch.

In den folgenden Themen wird beschrieben, wie Sie mithilfe der AWS Clean Rooms Konsole eine konfigurierte Tabelle einer Kollaboration zuordnen:

Themen

Informationen dazu, wie Sie Ihre konfigurierten Tabellen mithilfe der AWS SDKs der Kollaboration zuordnen, finden Sie in der AWS Clean Rooms API-Referenz.

Ordnen Sie eine konfigurierte Tabelle auf der Detailseite der konfigurierten Tabelle zu

Um der Kollaboration AWS Glue Tabellen von der konfigurierten Tabellendetailseite aus zuzuordnen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie die konfigurierte Tabelle aus.
4. Wählen Sie auf der Detailseite der konfigurierten Tabelle die Option Mit Kollaboration verknüpfen aus.
5. Wählen Sie im Dialogfeld Tabelle mit Kollaboration verknüpfen die Option Kollaboration aus der Dropdownliste aus.
6. Wählen Sie Zusammenarbeit auswählen aus.

   Auf der Seite Tabelle zuordnen wird der Name der ausgewählten konfigurierten Tabelle im Abschnitt Konfigurierte Tabelle auswählen angezeigt.
7. Gehen Sie unter Konfigurierte Tabelle auswählen wie folgt vor:

Wenn Sie …	Dann...
Konfiguriere eine neue Tabelle	Wählen Sie Tabelle konfigurieren und folgen Sie den Anweisungen auf der Seite Tabelle konfigurieren.
Zeigen Sie das Schema und die Analysere gel für die konfigurierte Tabelle an	Aktivieren Sie die Option Schema und Analyseregel anzeigen.

8. Geben Sie die Dienstzugriffsberechtigungen an, indem Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden auswählen.

Wenn Sie folgendes auswählen …	Dann...
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Clean Rooms erstellt eine Servicerolle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautet `cleanrooms-<timestamp>` • Sie müssen über die erforderlichen Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, können Sie Diese Daten sind mit einem KMS-Schlüssel verschlüsselt auswählen und dann einen eingeben AWS KMS key , der zur Entschlüsselung Ihrer Dateneingabe verwendet wird.

Wenn Sie folgendes auswählen …	Dann...
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicero llennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Wenn keine vorhandenen Servicero llen vorhanden sind, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. Versucht standardmäßig AWS Clean Rooms nicht, die bestehende Rollenric htlinie zu aktualisieren, um die erforderl ichen Berechtigungen hinzuzufügen. 3. (Optional) Aktivieren Sie das Kontrollk ästchen Eine vorkonfigurierte Richtlinie mit den erforderlichen Berechtigungen zu dieser Rolle hinzufügen, um der Rolle die erforderlichen Berechtigungen hinzuzufü gen. Sie benötigen Berechtigungen, um Rollen zu ändern und Richtlinien zu erstellen.

> **Note**
>
> - AWS Clean Rooms erfordert Berechtigungen für Abfragen gemäß den Analyseregeln. Weitere Informationen zu Berechtigungen für AWS Clean Rooms finden Sie unterAWS verwaltete Richtlinien für AWS Clean Rooms.
> - Wenn die Rolle nicht über ausreichende Berechtigungen für verfügt AWS Clean Rooms, erhalten Sie eine Fehlermeldung, dass die Rolle nicht über ausreichende Berechtigungen für verfügt AWS Clean Rooms. Die Rollenrichtlinie muss hinzugefügt werden, bevor Sie fortfahren können.
> - Wenn Sie die Rollenrichtlinie nicht ändern können, erhalten Sie eine Fehlermeldung, dass die Richtlinie für die Servicerolle nicht gefunden werden AWS Clean Rooms konnte.

9. Wenn Sie Tags für die konfigurierte Tabellenzuordnungsressource aktivieren möchten, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.
10. Wählen Sie Tabelle zuordnen aus.

Ordnen Sie eine konfigurierte Tabelle auf der Kollaborationsdetailseite zu

Um der Kollaboration AWS Glue Tabellen von der Kollaborationsdetailseite aus zuzuordnen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Wählen Sie auf der Registerkarte Tabellen die Option Tabelle zuordnen aus.
5. Gehen Sie unter Konfigurierte Tabelle auswählen wie folgt vor:

Wenn Sie …	Dann...
Wählen Sie eine bestehende konfigurierte Tabelle	Wählen Sie aus der Dropdownliste den Namen der konfigurierten Tabelle aus, die Sie der Kollaboration zuordnen möchten.
Konfigurieren Sie eine neue Tabelle	Wählen Sie Tabelle konfigurieren und folgen Sie den Anweisungen auf der Seite Tabelle konfigurieren.
Zeigen Sie das Schema und die Analysere gel für die konfigurierte Tabelle an	Aktivieren Sie die Option Schema und Analyseregel anzeigen.

6. Einzelheiten zur Tabellenverknüpfung finden Sie unter

   a. Geben Sie einen Namen für die zugehörige Tabelle ein.

      Sie können den Standardnamen verwenden oder diese Tabelle umbenennen.

   b. (Optional) Geben Sie eine Beschreibung der Tabelle ein.

      Die Beschreibung hilft beim Schreiben von Abfragen.

7. Geben Sie die Dienstzugriffsberechtigungen an, indem Sie entweder Neue Servicerolle erstellen und verwenden oder Bestehende Servicerolle verwenden auswählen.

Wenn Sie folgendes auswählen …	Dann...
Erstellen und verwenden Sie eine neue Servicerolle	• AWS Clean Rooms erstellt eine Servicero lle mit der erforderlichen Richtlinie für diese Tabelle. • Der Standardname der Servicerolle lautetcleanrooms-<timestamp> . • Sie müssen über die erforderlichen Berechtigungen verfügen, um Rollen zu erstellen und Richtlinien anzuhängen. • Wenn Ihre Eingabedaten verschlüsselt sind, können Sie Diese Daten sind mit

Wenn Sie folgendes auswählen …	Dann...
	einem KMS-Schlüssel verschlüsselt auswählen und dann einen eingeben AWS KMS key , der zur Entschlüsselung Ihrer Dateneingabe verwendet wird.
Verwenden Sie eine vorhandene Servicerolle	1. Wählen Sie einen vorhandenen Servicero llennamen aus der Dropdownliste aus. Die Liste der Rollen wird angezeigt, wenn Sie berechtigt sind, Rollen aufzulisten. Wenn Sie nicht berechtigt sind, Rollen aufzulisten, können Sie den Amazon-Ressourcennamen (ARN) der Rolle eingeben, die Sie verwenden möchten. 2. Rufen Sie die Servicerolle auf, indem Sie auf den externen Link In IAM anzeigen klicken. Wenn keine vorhandenen Servicero llen vorhanden sind, ist die Option „Eine bestehende Servicerolle verwenden“ nicht verfügbar. Versucht standardmäßig AWS Clean Rooms nicht, die bestehende Rollenric htlinie zu aktualisieren, um die erforderl ichen Berechtigungen hinzuzufügen. 3. (Optional) Aktivieren Sie das Kontrollk ästchen Eine vorkonfigurierte Richtlinie mit den erforderlichen Berechtigungen zu dieser Rolle hinzufügen, um der Rolle die erforderlichen Berechtigungen hinzuzufü gen. Sie benötigen Berechtigungen, um Rollen zu ändern und Richtlinien zu erstellen.

> **Note**
>
> - AWS Clean Rooms erfordert Berechtigungen für Abfragen gemäß den Analyseregeln. Weitere Informationen zu Berechtigungen für AWS Clean Rooms finden Sie unterAWS verwaltete Richtlinien für AWS Clean Rooms.
> - Wenn die Rolle nicht über ausreichende Berechtigungen für verfügt AWS Clean Rooms, erhalten Sie eine Fehlermeldung, dass die Rolle nicht über ausreichende Berechtigungen für verfügt AWS Clean Rooms. Die Rollenrichtlinie muss hinzugefügt werden, bevor Sie fortfahren können.
> - Wenn Sie die Rollenrichtlinie nicht ändern können, erhalten Sie eine Fehlermeldung, dass die Richtlinie für die Servicerolle nicht gefunden werden AWS Clean Rooms konnte.

8. Wenn Sie Tags für die konfigurierte Tabellenzuordnungsressource aktivieren möchten, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.
9. Wählen Sie Tabelle zuordnen aus.

Nächste Schritte

Nachdem Sie Ihre konfigurierte Datentabelle der Kollaboration zugeordnet haben, können Sie:

- Bearbeiten Sie die Kollaboration, wenn Sie der Kollaborationsersteller sind
- Fragen Sie die Datentabellen ab (als Mitglied, das Abfragen durchführen kann)

Konfiguration der differenzierten Datenschutzrichtlinie

In diesem Verfahren wird beschrieben, wie die differenzielle Datenschutzrichtlinie in einer Kollaboration mithilfe der Option Guided Flow in der AWS Clean Rooms Konsole konfiguriert wird. Dies ist ein einmaliger Schritt für alle Tabellen mit differenziellem Datenschutz.

So konfigurieren Sie differenzielle Datenschutzeinstellungen (geführter Ablauf)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Wählen Sie auf der Kollaborationsseite auf der Registerkarte Tabellen die Option Differenzielle Datenschutzrichtlinie konfigurieren aus.
5. Wählen Sie auf der Seite Differentielle Datenschutzrichtlinie konfigurieren Werte für die folgenden Eigenschaften aus:

   - Budget für den Datenschutz
   - Aktualisieren Sie das Datenschutzbudget monatlich
   - Pro Abfrage wurde ein Rauschen hinzugefügt

   Sie können die Standardwerte verwenden oder benutzerdefinierte Werte eingeben, die Ihren speziellen Anwendungsfall unterstützen. Nachdem Sie die Werte für das Datenschutzbudget und die pro Abfrage hinzugefügten Störungen ausgewählt haben, können Sie eine Vorschau des resultierenden Dienstprogramms im Hinblick auf die Anzahl der Aggregationen anzeigen, die für alle Abfragen Ihrer Daten möglich sind.
6. Wählen Sie Konfigurieren aus.

Es wird eine Bestätigungsnachricht angezeigt, dass Sie die differenzielle Datenschutzrichtlinie für die Zusammenarbeit erfolgreich konfiguriert haben.

Nächste Schritte

Nachdem Sie den differenziellen Datenschutz konfiguriert haben, können Sie:

- Fragen Sie die Datentabellen ab (als Mitglied, das Abfragen durchführen kann)
- Die Kollaboration verwalten (wenn Sie der Kollaborationsersteller sind)

Mit Analysevorlagen arbeiten

Analysevorlagen funktionieren mit demBenutzerdefinierte Analyseregel in AWS Clean Rooms. Mit einer Analysevorlage können Sie Parameter definieren, die Ihnen helfen, dieselbe Abfrage wiederzuverwenden. AWS Clean Rooms unterstützt eine Teilmenge der Parametrisierung mit Literalwerten.

Analysevorlagen sind kollaborationsspezifisch. Für jede Kollaboration können Mitglieder nur die Abfragen in dieser Kollaboration sehen. Wenn Sie beabsichtigen, Differential Privacy in einer Kollaboration zu verwenden, sollten Sie sicherstellen, dass Ihre Analysevorlagen mit der allgemeinen Abfragestruktur von AWS Clean Rooms Differential Privacy kompatibel sind.

Themen

Eine Analysevorlage erstellen

Informationen zum Erstellen einer Analysevorlage mithilfe der AWS SDKs finden Sie in der AWS Clean Rooms API-Referenz.

So erstellen Sie eine Analysevorlage mithilfe der Konsole AWS Clean Rooms

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit der AWS-Konto , die als Ersteller der Kollaboration fungiert.
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Gehen Sie auf der Registerkarte Vorlagen zum Abschnitt Von Ihnen erstellte Analysevorlagen.
5. Wählen Sie Analysevorlage erstellen aus.
6. Geben Sie auf der Seite Analysevorlage erstellen unter Details einen Namen und optional eine Beschreibung ein.
7. Sehen Sie sich unter Tabellen die konfigurierten Tabellen an, die der Kollaboration zugeordnet sind.
8. Zur Definition

a. Geben Sie die Definition für die Analysevorlage ein.

b. Wählen Sie Import aus, um eine Definition zu importieren.

c. (Optional) Geben Sie einen Parameter im SQL Editor an, indem Sie vor dem Parameternamen einen Doppelpunkt (`:`) eingeben.

   Beispielsweise:

   ```
   WHERE table1.date + :date_period > table1.date
   ```

9. Wenn Sie zuvor Parameter hinzugefügt haben, wählen Sie unter Parameter — optional für jeden Parameternamen den Typ und den Standardwert (optional) aus.
10. Wenn Sie Tags für die konfigurierte Tabellenressource aktivieren möchten, wählen Sie Neues Tag hinzufügen aus und geben Sie dann das Schlüssel - und Wertepaar ein.
11. Wählen Sie Erstellen.

Sie sind jetzt bereit für:

- Teilen Sie Ihrem Kollaborationsmitglied mit, dass es eine Analysevorlage überprüfen kann. (Optional, wenn Sie Ihre eigenen Daten abfragen möchten.)

Überprüfen einer Analysevorlage

Nachdem ein Mitglied der Kollaboration eine Analysevorlage erstellt hat, können Sie diese überprüfen und genehmigen. Nachdem die Analysevorlage genehmigt wurde, kann sie in einer Abfrage eingegeben AWS Clean Rooms werden.

Um eine Analysevorlage mithilfe der AWS Clean Rooms Konsole zu überprüfen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit der AWS-Konto , die als Ersteller der Kollaboration fungiert.
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Gehen Sie auf der Registerkarte Vorlagen zum Abschnitt Analysevorlagen, die von anderen Mitgliedern erstellt wurden.
5. Wählen Sie die Analysevorlage mit dem Status Kann ausgeführt werden auf Nein, Ihre Überprüfung ist erforderlich.

6. Wählen Sie Überprüfen aus.
7. Überprüfen Sie die Übersicht, die Definition und die Parameter der Analyseregel (falls vorhanden).
8. Überprüfen Sie die konfigurierten Tabellen, die unter In der Definition referenzierte Tabellen aufgeführt sind.

   Der Status neben jeder Tabelle lautet Vorlage nicht zulässig.
9. Wählen Sie eine -Tabelle aus.

Wenn Sie	Wählen Sie dann
Genehmigen Sie die Analysevorlage	Vorlage auf dem Tisch. Bestätigen Sie Ihre Zustimmung, indem Sie wählen.
Genehmigen Sie die Analysevorlage nicht	Nicht zulassen

Sie können nun die Analysevorlage verwenden, um die Datentabellen abzufragen (als Mitglied, das Abfragen durchführen kann).

Abfragen konfigurierter Tabellen mithilfe einer Analysevorlage

Dieses Verfahren zeigt, wie Sie eine Analysevorlage in der AWS Clean Rooms Konsole verwenden, um konfigurierte Tabellen mit der benutzerdefinierten Analyseregel abzufragen.

So verwenden Sie eine Analysevorlage, um konfigurierte Tabellen mit der benutzerdefinierten Analyseregel abzufragen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, deren Status „Ihre Mitgliederfähigkeiten“ auf „Anfrage“ gesetzt ist.
4. Sehen Sie sich auf der Registerkarte Abfragen unter Tabellen die Tabellen und den zugehörigen Analyseregeltyp an (benutzerdefinierte Analyseregel).

> **Note**
>
> Wenn Sie die erwarteten Tabellen in der Liste nicht sehen, kann das folgende Gründe haben:
>
> - Die Tabellen wurden nicht verknüpft.
> - Für die Tabellen ist keine Analyseregel konfiguriert.

5. Wählen Sie im Abschnitt Analyse die Analysevorlage aus der Dropdownliste aus.
6. Geben Sie den Wert der Parameter aus der Analysevorlage ein, die Sie in der Abfrage verwenden möchten. Der Wert muss dem angegebenen Datentyp des Parameters entsprechen. Sie können bei jeder Ausführung der Analysevorlage unterschiedliche Werte verwenden. Leer oder NULL Werte für den Parameter werden nicht unterstützt. Die Verwendung von Parametern in einer LIMIT Klausel wird ebenfalls nicht unterstützt.
7. Wählen Sie Ausführen aus.

> **Note**
>
> Sie können die Abfrage nicht ausführen, wenn das Mitglied, das Ergebnisse empfangen kann, die Einstellungen für die Abfrageergebnisse nicht konfiguriert hat.

8. Passen Sie die Parameter weiter an und führen Sie Ihre Abfrage erneut aus, oder klicken Sie auf die Schaltfläche +, um eine neue Abfrage auf einer neuen Registerkarte zu starten.

Daten in einer Zusammenarbeit abfragen

Als Mitglied, das Abfragen durchführen kann, können Sie einen der folgenden Schritte ausführen:

- Erstellen Sie eine SQL-Abfrage manuell mit dem SQL-Code-Editor.
- Verwenden Sie die Analysis Builder-Benutzeroberfläche, um eine Abfrage zu erstellen, ohne SQL-Code schreiben zu müssen.
- Verwenden Sie eine genehmigte Analysevorlage.

Wenn das Mitglied, das Abfragen durchführen kann, eine SQL-Abfrage für die Tabellen in der Kollaboration ausführt, AWS Clean Rooms übernimmt es die entsprechenden Rollen, um in seinem Namen auf die Tabellen zuzugreifen. AWS Clean Rooms wendet die Analyseregeln nach Bedarf auf die Eingabeabfrage und ihre Ausgabe an.

AWS Clean Rooms unterstützt SQL-Abfragen, die sich von anderen Abfrage-Engines unterscheiden können. Spezifikationen finden Sie in der AWS Clean Rooms SQL-Referenz. Wenn Sie Abfragen für Datentabellen ausführen möchten, die mit Differential Privacy geschützt sind, sollten Sie sicherstellen, dass Ihre Abfragen mit der allgemeinen Abfragestruktur von AWS Clean Rooms Differential Privacy kompatibel sind.

> **Note**
>
> Wenn Sie Cryptographic Computing für verwendenClean Rooms, generieren nicht alle SQL-Operationen gültige Ergebnisse. Sie können beispielsweise COUNT auf eine verschlüsselte Spalte zugreifen, aber die Ausführung SUM auf verschlüsselte Zahlen führt zu Fehlern. Darüber hinaus können Abfragen auch zu falschen Ergebnissen führen. Beispielsweise führen Abfragen, bei denen Spalten SUM versiegelt wurden, zu Fehlern. Eine GROUP BY Abfrage über versiegelte Spalten scheint jedoch erfolgreich zu sein, erzeugt aber andere Gruppen als die, die bei einer GROUP BY Abfrage über den Klartext erzeugt werden.

In den folgenden Themen wird erklärt, wie Daten in einer Kollaboration mithilfe der AWS Clean Rooms Konsole abgefragt werden.

Themen

- Verwenden des SQL-Code-Editors

- Verwenden Sie den Analysis Builder
- Abfragen von Daten mit differenziertem Datenschutz
- Anzeige kürzlicher Abfragen
- Anzeigen von Abfragedetails

Informationen dazu, wie Sie Daten abfragen oder Abfragen anzeigen, indem Sie den AWS Clean Rooms `StartProtectedQuery` API-Vorgang direkt aufrufen oder die AWS SDKs verwenden, finden Sie in der AWS Clean Rooms API-Referenz.

Hinweise zur Abfrageprotokollierung finden Sie unterAnmeldung abfragen AWS Clean Rooms.

> **Note**
>
> Wenn Sie eine Abfrage für verschlüsselte Datentabellen ausführen, werden die Ergebnisse der verschlüsselten Spalten verschlüsselt.

Hinweise zum Empfangen von Abfrageergebnissen finden Sie unterAbfrageergebnisse anzeigen.

Verwenden des SQL-Code-Editors

Als Mitglied, das Abfragen durchführen kann, können Sie eine Abfrage manuell erstellen, indem Sie SQL-Code in den SQL-Code-Editor schreiben. Der SQL-Code-Editor befindet sich in der AWS Clean Rooms Konsole auf der Registerkarte Abfragen im Abschnitt Analyse.

Der SQL-Code-Editor wird standardmäßig angezeigt. Wenn Sie den Analysis Builder zum Erstellen von Abfragen verwenden möchten, finden Sie weitere Informationen unterVerwenden Sie den Analysis Builder.

> **Important**
>
> Wenn Sie mit dem Schreiben einer SQL-Abfrage im Code-Editor beginnen und dann die Analysis Builder-Benutzeroberfläche einschalten, wird Ihre Abfrage nicht gespeichert.

AWS Clean Rooms unterstützt viele SQL-Befehle, Funktionen und Bedingungen. Weitere Informationen finden Sie in der AWS Clean Rooms SQL-Referenz.

> **Tip**
>
> Wenn während der Ausführung einer Abfrage eine geplante Wartung stattfindet, wird die Abfrage beendet und ein Rollback durchgeführt. Sie müssen die Abfrage neu starten.

Um die Abfrage manuell mit dem SQL-Code-Editor zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, deren Status „Ihre Mitgliederfähigkeiten“ auf „Anfrage“ gesetzt ist.
4. Gehen Sie auf der Registerkarte Abfragen zum Abschnitt Analyse.

   > **Note**
   >
   > Im Abschnitt Analyse wird nur angezeigt, ob das Mitglied, das Ergebnisse erhalten kann, und das Mitglied, das für die Bezahlung der Abfrage-Rechenkosten verantwortlich ist, der Kollaboration als aktives Mitglied beigetreten sind.

5. Sehen Sie sich auf der Registerkarte Abfragen unter Tabellen die Liste der Tabellen und den zugehörigen Analyseregeltyp an (Aggregationsanalyseregel, Listenanalyseregel oder Benutzerdefinierte Analyseregel).

   > **Note**
   >
   > Wenn Sie die erwarteten Tabellen in der Liste nicht sehen, kann das folgende Gründe haben:
   >
   > - Die Tabellen wurden nicht verknüpft.
   > - Für die Tabellen ist keine Analyseregel konfiguriert.

6. (Optional) Um das Schema und die Analyseregelsteuerelemente der Tabelle anzuzeigen, erweitern Sie die Tabelle, indem Sie das Pluszeichen (+) auswählen.
7. Erstellen Sie die Abfrage, indem Sie die Abfrage in den SQL-Code-Editor eingeben.

(Optional) Wenn Sie eine Beispielabfrage verwenden möchten	(Optional) Wenn Sie Spaltennamen oder Funktionen einfügen möchten
1. Wählen Sie die drei vertikalen Punkte neben der Tabelle aus. 2. Wählen Sie unter In Editor einfügen die Option Beispielabfrage aus. **Note** Beim Einfügen einer Beispielabfrage wird die Abfrage angehängt, die sich bereits im Editor befindet. Das Abfragebeispiel wird angezeigt. Alle unter Tabellen aufgeführten Tabellen sind in der Abfrage enthalten. 3. Bearbeiten Sie die Platzhalterwerte in der Abfrage.	1. Wählen Sie die drei vertikalen Punkte neben einer Spalte aus. 2. Wählen Sie unter In Editor einfügen die Option Spaltenname aus. 3. Um eine Funktion, die für eine Spalte zulässig ist, manuell einzufügen, wählen Sie die drei vertikalen Punkte neben einer Spalte aus, wählen Sie In Editor einfügen und wählen dann den Namen der zulässigen Funktion aus (z. B. INNER JOIN SUMDISTINCT, SUM oderCOUNT). 4. Drücken Sie Strg + Leertaste, um die Tabellenschemas im Code-Editor anzuzeigen. **Note** Mitglieder, die Abfragen durchführen können, können die Partitionsspalten in jeder konfigurierten Tabellenverknüpfung anzeigen und verwenden. Stellen Sie sicher, dass die Partitionsspalte in der AWS Glue Tabelle, die der konfigurierten Tabelle zugrunde

(Optional) Wenn Sie eine Beispielabfrage verwenden möchten	(Optional) Wenn Sie Spaltennamen oder Funktionen einfügen möchten
	liegt, als Partitionsspalte gekennzeichnet ist. 5. Bearbeiten Sie die Platzhalterwerte in der Abfrage.

8. Wählen Sie Ausführen aus.

> **Note**
>
> Sie können die Abfrage nicht ausführen, wenn das Mitglied, das Ergebnisse empfangen kann, die Einstellungen für die Abfrageergebnisse nicht konfiguriert hat.

9. Passen Sie die Parameter weiter an und führen Sie Ihre Abfrage erneut aus, oder klicken Sie auf die Schaltfläche +, um eine neue Abfrage auf einer neuen Registerkarte zu starten.

> **Note**
>
> AWS Clean Rooms zielt darauf ab, klare Fehlermeldungen bereitzustellen. Wenn eine Fehlermeldung nicht genügend Details enthält, um Ihnen bei der Fehlerbehebung zu helfen, wenden Sie sich an das Account-Team. Geben Sie ihnen eine Beschreibung, wie der Fehler aufgetreten ist, und geben Sie ihnen die Fehlermeldung (einschließlich aller Identifikatoren). Weitere Informationen finden Sie unter Problembehebung AWS Clean Rooms.

Verwenden Sie den Analysis Builder

Sie können den Analysis Builder verwenden, um Abfragen zu erstellen, ohne SQL-Code schreiben zu müssen. Mit dem Analysis Builder können Sie eine Abfrage für eine Kollaboration erstellen, die Folgendes bietet:

- Eine einzelne Tabelle, die die Aggregationsanalyseregel verwendet, ohne dass JOIN erforderlich ist
- Zwei Tabellen (eine von jedem Mitglied), die beide die Aggregationsanalyseregel verwenden

- Zwei Tabellen (eine für jedes Mitglied), die beide die Listenanalyseregel verwenden
- Zwei Tabellen (eine für jedes Mitglied), die beide die Aggregationsanalyseregel verwenden, und zwei Tabellen (eine für jedes Mitglied), die beide die Listenanalyseregel verwenden

Informationen zum manuellen Schreiben von SQL-Abfragen finden Sie unterVerwenden des SQL-Code-Editors.

Der Analysis Builder wird als Benutzeroberflächenoption für Analysis Builder im Abschnitt Analyse der Registerkarte Abfragen in der AWS Clean Rooms Konsole angezeigt.

> **Important**
>
> Wenn Sie die Analysis Builder-Benutzeroberfläche aktivieren, mit der Erstellung einer Abfrage im Analysis Builder beginnen und dann die Analysis Builder-Benutzeroberfläche ausschalten, wird Ihre Abfrage nicht gespeichert.

> **Tip**
>
> Wenn während der Ausführung einer Abfrage eine geplante Wartung stattfindet, wird die Abfrage beendet und ein Rollback durchgeführt. Sie müssen die Abfrage neu starten.

In den folgenden Themen wird die Verwendung des Analysis Builder erläutert.

Themen

- Verwenden Sie den Analysis Builder, um eine einzelne Tabelle abzufragen (Aggregation)
- Verwenden Sie den Analysis Builder, um zwei Tabellen (Aggregation oder Liste) abzufragen

Verwenden Sie den Analysis Builder, um eine einzelne Tabelle abzufragen (Aggregation)

Dieses Verfahren zeigt, wie Sie die Analysis Builder-Benutzeroberfläche in der AWS Clean Rooms Konsole verwenden, um eine Abfrage zu erstellen. Die Abfrage bezieht sich auf eine Kollaboration mit einer einzelnen Tabelle, die die Aggregationsanalyseregel verwendet, ohne dass JOIN dies erforderlich ist.

Um den Analysis Builder für die Abfrage einer einzelnen Tabelle zu verwenden

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, deren Status „Ihre Mitgliederfähigkeiten“ auf „Anfrage“ gesetzt ist.
4. Sehen Sie sich auf der Registerkarte Abfragen unter Tabellen die Tabelle und den zugehörigen Analyseregeltyp an. (Der Analyseregeltyp sollte die Aggregationsanalyseregel sein.)

   > **Note**
   >
   > Wenn Sie die erwartete Tabelle nicht sehen, kann das folgende Gründe haben:
   >
   > - Die Tabelle wurde nicht verknüpft.
   > - Für die Tabelle ist keine Analyseregel konfiguriert.

5. Aktivieren Sie im Abschnitt Analyse die Benutzeroberfläche von Analysis Builder.
6. Erstellen Sie eine Abfrage.

   Wenn Sie alle Aggregationsmetriken sehen möchten, fahren Sie mit Schritt 9 fort.

   a. Überprüfen Sie unter Metriken auswählen die aggregierten Metriken, die standardmäßig vorausgewählt wurden, und entfernen Sie bei Bedarf alle Metriken.

   b. (Optional) Wählen Sie unter Segmente hinzufügen — optional einen oder mehrere Parameter aus.

      > **Note**
      >
      > Segmente hinzufügen — optional wird nur angezeigt, wenn Dimensionen für die Tabelle angegeben sind.

   c. (Optional) Wählen Sie unter Filter hinzufügen — optional die Option Filter hinzufügen und wählen Sie dann einen Parameter, einen Operator und einen Wert aus.

      Um weitere Filter hinzuzufügen, wählen Sie „Weiteren Filter hinzufügen“.

      Um einen Filter zu entfernen, wählen Sie Entfernen.

> **Note**
>
> ORDER BYwird für Aggregationsabfragen nicht unterstützt.
> In Filtern wird nur der AND Operator unterstützt.

d. (Optional) Geben Sie unter Beschreibung hinzufügen — optional eine Beschreibung ein, um die Abfrage in der Abfrageliste leichter identifizieren zu können.

7. Erweitern Sie Vorschau-SQL-Code.

   a. Zeigen Sie den SQL-Code an, der vom Analysis Builder generiert wurde.

   b. Um den SQL-Code zu kopieren, wählen Sie Kopieren.

   c. Um den SQL-Code zu bearbeiten, wählen Sie Im SQL-Code-Editor bearbeiten.

8. Wählen Sie Ausführen aus.

> **Note**
>
> Sie können die Abfrage nicht ausführen, wenn das Mitglied, das Ergebnisse empfangen kann, die Einstellungen für die Abfrageergebnisse nicht konfiguriert hat.

9. Passen Sie die Parameter weiter an und führen Sie Ihre Abfrage erneut aus, oder klicken Sie auf die Schaltfläche +, um eine neue Abfrage auf einer neuen Registerkarte zu starten.

> **Note**
>
> AWS Clean Rooms zielt darauf ab, klare Fehlermeldungen bereitzustellen. Wenn eine Fehlermeldung nicht genügend Details enthält, um Ihnen bei der Fehlerbehebung zu helfen, wenden Sie sich an das Account-Team. Geben Sie ihnen eine Beschreibung, wie der Fehler aufgetreten ist, und geben Sie ihnen die Fehlermeldung (einschließlich aller Identifikatoren). Weitere Informationen finden Sie unter Problembehebung AWS Clean Rooms.

Verwenden Sie den Analysis Builder, um zwei Tabellen (Aggregation oder Liste) abzufragen

In diesem Verfahren wird beschrieben, wie Sie den Analysis Builder in der AWS Clean Rooms Konsole verwenden, um eine Abfrage für eine Kollaboration zu erstellen, die über Folgendes verfügt:

- Zwei Tabellen (eine für jedes Mitglied), die beide die Aggregationsanalyseregel verwenden
- Zwei Tabellen (eine für jedes Mitglied), die beide die Listenanalyseregel verwenden
- Zwei Tabellen (eine für jedes Mitglied), die beide die Aggregationsanalyseregel verwenden, und zwei Tabellen (eine für jedes Mitglied), die beide die Listenanalyseregel verwenden

So verwenden Sie den Analysis Builder, um zwei Tabellen abzufragen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, deren Status „Ihre Mitgliederfähigkeiten“ auf „Anfrage“ gesetzt ist.
4. Sehen Sie sich auf der Registerkarte Abfragen unter Tabellen die beiden Tabellen und den zugehörigen Analyseregeltyp an (Aggregationsanalyseregel oder Listenanalyseregel).

   > **Note**
   >
   > Wenn Sie die erwarteten Tabellen nicht in der Liste sehen, kann das folgende Gründe haben:
   >
   > - Die Tabellen wurden nicht verknüpft.
   > - Für die Tabellen ist keine Analyseregel konfiguriert.

5. Aktivieren Sie im Abschnitt Analyse die Benutzeroberfläche von Analysis Builder.
6. Erstellen Sie eine Abfrage.

   Wenn die Kollaboration zwei Tabellen enthält, die die Aggregationsanalyseregel verwenden, und zwei Tabellen, die die Analyseregel „Liste“ verwenden, wählen Sie zuerst Aggregation oder Liste aus, und folgen Sie dann den Anweisungen, die auf der ausgewählten Analyseregel basieren.

Wenn die beiden Tabellen die Aggregationsanalyseregel verwenden	Wenn die beiden Tabellen die Listenanalyseregel verwenden
1. Überprüfen Sie unter Metriken auswählen die aggregierten	1. Überprüfen Sie unter Attribute auswählen die Listenattribute,

Wenn die beiden Tabellen die Aggregationsanalyseregel verwenden	Wenn die beiden Tabellen die Listenanalyseregel verwenden
Metriken, die standardmäßig vorausgewählt wurden, und entfernen Sie bei Bedarf alle Metriken. 2. Wählen Sie für Datensätze zuordnen einen oder mehrere Datensätze aus. **Note** Wenn Sie den Analysegenerator verwenden, können Sie nur für ein einzelnes Spaltenpaar einen Abgleich durchführen. 3. (Optional) Wählen Sie unter Segmente hinzufügen — optional einen oder mehrere Parameter aus. **Note** Segmente hinzufügen — optional wird nur angezeigt, wenn Dimensionen für die Tabelle angegeben sind. 4. (Optional) Wählen Sie unter Filter hinzufügen — optional	die standardmäßig vorausgewählt wurden, und entfernen Sie bei Bedarf alle Metriken. 2. Wählen Sie für Datensätze zuordnen einen oder mehrere Datensätze aus. **Note** Wenn Sie den Analysegenerator verwenden, können Sie nur für ein einzelnes Spaltenpaar einen Abgleich durchführen. 3. (Optional) Wählen Sie unter Filter hinzufügen — optional die Option Filter hinzufügen und wählen Sie dann einen Parameter, einen Operator und einen Wert aus. Um weitere Filter hinzuzufügen, wählen Sie Weiteren Filter hinzufügen aus. Um einen Filter zu entfernen, wählen Sie Entfernen.

Wenn die beiden Tabellen die Aggregationsanalyseregel verwenden	Wenn die beiden Tabellen die Listenanalyseregel verwenden
die Option Filter hinzufügen und wählen Sie dann einen Parameter, einen Operator und einen Wert aus. Um weitere Filter hinzuzufügen, wählen Sie Weiteren Filter hinzufügen aus. Um einen Filter zu entfernen, wählen Sie Entfernen. **Note** ORDER BYwird für Aggregationsabfragen nicht unterstützt. In Filtern wird nur der AND Operator unterstützt. 5. (Optional) Geben Sie unter Beschreibung hinzufügen — optional eine Beschreibung ein, um die Abfrage in der Liste der letzten Abfragen leichter identifizieren zu können.	**Note** LIMITwird für Listenabfragen nicht unterstützt. In Filtern wird nur der AND Operator unterstützt. 4. (Optional) Geben Sie unter Beschreibung hinzufügen — optional eine Beschreibung ein, um die Abfrage in der Liste der letzten Abfragen leichter identifizieren zu können.

7. Erweitern Sie Vorschau-SQL-Code.
   a. Zeigen Sie den SQL-Code an, der vom Analysis Builder generiert wurde.
   b. Um den SQL-Code zu kopieren, wählen Sie Kopieren.
   c. Um den SQL-Code zu bearbeiten, wählen Sie Im SQL-Code-Editor bearbeiten.
8. Wählen Sie Ausführen aus.

> **Note**
>
> Sie können die Abfrage nicht ausführen, wenn das Mitglied, das Ergebnisse empfangen kann, die Einstellungen für die Abfrageergebnisse nicht konfiguriert hat

9. Passen Sie die Parameter weiter an und führen Sie Ihre Abfrage erneut aus, oder klicken Sie auf die Schaltfläche +, um eine neue Abfrage auf einer neuen Registerkarte zu starten.

> **Note**
>
> AWS Clean Rooms zielt darauf ab, klare Fehlermeldungen bereitzustellen. Wenn eine Fehlermeldung nicht genügend Details enthält, um Ihnen bei der Fehlerbehebung zu helfen, wenden Sie sich an das Account-Team. Geben Sie ihnen eine Beschreibung, wie der Fehler aufgetreten ist, und geben Sie ihnen die Fehlermeldung (einschließlich aller Identifikatoren). Weitere Informationen finden Sie unter Problembehebung AWS Clean Rooms.

Abfragen von Daten mit differenziertem Datenschutz

Im Allgemeinen ändert sich das Schreiben und Ausführen von Abfragen nicht, wenn Differential Privacy aktiviert ist. Sie können jedoch keine Abfrage ausführen, wenn nicht genügend Datenschutzbudget übrig ist. Wenn Sie Abfragen ausführen und das Datenschutzbudget verbrauchen, können Sie ungefähr sehen, wie viele Aggregationen Sie ausführen können und wie sich dies auf future Abfragen auswirken könnte.

Um die Auswirkungen des unterschiedlichen Datenschutzes in einer Zusammenarbeit zu untersuchen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, deren Status Ihre Mitgliedsdetails auf Abfragen ausführen lautet.
4. Sehen Sie sich auf der Registerkarte Abfragen unter Tabellen das verbleibende Datenschutzbudget an. Dies wird als geschätzte Anzahl der verbleibenden Aggregationsfunktionen und des verwendeten Dienstprogramms (in Prozent) angezeigt.

> **Note**
>
> Die geschätzte Anzahl der verbleibenden Aggregatfunktionen und der Prozentsatz des verwendeten Dienstprogramms werden nur für das Mitglied angezeigt, das Abfragen durchführen kann.

5. Wählen Sie „Auswirkung anzeigen“, um zu sehen, wie viel Rauschen in die Ergebnisse eingedrungen ist und wie viele Aggregationsfunktionen Sie ungefähr ausführen können.

Anzeige kürzlicher Abfragen

Auf der Registerkarte Aktuelle Abfragen können Sie sich die Abfragen ansehen, die in den letzten 90 Tagen ausgeführt wurden.

> **Note**
>
> Wenn Sie als Mitglied nur Contribute-Daten haben und Sie nicht das Mitglied sind, das für die Berechnung von Abfragen bezahlt, wird die Registerkarte Abfragen nicht in der Konsole angezeigt.

Um aktuelle Abfragen zu sehen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie eine Zusammenarbeit aus.
4. Sehen Sie sich auf der Registerkarte Abfragen unter Abfragen die Abfragen an, die in den letzten 90 Tagen ausgeführt wurden.
5. Um die letzten Abfragen nach Status zu sortieren, wählen Sie einen Status aus der Dropdownliste Alle Status aus.

   Die Status lauten: Eingereicht, Gestartet, Storniert, Erfolgreich, Fehlgeschlagen und Zeitlimit überschritten.

Anzeigen von Abfragedetails

Sie können die Abfragedetails als Mitglied anzeigen, das Abfragen ausführen kann, oder als Mitglied, das Ergebnisse erhalten kann.

Um die Details der Abfrage anzuzeigen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie eine Zusammenarbeit aus.
4. Führen Sie auf der Registerkarte Abfragen einen der folgenden Schritte aus:
   - Wählen Sie das Optionsfeld für die spezifische Abfrage, die Sie anzeigen möchten, und klicken Sie dann auf Details anzeigen.
   - Wählen Sie die ID der geschützten Abfrage aus.
5. Auf der Seite mit den Abfragedetails
   - Wenn Sie das Mitglied sind, das Abfragen ausführen kann, sehen Sie sich die Abfragedetails, den SQL-Text und die Ergebnisse an.

     Es wird eine Meldung angezeigt, die bestätigt, dass die Abfrageergebnisse an das Mitglied übermittelt wurden, das Ergebnisse empfangen kann.
   - Wenn Sie das Mitglied sind, das Ergebnisse erhalten kann, sehen Sie sich die Abfragedetails und Ergebnisse an.

Abfrageergebnisse anzeigen

AlsMitglied, das Ergebnisse erhalten kann, Sie können die Abfrageausgabe von erhaltenAWS Clean Roomsin den Amazon S3 S3-Bucket, den Sie beim Beitritt zur Zusammenarbeit angegeben haben.

In den folgenden Themen wird erklärt, wie Sie Abfrageergebnisse mit dem abrufenAWS Clean RoomsKonsole.

Themen

Informationen zum Abfragen von Daten oder zum Anzeigen von Abfragen finden Sie unterAWS Clean RoomsAPI direkt oder mithilfe derAWSSDKs, anzeigenAWS Clean RoomsAPI-Referenz.

Informationen zur Abfrageprotokollierung finden Sie unterAnmeldung abfragen AWS Clean Rooms.

> **Note**
>
> Wenn Sie eine Abfrage für verschlüsselte Datentabellen ausführen, werden die Ergebnisse der verschlüsselten Spalten verschlüsselt.

Abfrageergebnisse anzeigen

Die Ergebnisse der Abfrage befinden sich imStandardeinstellungen für AbfrageergebnisseAbschnitt und dieAbfragenAbschnitt derAbfragenRegisterkarte in derAWS Clean RoomsKonsole.

Um Abfrageergebnisse zu erhalten

1. Melden Sie sich beimAWS Management Consoleund öffne denAWS Clean RoomsKonsolemit deinemAWS-Konto(falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken NavigationsbereichKollaborationen.
3. Wählen Sie die Zusammenarbeit, dieIhre Fähigkeiten als MitgliedStatus vonErgebnisse erhalten.

4. Um die Abfrageergebnisse direkt zu erhalten vonAWS Clean Rooms, auf demAbfragenRegisterkarte, unterAbfragen, unter demGeschützte Abfrage-IDSpalte, wählen Sie die Abfrage aus.
5. Auf derEinzelheiten abfragenSeite, unterErgebnisse, führen Sie einen der folgenden Schritte aus:

Wenn du willst...	Dann wähle...
Kopieren Sie die Ergebnisse.	Copy
Laden Sie die Ergebnisse herunter.	Download **Note** Standardmäßig ist der Name der heruntergeladenen Datei der entsprechende `Query id` das wurde angezeigt, als die Abfrage ausgeführt wurdeAWS Clean Rooms.
Zeigen Sie die Ergebnisse in Amazon S3 anzeigen.	In Amazon S3 anzeigen Die Amazon S3 S3-Konsole wird in einem separaten Tab geöffnet.

6. Wenn Sie verschlüsselte Daten verwenden, können Sie jetztentschlüsselndie Datentabellen.

   Weitere Informationen finden Sie unter Datentabellen mit dem C3R-Verschlüsselungsclient entschlüsseln.

Bearbeiten Sie die Standardwerte für die Einstellungen für Abfrageergebnisse

Als Mitglied, das Ergebnisse empfangen kann, können Sie die Standardwerte für die Einstellungen für Abfrageergebnisse in derAWS Clean RoomsKonsole.

Um die Standardwerte für die Einstellungen für Abfrageergebnisse zu bearbeiten

1. Melden Sie sich beimAWS Management Consoleund öffne denAWS Clean RoomsKonsolemit deinemAWS-Konto(falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken NavigationsbereichKollaborationen.
3. Wählen Sie die Zusammenarbeit, dieIhre Fähigkeiten als MitgliedStatus vonErgebnisse erhalten.
4. Auf derAbfragenRegisterkarte, unterEinstellungen für Abfrageergebnisse, wählenBearbeiten.
5. Auf derStandardeinstellungen für Abfrageergebnisse bearbeitenSeite, ändern Sie nach Bedarf eine der folgenden Optionen:

   a. UnterEinstellungen für Abfrageergebnisse, modifiziere denZielort in Amazon S3-Ergebnissen in Amazon S3-oder dasFormat der Ergebnisse.

   b. UnterZugriff auf den Dienst, modifiziere denMethode zur AutorisierungAWS Clean Roomsum in den von Ihnen angegebenen Amazon-S3-Bucket und das Amazon S3-Bucket, den Sie angegeben haben.

   Das aktualisierteEinstellungen für Abfrageergebnisseerscheinen auf der Detailseite der Zusammenarbeit.

Verwenden der Abfrageausgabe in anderenAWS-Services

Ausgabe anzeigen vonAWS Clean Roomsist auf der Konsole verfügbar (wenn die Konsole zum Ausführen von Abfragen verwendet wird) und in einem angegebenen Amazon S3 S3-Bucket heruntergeladen. Von dort aus können Sie die Abfrageausgabe in anderen Programmen verwendenAWS-Services, wie Amazon QuickSight und Amazon SageMaker, je nachdem, wie diese Dienste Daten aus dem Amazon S3 verwenden.

Für weitere Informationen über Amazon QuickSight, siehe dieAmazon QuickSightDokumentation.

Für weitere Informationen über Amazon SageMaker, siehe dieAmazon SageMakerDokumentation.

Datentabellen mit dem C3R-Verschlüsselungsclient entschlüsseln

Folgen Sie diesem Verfahren für Kollaborationen, bei denen Cryptographic Computing fürClean Roomsund den C3R-Verschlüsselungsclient zum Verschlüsseln von Datentabellen. Verwenden Sie dieses Verfahren, nachdem SieDaten wurden in der Zusammenarbeit abgefragt.

Der gemeinsame geheime Schlüssel und die Kollaborations-ID sind für dieses Verfahren erforderlich.

Das Mitglied, das Ergebnisse erhalten kann, entschlüsselt die Daten mit demselben gemeinsamen geheimen Schlüssel und derselben Kollaborations-ID, die zur Verschlüsselung der Daten für die Kollaboration verwendet wurden.

> **Note**
>
> AWS Clean RoomsKollaborationen schränken bereits ein, wer Abfrageergebnisse ausführen und anzeigen kann. Um die Entschlüsselung durchzuführen, benötigt jeder, der Zugriff auf diese Ergebnisse hat, denselben gemeinsamen geheimen Schlüssel und dieselbe Kollaborations-ID, mit der die Daten verschlüsselt wurden.

Um eine verschlüsselte Datentabelle zu entschlüsseln

1. (Fakultativ)Sehen Sie sich die verfügbaren Befehle im C3R-Verschlüsselungsclient an.
2. (Optional) Navigieren Sie zum gewünschten Verzeichnis und führen Sie Folgendes aus`ls`(macOS) oder`dir`(Windows).

   - Vergewissern Sie sich, dassc3r-cli.jarDatei und Datendatei mit verschlüsselten Abfrageergebnissen befinden sich im gewünschten Verzeichnis.

     > **Note**
     >
     > Wenn Abfrageergebnisse von der heruntergeladen werdenAWS Clean RoomsKonsolenschnittstelle, sie befinden sich wahrscheinlich in derDownloadsOrdner für Ihr Benutzerkonto. (Zum Beispiel dieDownloadsOrdner in Ihrem Benutzerverzeichnis aufWindowsundmacOS.) Wir empfehlen, dass Sie die Datei mit den Abfrageergebnissen in denselben Ordner verschieben wiec3r-cli.jar.

3. Speichern Sie den gemeinsamen geheimen Schlüssel im`C3R_SHARED_SECRET`Umgebungsvariable. Weitere Informationen finden Sie unter Schritt 6: Speichern Sie den gemeinsamen geheimen Schlüssel in einer Umgebungsvariablen.
4. Von derAWS Command Line Interface(AWS CLI), führen Sie den folgenden Befehl aus.

   java -jar c3r-cli.jar decrypt ***<name of input .csv file>*** --id=***<collaboration id>*** --output=***<output file name>***
5. Ersetze jeden*`Platzhalter für Benutzereingaben`*mit Ihren eigenen Informationen:

   a. Für`id=`, geben Sie die Kollaborations-ID ein.

   b. Für`output=`, geben Sie den Optionsgruppennamen ein (z. B.`results-decrypted.csv`).

      Wenn Sie keinen Optionsnamen angeben, wird im Terminal ein Optionsname angezeigt.

   c. Zeigen Sie die entschlüsselten Daten in der angegebenen Ausgabedatei mit Ihrer bevorzugten CSV-Datei an oderParquetAnwendung anzeigen (z. B.Microsoft Excel, ein Texteditor oder eine andere Anwendung).

Verwaltung AWS Clean Rooms

In den folgenden Themen wird beschrieben, wie Sie eine Kollaboration, Mitglieder und konfigurierte Tabellen AWS Clean Rooms mithilfe der AWS Clean Rooms Konsole verwalten.

Informationen zur Verwaltung der AWS Clean Rooms Verwendung der AWS SDKs finden Sie in der AWS Clean Rooms API-Referenz.

Themen

- Verwaltung von Kollaborationen in AWS Clean Rooms
- Verwaltung konfigurierter Tabellen in AWS Clean Rooms

Verwaltung von Kollaborationen in AWS Clean Rooms

In den folgenden Themen wird beschrieben, wie der Kollaborationsersteller eine Kollaboration AWS Clean Rooms mithilfe der AWS Clean Rooms Konsole verwalten kann.

Informationen zur Verwaltung einer Kollaboration mithilfe der AWS SDKs finden Sie in der AWS Clean RoomsAPI-Referenz.

Themen

- Kollaborationen bearbeiten
- Kollaborationen löschen
- Kollaborationen anzeigen
- Tabellen und Analyseregeln anzeigen
- Differenzielle Nutzungsprotokolle für Datenschutz anzeigen
- Den Mitgliedsstatus überwachen
- Ein Mitglied aus einer Kollaboration entfernen
- Verlassen einer Kollaboration
- Konfigurierte Tabellenzuordnungen bearbeiten
- Aufheben der Zuordnung konfigurierter Tabellen
- Eine differenzielle Datenschutzrichtlinie bearbeiten
- Löschen einer differenzierten Datenschutzrichtlinie

- Anzeige der berechneten differenziellen Datenschutzparameter

Kollaborationen bearbeiten

Erfahren Sie, wie Sie die verschiedenen Teile einer Zusammenarbeit bearbeiten.

Themen

- Bearbeiten Sie den Namen und die Beschreibung der Kollaboration
- Bearbeiten Sie die Tags für die Zusammenarbeit
- Bearbeiten Sie Mitgliedskennungen
- Bearbeiten Sie die zugehörigen Tabellen-Tags
- Bearbeiten Sie die Tags der Analysevorlage
- Bearbeiten Sie unterschiedliche Datenschutzrichtlinientags

Bearbeiten Sie den Namen und die Beschreibung der Kollaboration

Nachdem Sie die Kollaboration erstellt haben, können Sie nur den Namen und die Beschreibung der Kollaboration bearbeiten.

> **Note**
>
> Wenn Sie die Abfrageprotokollierung aktiviert haben, können Sie bearbeiten, ob die Abfrageprotokolle in Ihrem Amazon CloudWatch Logs-Konto gespeichert werden.

Um den Namen und die Beschreibung der Zusammenarbeit zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, die Sie erstellt haben.
4. Wählen Sie auf der Seite mit den Kollaborationsdetails Aktionen und dann Zusammenarbeit bearbeiten aus.
5. Bearbeiten Sie für Details den Namen und die Beschreibung der Kollaboration.

6. Wählen Sie Änderungen speichern.

Bearbeiten Sie die Tags für die Zusammenarbeit

Als Ersteller einer Kollaboration können Sie, nachdem Sie eine Kollaboration erstellt haben, die Tags auf der Kollaborationsressource verwalten.

Um die Kollaborations-Tags zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, die Sie erstellt haben.
4. Wählen Sie eine der folgenden Optionen aus:

Wenn Sie …	Dann...
Ein Mitglied der Kollaboration	Wählen Sie die Registerkarte Details.
Der Ersteller der Kollaboration, aber kein Mitglied der Kollaboration	Scrollen Sie auf der Seite nach unten zum Abschnitt Tags.

5. Für Details zur Zusammenarbeit wählen Sie Tags verwalten aus.
6. Auf der Seite Tags verwalten haben Sie folgende Möglichkeiten:

   - Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
   - Um einen Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen).
   - Um Ihre Änderungen zu speichern, wählen Sie Änderungen speichern

Bearbeiten Sie Mitgliedskennungen

Als Ersteller einer Kollaboration können Sie, nachdem Sie eine Kollaboration erstellt haben, die Tags in der Mitgliedschaftsressource verwalten.

Um die Mitgliedschafts-Tags zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).

2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, die Sie erstellt haben.
4. Wählen Sie die Registerkarte Details.
5. Wählen Sie für Mitgliedschaftsdetails die Option Stichwörter verwalten aus.
6. Auf der Seite Mitgliedschafts-Tags verwalten können Sie Folgendes tun:

   - Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
   - Um einen Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen).
   - Klicken Sie auf Save changes (Änderungen speichern), um die Änderungen zu speichern.

Bearbeiten Sie die zugehörigen Tabellen-Tags

Als Ersteller einer Kollaboration können Sie, nachdem Sie Tabellen mit einer Kollaboration verknüpft haben, die Tags in der zugehörigen Tabellenressource verwalten.

Um die zugehörigen Tabellen-Tags zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, die Sie erstellt haben.
4. Wählen Sie die Registerkarte Tables (Tabellen).
5. Wählen Sie für Von Ihnen zugeordnete Tabellen eine Tabelle aus.
6. Wählen Sie auf der konfigurierten Tabellendetailseite für Tags die Option Tags verwalten aus.

   Auf der Seite Tags verwalten haben Sie folgende Möglichkeiten:

   - Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
   - Um einen Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen).
   - Klicken Sie auf Save changes (Änderungen speichern), um die Änderungen zu speichern.

Bearbeiten Sie die Tags der Analysevorlage

Als Ersteller einer Kollaboration können Sie, nachdem Sie eine Kollaboration erstellt haben, die Tags in der Analysevorlagenressource verwalten.

Um die Mitgliedschafts-Tags zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, die Sie erstellt haben.
4. Wählen Sie die Registerkarte Templates (Vorlagen) aus.
5. Wählen Sie im Abschnitt Von Ihnen erstellte Analysevorlagen die Analysevorlage aus.
6. Scrollen Sie auf der Detailseite der Analysevorlagentabelle nach unten zum Abschnitt Tags.
7. Wählen Sie Tags verwalten aus.
8. Auf der Seite Tags verwalten haben Sie folgende Möglichkeiten:

   - Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
   - Um einen Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen).
   - Klicken Sie auf Save changes (Änderungen speichern), um die Änderungen zu speichern.

Bearbeiten Sie unterschiedliche Datenschutzrichtlinientags

Als Ersteller einer Kollaboration können Sie, nachdem Sie eine Kollaboration erstellt haben, die Tags in der Analysevorlagenressource verwalten.

Um die Mitgliedschafts-Tags zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, die die differenzielle Datenschutzrichtlinie enthält, die Sie bearbeiten möchten.
4. Wählen Sie die Registerkarte Tables (Tabellen).
5. Wählen Sie auf der Registerkarte Tabellen die Option Tags verwalten aus.
6. Auf der Seite Tags verwalten haben Sie folgende Möglichkeiten:

   - Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
   - Um einen Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen).
   - Klicken Sie auf Save changes (Änderungen speichern), um die Änderungen zu speichern.

Kollaborationen löschen

Als Ersteller einer Kollaboration können Sie eine von Ihnen erstellte Kollaboration löschen.

> **Note**
>
> Wenn Sie eine Kollaboration löschen, können Sie und alle Mitglieder keine Abfragen ausführen, keine Ergebnisse erhalten oder Daten beitragen. Jedes Mitglied der Kollaboration hat im Rahmen seiner Mitgliedschaft weiterhin Zugriff auf seine eigenen Daten.

Um eine Kollaboration zu löschen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, die Sie löschen möchten.
4. Wählen Sie unter Aktionen die Option Kollaboration löschen aus.
5. Bestätigen Sie den Löschvorgang und wählen Sie dann Löschen.

Kollaborationen anzeigen

Als Ersteller einer Kollaboration können Sie sich alle Kollaborationen ansehen, die Sie erstellt haben.

Um Kollaborationen anzusehen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Sehen Sie sich auf der Seite Kollaborationen unter Zuletzt verwendet die letzten 5 verwendeten Kollaborationen an.
4. Sehen Sie sich auf der Registerkarte Mit aktiver Mitgliedschaft die Liste der Kollaborationen mit aktiver Mitgliedschaft an.

   Sie können nach dem Namen, dem Erstellungsdatum der Mitgliedschaft und Ihren Mitgliedsdetails sortieren.

Sie können die Suchleiste verwenden, um nach einer Kollaboration zu suchen.

5. Sehen Sie sich auf der Registerkarte „Für den Beitritt verfügbar“ die Liste der Kollaborationen an, denen Sie beitreten können.
6. Sehen Sie sich auf der Registerkarte Nicht mehr verfügbar die Liste der gelöschten Kollaborationen und Mitgliedschaften für Kollaborationen an, die nicht mehr verfügbar sind (entfernte Mitgliedschaften).

Tabellen und Analyseregeln anzeigen

Um Tabellen anzuzeigen, die der Kollaboration und den Analyseregeln zugeordnet sind

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Wählen Sie die Registerkarte Tables (Tabellen).
5. Wählen Sie eine der folgenden Optionen aus:

   a. Um Ihre der Kollaboration zugehörigen Tabellen anzuzeigen, wählen Sie unter Von Ihnen zugeordnete Tabellen eine Tabelle aus (blauer Text).

   b. Um andere der Kollaboration zugeordnete Tabellen anzuzeigen, wählen Sie unter Von Mitarbeitern zugeordnete Tabellen eine Tabelle aus (blauer Text).
6. Sehen Sie sich die Tabellendetails und Analyseregeln auf der Seite mit den Tabellendetails an.

Differenzielle Nutzungsprotokolle für Datenschutz anzeigen

Als Collaboration-Mitglied, das Daten mit Differential Privacy schützt, können Sie, nachdem Sie eine Collaboration mit Differential Privacy erstellt haben, die Nutzung des Datenschutzbudgets überwachen.

Um zu sehen, wie viele Aggregationen ausgeführt wurden und wie viel des Datenschutzbudgets aufgebraucht wurde

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).

2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Wählen Sie die Registerkarte Tables (Tabellen).
5. Wählen Sie Nutzungsprotokolle anzeigen (blauer Text).
6. Sehen Sie sich die Nutzungsdetails an, einschließlich des Datenschutzbudgets und der Anzahl der bereitgestellten Funktionen.

Den Mitgliedsstatus überwachen

Als Ersteller einer Kollaboration können Sie, nachdem Sie eine Kollaboration erstellt haben, den Status aller Mitglieder auf der Registerkarte Mitglieder überwachen.

Um den Status eines Mitglieds zu überprüfen

1. Melde dich an AWS Management Console und öffne die AWS Clean RoomsKonsole mit deinem AWS-Konto (falls du das noch nicht getan hast).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, die Sie erstellt haben.
4. Wählen Sie den Tab Mitglieder.
5. Sehen Sie sich den Mitgliedsstatus jedes Mitglieds an.

Ein Mitglied aus einer Kollaboration entfernen

> **Note**
>
> Wenn Sie ein Mitglied entfernen, werden auch alle zugehörigen Datensätze aus der Kollaboration entfernt.

Um ein Mitglied aus einer Kollaboration zu entfernen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus, die Sie erstellt haben.

4. Wählen Sie den Tab Mitglieder.
5. Wählen Sie das Optionsfeld neben dem Mitglied aus, das entfernt werden soll.

> **Note**
>
> Ein Kollaborationsersteller kann seine eigene Konto-ID nicht wählen.

6. Wählen Sie Remove (Entfernen) aus.
7. Bestätigen Sie im Dialogfeld die Entscheidung, das Mitglied zu entfernen, indem Sie es **`confirm`** in das Texteingabefeld eingeben.

> **Note**
>
> Wenn Sie das Mitglied entfernen, das für die Rechenkosten für Abfragen bezahlt, dürfen in der Kollaboration keine Abfragen mehr ausgeführt werden.

Verlassen einer Kollaboration

Als Mitglied einer Kollaboration können Sie eine Kollaboration verlassen, indem Sie Ihre Mitgliedschaft löschen. Wenn Sie der Ersteller der Kollaboration sind, können Sie eine Kollaboration nur verlassen, indem Sie die Kollaboration löschen.

> **Note**
>
> Wenn Sie Ihre Mitgliedschaft löschen, verlassen Sie die Kollaboration und können ihr nicht wieder beitreten. Wenn Sie das Mitglied sind, das die Kosten für die Datenverarbeitung bei Abfragen bezahlt, und Sie Ihre Mitgliedschaft löschen, dürfen keine Abfragen mehr ausgeführt werden.

Um eine Kollaboration zu verlassen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie unter Mit aktiver Mitgliedschaft die Kollaboration aus, bei der Sie Mitglied sind.

4. Wählen Sie Aktionen.
5. Wählen Sie Mitgliedschaft löschen.
6. Bestätigen Sie im Dialogfeld die Entscheidung, die Kollaboration zu verlassen, indem Sie etwas **`confirm`** in das Texteingabefeld eingeben, und wählen Sie dann Leeren und Mitgliedschaft löschen.

   Auf der Konsole wird eine Meldung angezeigt, die darauf hinweist, dass die Mitgliedschaft gelöscht wurde.

   Für den Ersteller der Kollaboration wird der Mitgliedsstatus „Links“ angezeigt.

Konfigurierte Tabellenzuordnungen bearbeiten

Als Mitglied einer Kollaboration können Sie die konfigurierten Tabellenverknüpfungen bearbeiten, die Sie erstellt haben.

Um konfigurierte Tabellenzuordnungen zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Wählen Sie den Tab Tabellen.
5. Wählen Sie für von Ihnen zugeordnete Tabellen eine Tabelle aus.
6. Scrollen Sie auf der Seite mit den Tabellendetails nach unten, um die Details zur Tabellenverknüpfung anzuzeigen.
7. Wählen Sie Bearbeiten aus.
8. Aktualisieren Sie auf der Seite „Konfigurierte Tabellenzuordnungen bearbeiten“ die Beschreibung oder die Informationen zum Zugriff auf den Dienst.
9. Wählen Sie Änderungen speichern.

Aufheben der Zuordnung konfigurierter Tabellen

Als Mitglied einer Kollaboration können Sie die Zuordnung einer konfigurierten Tabelle zur Kollaboration aufheben. Diese Aktion verhindert, dass das Mitglied, das Abfragen durchführen kann, die Tabelle abfragt.

Um die Zuordnung einer konfigurierten Tabelle aufzuheben

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Wählen Sie den Tab Tabellen.
5. Wählen Sie für von Ihnen zugeordnete Tabellen das Optionsfeld neben der Tabelle aus, deren Zuordnung Sie aufheben möchten.
6. Wählen Sie Disassociate (Zuordnung aufheben) aus.
7. Bestätigen Sie im Dialogfeld die Entscheidung, die Zuordnung der konfigurierten Tabelle aufzuheben, und verhindern Sie, dass das Mitglied, das Abfragen durchführen kann, die Tabelle abfragt, indem Sie die Option Zuordnung aufheben wählen.

Eine differenzielle Datenschutzrichtlinie bearbeiten

Nachdem Sie die differenzielle Datenschutzrichtlinie konfiguriert haben, können Sie sie jederzeit aktualisieren, um Ihren Datenschutzanforderungen besser gerecht zu werden.

Um die differenzielle Datenschutzrichtlinie zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Wählen Sie auf der Registerkarte Tabellen der Kollaborationsseite unter Von Ihnen zugeordnete Tabellen die Option Bearbeiten aus.
5. Wählen Sie auf der Seite Differentiellen Datenschutz bearbeiten neue Werte für die folgenden Eigenschaften aus:

- Datenschutzbudget — Bewegen Sie den Schieberegler, um das Budget zu einem beliebigen Zeitpunkt während einer Zusammenarbeit entweder zu erhöhen oder zu verringern. Sie können das Budget nicht verringern, nachdem das Mitglied, das Abfragen durchführen kann, mit der Abfrage Ihrer Daten begonnen hat. Wenn das Datenschutzbudget erhöht wird, AWS Clean Rooms wird das vorhandene Budget weiter verwendet, bis es vollständig aufgebraucht ist, bevor das neu hinzugefügte Datenschutzbudget verwendet wird.
- Pro Abfrage hinzugefügtes Rauschen — Bewegen Sie den Schieberegler, um das pro Abfrage hinzugefügte Rauschen zu einem beliebigen Zeitpunkt während einer Zusammenarbeit entweder zu erhöhen oder zu verringern.

> **Note**
>
> Mithilfe interaktiver Beispiele können Sie untersuchen, wie sich unterschiedliche Werte für Datenschutzbudget und hinzugefügtes Rauschen pro Abfrage auf die Anzahl der Aggregatfunktionen auswirken, die Sie ausführen können.

Sie können den Wert der Aktualisierung des Datenschutzbudgets nicht ändern. Um Ihre Auswahl zu ändern, müssen Sie die differenzielle Datenschutzrichtlinie löschen und eine neue erstellen.

6. Wählen Sie Änderungen speichern.

Sie erhalten eine Bestätigungsnachricht, dass Sie die differenzielle Datenschutzrichtlinie erfolgreich bearbeitet haben.

Löschen einer differenzierten Datenschutzrichtlinie

Sie können die differenzielle Datenschutzrichtlinie auf der Registerkarte Tabellen einer Kollaboration löschen.

Um die differenzielle Datenschutzrichtlinie zu löschen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.

4. Wählen Sie auf der Kollaborationsseite auf der Registerkarte Tabellen neben Differenzielle Datenschutzrichtlinie die Option Löschen aus.
5. Wenn Sie sicher sind, dass Sie die differenzielle Datenschutzrichtlinie löschen möchten, wählen Sie Löschen aus.

Nach dem Löschen einer differenzierten Datenschutzrichtlinie können Sie in dieser Richtlinie nicht mehr auf die Nutzungsprotokolle des Datenschutzbudgets zugreifen. Tabellen mit aktiviertem differenziellen Datenschutz können nicht abgefragt werden, wenn die differenzielle Datenschutzrichtlinie gelöscht wird.

Anzeige der berechneten differenziellen Datenschutzparameter

Benutzer mit Erfahrung im Bereich Differential Privacy können die berechneten differenziellen Datenschutzparameter auf der Registerkarte Abfragen einer Kollaboration einsehen.

Um die berechneten differenziellen Datenschutzparameter einzusehen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean RoomsKonsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich Collaborations aus.
3. Wählen Sie die Kollaboration aus.
4. Wählen Sie auf der Registerkarte Abfragen im Abschnitt Ergebnisse die Option Berechnete differenzielle Datenschutzparameter anzeigen aus.

In der Tabelle Berechnete differenzielle Datenschutzparameter können Sie die Sensitivitätswerte von Aggregatfunktionen sehen. Diese Werte sind als Höchstwert definiert, um den sich das Ergebnis einer Funktion ändern kann, wenn die Datensätze eines einzelnen Benutzers hinzugefügt, entfernt oder geändert werden. Die Liste enthält die folgenden unterschiedlichen Datenschutzparameter:

- Das Benutzerbeitragslimit (User Contribution Limit, UCL) ist die maximale Anzahl von Zeilen, die ein Benutzer zu einer SQL-Abfrage beigetragen hat. Wenn Sie beispielsweise die Gesamtzahl der übereinstimmenden Impressionen in einer bestimmten Kampagne zählen möchten, bei der jeder Nutzer mehrere Impressionen haben kann, muss AWS Clean Rooms Differential Privacy die Anzahl der Impressionen eines einzelnen Benutzers begrenzen, um sicherzustellen, dass die Berechnung des unterschiedlichen Datenschutzes korrekt ist. Mit anderen Worten, wenn ein Benutzer mehr Impressionen als die Grenze hat, nimmt er AWS Clean Rooms automatisch eine einheitliche Zufallsstichprobe der Impressionen dieses Benutzers gemäß dem berechneten

UCL-Wert und schließt die verbleibenden Impressionen dieses Benutzers bei der Ausführung der Abfrage aus. Der UCL-Wert entspricht 1, wenn Sie die Anzahl der eindeutigen Benutzer zählen. Das liegt daran, dass durch das Hinzufügen, Entfernen oder Ändern eines einzelnen Benutzers die Anzahl der einzelnen Benutzer um höchstens 1 geändert werden kann.

- Der Mindestwert ist die Untergrenze eines Ausdrucks, der in einer Aggregatfunktion wie verwendet wird`sum()`. Wenn es sich bei dem Ausdruck beispielsweise um eine Spalte handelt, die als bekannt ist`purchase_value`, ist der Mindestwert die Untergrenze der Spalte.
- Der Höchstwert ist die Obergrenze eines Ausdrucks, der in einer Aggregatfunktion wie verwendet wird`sum()`. Wenn es sich bei dem Ausdruck beispielsweise um eine Spalte handelt, die als bezeichnet wird`purchase_value`, ist der Höchstwert die Obergrenze der Spalte.

In der Tabelle Berechnete differenzielle Datenschutzparameter können Sie diese Parameter verwenden, um das Gesamtvolumen des Rauschens in den Abfrageergebnissen besser zu verstehen. Wenn die konfigurierte Anzahl der pro Abfrage hinzugefügten Störungen beispielsweise 30 Benutzer umfasst und eine `COUNT DISTINCT (user_id)` Abfrage ausgeführt wird, fügt AWS Clean Rooms Differential Privacy zufälliges Rauschen hinzu, das mit hoher Wahrscheinlichkeit zwischen -30 und 30 liegt, da die Sensitivität von 1 `COUNT DISTINCT` ist. Bei einer `COUNT` Abfrage mit derselben Konfiguration fügt AWS Clean Rooms Differential Privacy statistisches Rauschen hinzu, das nach dem Benutzerbeitragslimit skaliert wird, da ein einzelner Benutzer mehrere Zeilen zum Abfrageergebnis beitragen könnte. Bei einer `SUM` Abfrage wie `SUM (purchase_value)` bei der alle Spaltenwerte positiv sind, wird das Gesamtrauschen durch das Benutzerbeitragslimit multipliziert mit dem Höchstwert skaliert. AWS Clean Rooms Differential Privacy berechnet automatisch die Sensitivitätsparameter, um das Rauschen während der Abfragelaufzeit hinzuzufügen, wodurch das Datenschutzbudget aufgebraucht wird. Das Budget für den Datenschutz muss aufgebraucht werden, da die Sensitivitätsparameter datenabhängig sind.

Verwaltung konfigurierter Tabellen in AWS Clean Rooms

In den folgenden Themen wird beschrieben, wie Sie konfigurierte Tabellen AWS Clean Rooms mithilfe der AWS Clean Rooms Konsole verwalten.

Informationen zur Verwaltung konfigurierter Tabellen mithilfe der AWS SDKs finden Sie in der AWS Clean Rooms API-Referenz.

Themen

- Bearbeiten konfigurierter Tabellendetails

- Konfigurierte Tabellen-Tags bearbeiten
- Bearbeiten der konfigurierten Tabellenanalyseregel
- Die konfigurierte Tabellenanalyseregel wird gelöscht

Bearbeiten konfigurierter Tabellendetails

Als Mitglied einer Kollaboration können Sie die konfigurierten Tabellendetails bearbeiten.

Um konfigurierte Tabellendetails zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie die konfigurierte Tabelle aus, die Sie erstellt haben.
4. Scrollen Sie auf der Detailseite der konfigurierten Tabelle nach unten zu den Details der konfigurierten Tabelle.
5. Wählen Sie Bearbeiten aus.
6. Aktualisieren Sie den Namen oder die Beschreibung der konfigurierten Tabelle.
7. Wählen Sie Änderungen speichern aus.

Konfigurierte Tabellen-Tags bearbeiten

Als Mitglied der Kollaboration können Sie, nachdem Sie eine konfigurierte Tabelle erstellt haben, die Tags in der konfigurierten Tabellenressource auf der Registerkarte Konfigurierte Tabellen verwalten.

Um die konfigurierten Tabellen-Tags zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie die konfigurierte Tabelle aus, die Sie erstellt haben.
4. Scrollen Sie auf der Detailseite der konfigurierten Tabelle nach unten zum Abschnitt Tags.
5. Wählen Sie Tags verwalten aus.
6. Auf der Seite Tags verwalten haben Sie folgende Möglichkeiten:

- Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
- Um einen Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen).
- Klicken Sie auf Save changes (Änderungen speichern), um die Änderungen zu speichern.

Bearbeiten der konfigurierten Tabellenanalyseregel

Um die konfigurierte Tabellenanalyseregel zu bearbeiten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie die konfigurierte Tabelle aus, die Sie erstellt haben.
4. Scrollen Sie auf der Detailseite der konfigurierten Tabelle entweder nach unten zum Abschnitt Aggregationsanalyseregel, Listenanalyseregel oder Benutzerdefinierte Analyseregel. (Ihre Auswahl hängt davon ab, welche Art von Analyseregel Sie für die konfigurierte Tabelle ausgewählt haben.)
5. Wählen Sie Bearbeiten aus.
6. Auf der Seite Analyseregel bearbeiten können Sie:
   - Ändern Sie die Definition der Analyseregel wie folgt:
     - Ändern des JSON-Editors.
     - Wählen Sie Aus Datei importieren, um eine neue Analyseregeldefinition hochzuladen.
   - Wählen Sie aus den folgenden Optionen eine Vorschau dessen, was Mitglieder in einer Kollaboration sehen werden:
     - Tabellen-Ansicht
     - JSON
     - Beispielabfrage
7. Wählen Sie Änderungen speichern aus, um Ihre Änderungen zu speichern.

Die konfigurierte Tabellenanalyseregel wird gelöscht

> **Warning**
>
> Diese Aktion kann nicht rückgängig gemacht werden und wirkt sich auf alle zugehörigen Ressourcen aus.

Um die konfigurierte Tabellenanalyseregel zu löschen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Clean Rooms Konsole mit Ihrem AWS-Konto (falls Sie dies noch nicht getan haben).
2. Wählen Sie im linken Navigationsbereich die Option Konfigurierte Tabellen aus.
3. Wählen Sie die konfigurierte Tabelle aus, die Sie erstellt haben.
4. Scrollen Sie auf der Detailseite der konfigurierten Tabelle entweder nach unten zum Abschnitt Aggregationsanalyseregel, Listenanalyseregel oder Benutzerdefinierte Analyseregel. (Ihre Auswahl hängt davon ab, welche Art von Analyseregel Sie für die konfigurierte Tabelle ausgewählt haben.)
5. Wählen Sie Löschen aus.
6. Wenn Sie sicher sind, dass Sie die Analyseregel löschen möchten, wählen Sie Löschen.

Problembehebung AWS Clean Rooms

In diesem Abschnitt werden einige häufig auftretende Probleme beschrieben, die bei der Verwendung auftreten können, AWS Clean Rooms und deren Behebung.

Problembereiche

Auf eine oder mehrere Tabellen, auf die in der Abfrage verwiesen wird, kann über die zugehörige Dienstrolle nicht zugegriffen werden. Der Eigentümer der Tabellen/Rolle muss der Servicerolle Zugriff auf die Tabelle gewähren.

- Stellen Sie sicher, dass die Berechtigungen für die Servicerolle wie erforderlich eingerichtet sind. Weitere Informationen finden Sie unterEinrichten AWS Clean Rooms.

Einer der zugrunde liegenden Datensätze hat ein nicht unterstütztes Dateiformat.

- Stellen Sie sicher, dass Ihr Datensatz in einem der unterstützten Dateiformate vorliegt:
  - Parquet
  - RCFile
  - TextFile
  - SequenceFile
  - RegexSerde
  - OpenCSV

- AVRO
- JSON

Weitere Informationen finden Sie unter Datenformate für AWS Clean Rooms.

Die Abfrageergebnisse entsprechen nicht den Erwartungen, wenn Sie Cryptographic Computing for Clean Rooms verwenden.

Wenn Sie Cryptographic Computing for Clean Rooms (C3R) verwenden, stellen Sie sicher, dass Ihre Abfrage verschlüsselte Spalten korrekt verwendet:

- Die sealed Spalten werden nur in SELECT Klauseln verwendet.
- Die fingerprint Spalten werden nur in JOIN Klauseln (und GROUP BY Klauseln unter bestimmten Bedingungen) verwendet.
- Dass Sie nur JOINing fingerprint Spalten mit demselben Namen sind, wenn die Einstellungen für die Zusammenarbeit dies erfordern.

Weitere Informationen finden Sie unter Kryptografisches Rechnen und the section called “Spaltentypen”.

Sicherheit in AWS Clean Rooms

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den geltenden Compliance-Programmen finden Sie unter AWS-Services in Umfang nach Compliance-Programm . AWS Clean Rooms
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS Clean Rooms. Es zeigt Ihnen, wie Sie die Konfiguration vornehmen AWS Clean Rooms , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Clean Rooms Ressourcen unterstützen.

Inhalt

Datenschutz in AWS Clean Rooms

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Clean Rooms. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API AWS Clean Rooms oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung im Ruhezustand

AWS Clean Rooms verschlüsselt immer alle Dienstmetadaten im Ruhezustand, ohne dass eine zusätzliche Konfiguration erforderlich ist. Diese Verschlüsselung erfolgt automatisch, wenn Sie sie verwenden AWS Clean Rooms.

Clean Rooms ML verschlüsselt alle im Service gespeicherten Daten im Ruhezustand mit AWS KMS. Wenn Sie Ihren eigenen KMS-Schlüssel angeben, werden die Inhalte Ihrer Lookalike-Modelle und Jobs zur Generierung von Lookalike-Segmenten im Ruhezustand mit Ihrem KMS-Schlüssel verschlüsselt.

> **Note**
>
> Sie können die Verschlüsselungsoptionen in Amazon S3 verwenden, um Ihre Daten im Ruhezustand zu schützen.
> Weitere Informationen finden Sie unter Spezifizierung der Amazon S3 S3-Verschlüsselung im Amazon S3 S3-Benutzerhandbuch.

Verschlüsselung während der Übertragung

AWS Clean Rooms verwendet Transport Layer Security (TLS) und clientseitige Verschlüsselung für die Verschlüsselung bei der Übertragung. Die Kommunikation mit AWS Clean Rooms erfolgt immer über HTTPS, sodass Ihre Daten bei der Übertragung immer verschlüsselt werden. Dies schließt alle Daten ein, die bei der Verwendung von Clean Rooms ML übertragen werden.

Verschlüsselung der zugrunde liegenden Daten

Weitere Hinweise zum Verschlüsseln der zugrunde liegenden Daten finden Sie unter. Kryptografisches Rechnen für Clean Rooms

Aufbewahrung von Daten in AWS Clean Rooms

Wenn Sie ein Lookalike-Modell erstellen, liest Clean Rooms ML Ihre Trainingsdaten, wandelt sie in ein für unser ML-Modell geeignetes Format um und speichert die trainierten Modellparameter

in Clean Rooms ML. Clean Rooms ML speichert keine Kopie Ihrer Trainingsdaten. AWS Clean Rooms In SQL-Abfragen werden keine Ihrer Daten gespeichert, nachdem die Abfrage ausgeführt wurde. Clean Rooms ML verwendet dann das trainierte Modell, um das Verhalten all Ihrer Benutzer zusammenzufassen. Clean Rooms ML speichert für jeden Benutzer in Ihren Daten einen Datensatz auf Benutzerebene, solange Ihr Lookalike-Modell aktiv ist.

Wenn Sie einen Job zur Generierung von Lookalike-Segmenten starten, liest Clean Rooms ML die Ausgangsdaten, liest die Verhaltenszusammenfassungen aus dem zugehörigen Lookalike-Modell und erstellt ein Lookalike-Segment, das im Service gespeichert wird. AWS Clean Rooms Clean Rooms ML speichert keine Kopie Ihrer Ausgangsdaten. Clean Rooms ML speichert die Ausgabe des Jobs auf Benutzerebene, solange der Job aktiv ist.

Wenn Sie die Auftragsdaten Ihres Lookalike-Modells oder der Generierung von Lookalike-Segmenten entfernen möchten, verwenden Sie die API, um sie zu löschen. Clean Rooms ML löscht asynchron alle mit dem Modell oder Job verknüpften Daten. Sobald dieser Vorgang abgeschlossen ist, löscht Clean Rooms ML die Metadaten für das Modell oder den Job und sie sind in der API nicht mehr sichtbar. Clean Rooms ML bewahrt gelöschte Daten 3 Tage lang auf, um eine Notfallwiederherstellung zu verhindern. Sobald der Job oder das Modell in der API nicht mehr sichtbar ist und 3 Tage vergangen sind, wurden alle mit dem Modell oder Job verknüpften Daten dauerhaft gelöscht.

Bewährte Methoden für die Zusammenarbeit bei Daten in AWS Clean Rooms

In diesem Thema werden die bewährten Methoden für die Durchführung von Datenkooperationen in beschrieben. AWS Clean Rooms

AWS Clean Rooms folgt dem Modell der AWS gemeinsamen Verantwortung. AWS Clean Rooms bietet Analyseregeln, die Sie konfigurieren können, um Ihre Fähigkeit zu verbessern, vertrauliche Daten in einer Zusammenarbeit zu schützen. Die Analyseregeln, in denen Sie konfigurieren, setzen die von AWS Clean Rooms Ihnen konfigurierten Einschränkungen (Abfragesteuerelemente und Abfrageausgabesteuerungen) durch. Sie sind dafür verantwortlich, die Einschränkungen festzulegen und die Analyseregeln entsprechend zu konfigurieren.

Datenkooperationen können mehr als nur Ihre Nutzung von AWS Clean Rooms beinhalten. Damit Sie den größtmöglichen Nutzen aus Datenkooperationen ziehen können, empfehlen wir Ihnen, bei der Verwendung von Analyseregeln AWS Clean Rooms und insbesondere bei der Verwendung von Analyseregeln die folgenden bewährten Methoden anzuwenden.

Themen

Bewährte Methoden mit AWS Clean Rooms

Sie sind dafür verantwortlich, das Risiko jeder Datenzusammenarbeit zu bewerten und es mit Ihren Datenschutzanforderungen wie externen und internen Compliance-Programmen und -Richtlinien zu vergleichen. Wir empfehlen Ihnen, bei der Verwendung von zusätzliche Maßnahmen zu ergreifen AWS Clean Rooms. Diese Maßnahmen können dazu beitragen, Risiken besser zu managen und vor Versuchen Dritter zu schützen, Ihre Daten neu zu identifizieren (z. B. differenzierende Angriffe oder Side-Channel-Angriffe).

Erwägen Sie beispielsweise, bei Ihren anderen Mitarbeitern eine Due-Diligence-Prüfung durchzuführen und rechtliche Vereinbarungen mit ihnen zu treffen, bevor Sie eine Zusammenarbeit eingehen. Um die Verwendung Ihrer Daten zu überwachen, sollten Sie auch die Einführung anderer Prüfmechanismen in Betracht ziehen. AWS Clean Rooms

Bewährte Methoden für die Verwendung von Analyseregeln in AWS Clean Rooms

Mit den Analyseregeln in AWS Clean Rooms können Sie die Abfragen einschränken, die ausgeführt werden können, indem Sie die Abfragesteuerelemente für eine konfigurierte Tabelle festlegen. Sie können beispielsweise eine Abfragesteuerung dafür einrichten, wie eine konfigurierte Tabelle verknüpft und welche Spalten ausgewählt werden können. Sie können die Abfrageausgabe auch einschränken, indem Sie Steuerelemente für Abfrageergebnisse festlegen, z. B. Aggregationsschwellenwerte für Ausgabezeilen. Der Dienst lehnt jede Abfrage ab und entfernt Zeilen, die nicht den Analyseregeln entsprechen, die von Mitgliedern in ihren konfigurierten Tabellen in der Abfrage festgelegt wurden.

Wir empfehlen die folgenden 10 bewährten Methoden für die Verwendung von Analyseregeln in Ihrer konfigurierten Tabelle:

- Erstellen Sie separate konfigurierte Tabellen für separate Anwendungsfälle für Abfragen (z. B. Zielgruppenplanung oder Zuordnung). Sie können mehrere konfigurierte Tabellen mit derselben zugrunde liegenden AWS Glue Tabelle erstellen.

- Geben Sie in der Analyseregel Spalten an (z. B. Dimensionsspalten, Listenspalten, Verbindungsspalten), die für Abfragen in einer Kollaboration erforderlich sind. Dies kann dazu beitragen, das Risiko zu verringern, dass Angriffe differenziert werden oder dass andere Mitglieder Ihre Daten zurückentwickeln können. Verwenden Sie die Funktion Allowlist-Spalten, um andere Spalten zu notieren, die Sie möglicherweise in future abfragbar machen möchten. Um die Spalten anzupassen, die für eine bestimmte Zusammenarbeit verwendet werden können, erstellen Sie zusätzliche konfigurierte Tabellen mit derselben Basistabelle. AWS Glue
- Geben Sie in der Analyseregel die Funktionen an, die für die Analyse in der Kollaboration erforderlich sind. Dies kann dazu beitragen, das Risiko zu verringern, das durch seltene Funktionsfehler entsteht, die Informationen zu einem einzelnen Datenpunkt enthalten können. Um die Funktionen anzupassen, die für eine bestimmte Zusammenarbeit verwendet werden können, erstellen Sie zusätzliche konfigurierte Tabellen mit derselben zugrunde liegenden AWS Glue Tabelle.
- Fügen Sie Aggregationseinschränkungen für alle Spalten hinzu, deren Werte auf Zeilenebene sensibel sind. Dies schließt Spalten in Ihrer konfigurierten Tabelle ein, die auch in den Tabellen und Analyseregeln anderer Kollaborationsmitglieder als Aggregationseinschränkung vorhanden sind. Dazu gehören auch Spalten in Ihrer konfigurierten Tabelle, die nicht abfragbar sind, d. h. Spalten, die sich in Ihrer konfigurierten Tabelle befinden, aber nicht in der Analyseregel enthalten sind. Aggregationsbeschränkungen können dazu beitragen, das Risiko zu verringern, das durch die Korrelation von Abfrageergebnissen mit Daten außerhalb der Zusammenarbeit entsteht.
- Erstellen Sie Testkollaborationen und Analyseregeln, um Einschränkungen zu testen, die mit bestimmten Analyseregeln erstellt wurden.
- Überprüfen Sie die von den Mitarbeitern konfigurierten Tabellen und die Analyseregeln der Mitglieder in den konfigurierten Tabellen, um sicherzustellen, dass sie den für die Zusammenarbeit vereinbarten Regeln entsprechen. Dies kann dazu beitragen, das Risiko zu verringern, dass andere Mitglieder ihre eigenen Daten manipulieren, um Abfragen auszuführen, die nicht vereinbart wurden.
- Sehen Sie sich die bereitgestellte Beispielabfrage (nur Konsole) an, die in Ihrer konfigurierten Tabelle aktiviert ist, nachdem Sie die Analyseregel eingerichtet haben.

> **Note**
>
> Zusätzlich zu der bereitgestellten Beispielabfrage sind weitere Abfragen möglich, die auf der Analyseregel und anderen Tabellen und Analyseregeln für Kollaborationsmitglieder basieren.

- Sie können eine Analyseregel für eine konfigurierte Tabelle in einer Kollaboration hinzufügen oder aktualisieren. Wenn Sie dies tun, überprüfen Sie alle Kollaborationen, denen die konfigurierte Tabelle zugeordnet ist, und die sich daraus ergebenden Auswirkungen. Auf diese Weise können Sie sicherstellen, dass keine Kollaborationen veraltete Analyseregeln verwenden.
- Überprüfen Sie die in der Kollaboration ausgeführten Abfragen, um sicherzustellen, dass die Abfragen den Anwendungsfällen oder Abfragen entsprechen, die für die Zusammenarbeit vereinbart wurden. (Die Abfragen sind in den Abfrageprotokollen verfügbar, wenn die Funktion zur Abfrageprotokollierung aktiviert ist.) Dies kann dazu beitragen, das Risiko zu verringern, dass Mitglieder Analysen durchführen, die nicht vereinbart wurden, und potenzielle Angriffe wie Seitenkanalangriffe.
- Überprüfen Sie die konfigurierten Tabellenspalten, die in den Analyseregeln der Kollaborationsmitglieder und in Abfragen verwendet werden, um sicherzustellen, dass sie den in der Zusammenarbeit vereinbarten Werten entsprechen. (Die Abfragen sind in den Abfrageprotokollen verfügbar, wenn diese Funktion aktiviert ist.) Dies kann dazu beitragen, das Risiko zu verringern, dass andere Mitglieder ihre eigenen Daten manipulieren, um Abfragen durchzuführen, über die keine Einigung erzielt wurde.

Identity and Access Management für AWS Clean Rooms

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Clean Rooms IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- IAM-Verhalten für ML AWS Clean Rooms

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS Clean Rooms

Dienstbenutzer — Wenn Sie den AWS Clean Rooms Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS Clean Rooms Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Fehlerbehebung bei AWS Clean Rooms Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS Clean Rooms haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS Clean Rooms Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS Clean Rooms. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS Clean Rooms Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann AWS Clean Rooms, finden Sie unterWie AWS Clean Rooms funktioniert mit IAM.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS Clean Rooms verfassen können. Beispiele für AWS Clean Rooms identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Clean Rooms

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) - Benutzer oder die Single Sign-On-Authentifizierung Ihres Unternehmens sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von

IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über einen Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mit Ihren Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen über die empfohlene Methode zur eigenständigen Signierung von Anfragen finden Sie unter Signierprozess mit Signaturversion 4 in der Allgemeine AWS-Referenz.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto -Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden, auch nicht für administrative Aufgaben. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Root-Benutzer des AWS-Kontos Anmeldeinformationen und IAM-Identitäten in der. Allgemeine AWS-Referenz

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services

könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen

in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Eine IAM-Entität (Benutzer oder Rolle) besitzt zunächst keine Berechtigungen. Standardmäßig können Benutzer nichts tun, nicht einmal ihr eigenes Passwort ändern. Um einem Benutzer die Berechtigung für eine Aktion zu erteilen, muss ein Administrator einem Benutzer eine Berechtigungsrichtlinie zuweisen. Alternativ kann der Administrator den Benutzer zu einer Gruppe hinzufügen, die über die gewünschten Berechtigungen verfügt. Wenn ein Administrator einer Gruppe Berechtigungen erteilt, erhalten alle Benutzer in dieser Gruppe diese Berechtigungen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die resultierenden Berechtigungen sind eine Schnittmenge der identitätsbasierten Richtlinien der Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS Clean Rooms funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf zu verwalten AWS Clean Rooms, sollten Sie sich darüber informieren, welche IAM-Funktionen zur Verfügung stehen. AWS Clean Rooms

IAM-Funktionen, die Sie mit verwenden können AWS Clean Rooms

IAM-Feature	AWS Clean Rooms Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Teilweise
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Teilweise
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja

IAM-Feature	AWS Clean Rooms Unterstützung
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie die meisten IAM-Funktionen AWS-Services funktionieren AWS Clean Rooms und wie sie funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für AWS Clean Rooms

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS Clean Rooms

Beispiele für AWS Clean Rooms identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Clean Rooms

Ressourcenbasierte Richtlinien finden Sie in AWS Clean Rooms

Unterstützt ressourcenbasierte Richtlinien	Teilweise

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Der AWS Clean Rooms Service unterstützt nur eine Art von ressourcenbasierter Richtlinie, die als konfiguriertes Lookalike-Modell (verwaltete Ressourcenrichtlinie) bezeichnet wird und an ein konfiguriertes Lookalike-Modell angehängt ist. Diese Richtlinie definiert, welche Principals Aktionen auf dem konfigurierten Lookalike-Modell ausführen können.

Informationen zum Anhängen einer ressourcenbasierten Richtlinie an ein konfiguriertes Lookalike-Modell finden Sie unter. IAM-Verhalten für ML AWS Clean Rooms

Politische Maßnahmen für AWS Clean Rooms

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS Clean Rooms Aktionen finden Sie unter Aktionen definiert von AWS Clean Rooms in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Clean Rooms verwendet.

```
cleanrooms
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "cleanrooms:action1",
      "cleanrooms:action2"
         ]
```

Beispiele für AWS Clean Rooms identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Clean Rooms

Politische Ressourcen für AWS Clean Rooms

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der AWS Clean Rooms Ressourcentypen und ihrer ARNs finden Sie unter Ressourcen definiert von AWS Clean Rooms in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Clean Rooms definierte Aktionen.

Beispiele für AWS Clean Rooms identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Clean Rooms

Bedingungsschlüssel für Richtlinien für AWS Clean Rooms

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Teilweise

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Informationen darüber, wie AWS Clean Rooms ML Bedingungsschlüssel für Richtlinien verwendet, finden Sie unter IAM-Verhalten für ML AWS Clean Rooms.

ACLs in AWS Clean Rooms

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS Clean Rooms

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit AWS Clean Rooms

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Zugriffssitzungen weiterleiten für AWS Clean Rooms

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Clean Rooms

Unterstützt Servicerollen	Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS Clean Rooms Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, AWS Clean Rooms wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für AWS Clean Rooms

Unterstützt serviceverknüpfte Rollen	Nein

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene

Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS Clean Rooms

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS Clean Rooms -Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der API AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden AWS Clean Rooms, einschließlich des Formats der ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Clean Rooms in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der AWS Clean Rooms -Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Clean Rooms Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der AWS Clean Rooms -Konsole

Um auf die AWS Clean Rooms Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Clean Rooms Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS Clean Rooms Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS Clean Rooms *FullAccess* oder die *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI AWS OR-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinien für AWS Clean Rooms

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: **AWSCleanRoomsReadOnlyAccess**

Sie können eine Verbindung `AWSCleanRoomsReadOnlyAccess` zu Ihren IAM-Prinzipalen herstellen.

Diese Richtlinie gewährt nur Leseberechtigungen für Ressourcen und Metadaten in einer Kollaboration. `AWSCleanRoomsReadOnlyAccess`

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `CleanRoomsRead`— Ermöglicht Prinzipalen nur Lesezugriff auf den Dienst.
- `ConsoleDisplayTables`— Ermöglicht Prinzipalen den schreibgeschützten Zugriff auf die AWS Glue Metadaten, die für die Anzeige von Daten zu den zugrunde liegenden Tabellen auf der Konsole erforderlich sind. AWS Glue
- `ConsoleLogSummaryQueryLogs`— Ermöglicht es den Prinzipalen, die Abfrageprotokolle zu sehen.
- `ConsoleLogSummaryObtainLogs`— Ermöglicht Prinzipalen das Abrufen der Protokollergebnisse.

```
{
 "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 verwaltete Richtlinie: **`AWSCleanRoomsFullAccess`**

Sie können eine Verbindung `AWSCleanRoomsFullAccess` zu Ihren IAM-Prinzipalen herstellen.

Diese Richtlinie gewährt Administratorberechtigungen, die vollen Zugriff (Lesen, Schreiben und Aktualisieren) auf Ressourcen und Metadaten in einer AWS Clean Rooms Kollaboration ermöglichen. Diese Richtlinie beinhaltet den Zugriff zur Durchführung von Abfragen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `CleanRoomsAccess`— Gewährt vollen Zugriff auf alle Aktionen auf allen Ressourcen für AWS Clean Rooms.

- `PassServiceRole`— Gewährt Zugriff zur Übergabe einer Servicerolle nur an den Dienst (`PassedToService`Bedingung), dessen Name cleanrooms "" enthält.
- `ListRolesToPickServiceRole`— Ermöglicht es Prinzipalen, alle ihre Rollen aufzulisten, um bei der Verwendung AWS Clean Rooms eine Servicerolle auszuwählen.
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Ermöglicht Prinzipalen, die Servicerolle und die entsprechende Richtlinie in IAM zu sehen.
- `ListPoliciesToInspectServiceRolePolicy`— Ermöglicht Prinzipalen, die Servicerolle und die entsprechende Richtlinie in IAM zu sehen.
- `GetPolicyToInspectServiceRolePolicy`— Ermöglicht Prinzipalen, die Servicerolle und die entsprechende Richtlinie in IAM zu sehen.
- `ConsoleDisplayTables`— Ermöglicht Prinzipalen den schreibgeschützten Zugriff auf die AWS Glue Metadaten, die für die Anzeige von Daten zu den zugrunde liegenden AWS Glue Tabellen auf der Konsole erforderlich sind.
- `ConsolePickQueryResultsBucketListAll`— Ermöglicht Prinzipalen, einen Amazon S3 S3-Bucket aus einer Liste aller verfügbaren S3-Buckets auszuwählen, in die ihre Abfrageergebnisse geschrieben werden.
- `SetQueryResultsBucket`— Ermöglicht Prinzipalen, einen S3-Bucket auszuwählen, in den ihre Abfrageergebnisse geschrieben werden.
- `ConsoleDisplayQueryResults`— Ermöglicht es den Prinzipalen, dem Kunden die Abfrageergebnisse anzuzeigen, die aus dem S3-Bucket gelesen wurden.
- `WriteQueryResults`— Ermöglicht Prinzipalen, die Abfrageergebnisse in einen kundeneigenen S3-Bucket zu schreiben.
- `EstablishLogDeliveries`— Ermöglicht Principals, Abfrageprotokolle an die Amazon CloudWatch Logs-Protokollgruppe eines Kunden zu senden.
- `SetupLogGroupsDescribe`— Ermöglicht Prinzipalen, den Prozess zur Erstellung von Amazon CloudWatch Logs-Protokollgruppen zu verwenden.
- `SetupLogGroupsCreate`— Ermöglicht Prinzipalen, eine Amazon CloudWatch Logs-Protokollgruppe zu erstellen.
- `SetupLogGroupsResourcePolicy`— Ermöglicht Prinzipalen, eine Ressourcenrichtlinie für die Amazon CloudWatch Logs-Protokollgruppe einzurichten.
- `ConsoleLogSummaryQueryLogs`— Ermöglicht es den Prinzipalen, die Abfrageprotokolle einzusehen.

- `ConsoleLogSummaryObtainLogs`— Ermöglicht Prinzipalen das Abrufen der Protokollergebnisse.

```
{
 "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 verwaltete Richtlinie: **AWSCleanRoomsFullAccessNoQuerying**

Sie können es `AWSCleanRoomsFullAccessNoQuerying` an Ihre anhängenIAM principals.

Diese Richtlinie gewährt Administratorberechtigungen, die vollen Zugriff (Lesen, Schreiben und Aktualisieren) auf Ressourcen und Metadaten in einer AWS Clean Rooms Kollaboration ermöglichen. Diese Richtlinie schließt den Zugriff zur Durchführung von Abfragen aus.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `CleanRoomsAccess`— Gewährt vollen Zugriff auf alle Aktionen auf allen Ressourcen für AWS Clean Rooms, mit Ausnahme von Abfragen in Kollaborationen.
- `CleanRoomsNoQuerying`— Verweigert ausdrücklich das Abfragen `StartProtectedQuery` und verhindert `UpdateProtectedQuery` es.
- `PassServiceRole`— Gewährt Zugriff auf die Übergabe einer Servicerolle nur an den Dienst (`PassedToService`Bedingung), dessen Name "cleanrooms" enthält.
- `ListRolesToPickServiceRole`— Ermöglicht es Prinzipalen, alle ihre Rollen aufzulisten, um bei der Verwendung AWS Clean Rooms eine Servicerolle auszuwählen.
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Ermöglicht Prinzipalen, die Servicerolle und die entsprechende Richtlinie in IAM zu sehen.

- `ListPoliciesToInspectServiceRolePolicy`— Ermöglicht Prinzipalen, die Servicerolle und die entsprechende Richtlinie in IAM zu sehen.
- `GetPolicyToInspectServiceRolePolicy`— Ermöglicht Prinzipalen, die Servicerolle und die entsprechende Richtlinie in IAM zu sehen.
- `ConsoleDisplayTables`— Ermöglicht Prinzipalen den schreibgeschützten Zugriff auf die AWS Glue Metadaten, die für die Anzeige von Daten zu den zugrunde liegenden AWS Glue Tabellen auf der Konsole erforderlich sind.
- `EstablishLogDeliveries`— Ermöglicht Principals, Abfrageprotokolle an die Amazon CloudWatch Logs-Protokollgruppe eines Kunden zu senden.
- `SetupLogGroupsDescribe`— Ermöglicht Prinzipalen, den Prozess zur Erstellung von Amazon CloudWatch Logs-Protokollgruppen zu verwenden.
- `SetupLogGroupsCreate`— Ermöglicht Prinzipalen, eine Amazon CloudWatch Logs-Protokollgruppe zu erstellen.
- `SetupLogGroupsResourcePolicy`— Ermöglicht Prinzipalen, eine Ressourcenrichtlinie für die Amazon CloudWatch Logs-Protokollgruppe einzurichten.
- `ConsoleLogSummaryQueryLogs`— Ermöglicht es den Prinzipalen, die Abfrageprotokolle einzusehen.
- `ConsoleLogSummaryObtainLogs`— Ermöglicht Prinzipalen das Abrufen der Protokollergebnisse.
- `cleanrooms`— Verwaltet Kollaborationen, Analysevorlagen, konfigurierte Tabellen, Mitgliedschaften und zugehörige Ressourcen innerhalb des Service. AWS Clean Rooms Führen Sie verschiedene Operationen durch, z. B. das Erstellen, Aktualisieren, Löschen, Auflisten und Abrufen von Informationen zu diesen Ressourcen.
- `iam`— Übergibt Dienstrollen, deren Namen "`cleanrooms`" enthalten, an den AWS Clean Rooms Dienst. Listen Sie Rollen und Richtlinien auf und überprüfen Sie die Dienstrollen und Richtlinien, die sich auf den AWS Clean Rooms Dienst beziehen.
- `glue`— Rufen Sie Informationen zu Datenbanken, Tabellen, Partitionen und Schemas von ab AWS Glue. Dies ist erforderlich, damit der AWS Clean Rooms Dienst die zugrunde liegenden Datenquellen anzeigen und mit ihnen interagieren kann.
- `logs`— Verwalten Sie Protokollzustellungen, Protokollgruppen und Ressourcenrichtlinien für CloudWatch Protokolle. Abfragen und Abrufen von Protokollen, die sich auf den AWS Clean Rooms Dienst beziehen. Diese Berechtigungen sind für Überwachungs-, Überprüfungs- und Fehlerbehebungszwecke innerhalb des Dienstes erforderlich.

Die Richtlinie lehnt die Aktionen auch ausdrücklich ab `cleanrooms:StartProtectedQuery` und verhindert`cleanrooms:UpdateProtectedQuery`, dass Benutzer geschützte Abfragen direkt ausführen oder aktualisieren, was über die AWS Clean Rooms kontrollierten Mechanismen geschehen sollte.

```
{
 "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 verwaltete Richtlinie: **AWSCleanRoomsMLReadOnlyAccess**

Sie können eine Verbindung `AWSCleanRoomsMLReadOnlyAccess` zu Ihren IAM-Prinzipalen herstellen.

Diese Richtlinie gewährt nur Leseberechtigungen für Ressourcen und Metadaten in einer Kollaboration. `AWSCleanRoomsMLReadOnlyAccess`

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `CleanRoomsConsoleNavigation`— Gewährt Zugriff auf die Bildschirme der AWS Clean Rooms Konsole.
- `CleanRoomsMLRead`— Ermöglicht Prinzipalen nur Lesezugriff auf den Clean Rooms ML-Dienst.

```
{
    "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 verwaltete Richtlinie: **AWSCleanRoomsMLFullAccess**

Sie können eine Verbindung `AWSCleanRoomsMLFullAcces` zu Ihren IAM-Prinzipalen herstellen. Diese Richtlinie gewährt Administratorberechtigungen, die vollen Zugriff (Lesen, Schreiben und Aktualisieren) auf Ressourcen und Metadaten ermöglichen, die von Clean Rooms ML benötigt werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `CleanRoomsMLFullAccess`— Gewährt Zugriff auf alle Clean Rooms ML-Aktionen.
- `PassServiceRole`— Gewährt Zugriff auf die Weitergabe einer Servicerolle nur an den Dienst (`PassedToService`Bedingung), dessen Name cleanrooms-ml "" enthält.
- `CleanRoomsConsoleNavigation`— Gewährt Zugriff auf die Bildschirme der AWS Clean Rooms Konsole.
- `CollaborationMembershipCheck`— Wenn Sie innerhalb einer Kollaboration einen Job zur Zielgruppengenerierung (Lookalike-Segment) starten, ruft der Clean Rooms ML-Service an, `ListMembers` um zu überprüfen, ob die Kollaboration gültig ist, ob der Anrufer ein aktives Mitglied und der Besitzer des konfigurierten Zielgruppenmodells ein aktives Mitglied ist. Diese Berechtigung ist immer erforderlich. Die SID für die Konsolennavigation ist nur für Konsolenbenutzer erforderlich.
- `AssociateModels`— Ermöglicht Prinzipalen, Ihrer Zusammenarbeit ein Clean Rooms-ML-Modell zuzuordnen.
- `TagAssociations`— Ermöglicht es Prinzipalen, der Verknüpfung zwischen einem Lookalike-Modell und einer Kollaboration Tags hinzuzufügen.
- `ListRolesToPickServiceRole`— Ermöglicht es Prinzipalen, alle ihre Rollen aufzulisten, um bei der Verwendung eine Servicerolle auszuwählen. AWS Clean Rooms
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Ermöglicht Prinzipalen, die Servicerolle und die entsprechende Richtlinie in IAM zu sehen.
- `ListPoliciesToInspectServiceRolePolicy`— Ermöglicht Prinzipalen, die Servicerolle und die entsprechende Richtlinie in IAM zu sehen.
- `GetPolicyToInspectServiceRolePolicy`— Ermöglicht Prinzipalen, die Servicerolle und die entsprechende Richtlinie in IAM zu sehen.
- `ConsoleDisplayTables`— Ermöglicht Prinzipalen den schreibgeschützten Zugriff auf die AWS Glue Metadaten, die für die Anzeige von Daten zu den zugrunde liegenden AWS Glue Tabellen auf der Konsole erforderlich sind.

- `ConsolePickOutputBucket`— Ermöglicht Prinzipalen die Auswahl von Amazon S3 S3-Buckets für konfigurierte Zielgruppenmodellausgaben.
- `ConsolePickS3Location`— Ermöglicht Prinzipalen die Auswahl des Speicherorts innerhalb eines Buckets für konfigurierte Zielgruppenmodell-Ausgaben.

```
{
    "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 Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS Clean Rooms seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite AWS Clean Rooms Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWSCleanRoomsFullAccessNoQuerying – Aktualisierung auf eine bestehende Richtlinie	cleanrooms:BatchGetSchemaAnalysisRule wurde CleanRoomsAccess hinzugefügt.	13. Mai 2024

Änderung	Beschreibung	Datum
AWSCleanRoomsFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die Statement ID in der Zeile AWSCleanRoomsFullAccess von ConsolePickQueryResultsBucket bis wurde SetQueryResultsBucket in dieser Richtlinie aktualisiert, um die Berechtigungen besser darzustellen, da die Berechtigungen für die Einstellung des Abfrageergebnis-Buckets sowohl mit als auch ohne Konsole benötigt werden.	21. März 2024
AWSCleanRoomsMLReadOnlyAccess – Neue Richtlinie. AWSCleanRoomsMLFullAccess – Neue Richtlinie.	Hinzugefügt AWSCleanRoomsMLReadOnlyAccess und AWSCleanRoomsMLFullAccess zur Unterstützung von AWS Clean Rooms ML.	29. November 2023
AWSCleanRoomsFullAccessNoQuerying – Aktualisierung auf eine bestehende Richtlinie	cleanrooms:CreateAnalysisTemplate,,cleanrooms:GetAnalysisTemplate,cleanrooms:UpdateAnalysisTemplate, cleanrooms:DeleteAnalysisTemplatecleanrooms:ListAnalysisTemplates, und hinzugefügt cleanrooms:GetCollaborationAnalysisTemplatecleanrooms:BatchGetCollaborationAnalysisTemplate, cleanrooms:ListCollaborationAnalysisTemplates CleanRoomsAccess um die neue Funktion für Analysevorlagen zu aktivieren.	31. Juli 2023
AWSCleanRoomsFullAccessNoQuerying – Aktualisierung auf eine bestehende Richtlinie	cleanrooms:ListTagsForResource, und cleanrooms:TagResource zu hinzugefügtcleanrooms:UntagResource, CleanRoomsAccess um das Ressourcen-Tagging zu aktivieren.	21. März 2023

Änderung	Beschreibung	Datum
AWS Clean Rooms hat begonnen, Änderungen zu verfolgen	AWS Clean Rooms hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	12. Januar 2023

Fehlerbehebung bei AWS Clean Rooms Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Clean Rooms und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Clean Rooms
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Clean Rooms Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Clean Rooms

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `cleanrooms:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cleanrooms:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Mateo-Richtlinie aktualisiert werden, damit er mit der `cleanrooms:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Clean Roomsübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Clean Rooms auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Clean Rooms Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS Clean Rooms unterstützt werden, finden Sie unterWie AWS Clean Rooms funktioniert mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In AWS kann ein dienstübergreifendes Identitätswechsels zum Problem des verwirrten Stellvertreters führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die `aws:SourceArn`globalen Bedingungskontextschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWSClean Rooms Ressource einen anderen Dienst gewähren. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. AWSClean RoomsIn müssen Sie auch mit dem `sts:ExternalId` Bedingungsschlüssel vergleichen.

Der Wert von `aws:SourceArn` muss auf den ARN der Mitgliedschaft der übernommenen Rolle gesetzt werden.

Das folgende Beispiel zeigt, wie Sie den Kontextschlüssel für `aws:SourceArn` globale Bedingungen verwenden können, AWSClean Rooms um das Problem des verwirrten Stellvertreters zu vermeiden.

> **Note**
>
> Die Beispielrichtlinie bezieht sich auf die Vertrauensrichtlinie der Servicerolle, die für den Zugriff auf Kundendaten AWSClean Rooms verwendet wird.
> Der Wert von *MembershipID ist Ihre AWSClean Rooms Mitglieds-ID* in der Kollaboration.

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

IAM-Verhalten für ML AWS Clean Rooms

Kontoübergreifende Jobs

Mit Clean Rooms ML können bestimmte Ressourcen, die von einer Person erstellt wurden AWS-Konto , von einer anderen AWS-Konto Person sicher in ihrem Konto abgerufen werden. Wenn ein Kunde in AWS-Konto A eine `ConfiguredAudienceModel` Ressource `StartAudienceGenerationJob` aufruft, die AWS-Konto B gehört, erstellt Clean Rooms ML zwei ARNs für den Job. Ein ARN in AWS-Konto A und ein weiterer in AWS-Konto B. Die ARNs sind bis auf ihre AWS-Konto identisch.

Clean Rooms ML erstellt zwei ARNs für den Job, um sicherzustellen, dass beide Konten ihre eigenen IAM-Richtlinien auf die Jobs anwenden können. Beispielsweise können beide Konten eine tagbasierte Zugriffskontrolle verwenden und die Richtlinien ihrer Organisation anwenden. AWS Der Job verarbeitet Daten von beiden Konten, sodass beide Konten den Job und die zugehörigen Daten löschen können. Keines der Konten kann das andere Konto daran hindern, den Job zu löschen.

Es gibt nur eine Auftragsausführung und beide Konten können den Job sehen, wenn sie aufrufen`ListAudienceGenerationJobs`. Beide Konten können die `Export` APIs `GetDelete`, und für den Job aufrufen, indem sie den ARN mit ihrer eigenen AWS-Konto ID verwenden.

Keiner AWS-Konto kann auf den Job zugreifen, wenn er einen ARN mit der anderen AWS-Konto ID verwendet.

Der Name des Jobs muss innerhalb eines eindeutig sein AWS-Konto. Der Name in AWS-Konto B ist *`$AccountA-$name`*. Dem von AWS-Konto A ausgewählten Namen wird A vorangestellt, wenn der Job in AWS-Konto B angezeigt wird. AWS-Konto

Damit ein Cross-Account `StartAudienceGenerationJob` erfolgreich ist, muss AWS-Konto B diese Aktion sowohl für den neuen Job in B als auch für den Job in AWS-Konto B zulassen. Dabei `ConfiguredAudienceModel` muss eine Ressourcenrichtlinie verwendet werden, die dem folgenden Beispiel ähnelt: AWS-Konto

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

Wenn Sie die AWS Clean Rooms ML-API verwenden, um ein konfiguriertes Lookalike-Modell mit dem Wert `manageResourcePolicies` true zu erstellen, AWS Clean Rooms erstellt diese Richtlinie für Sie.

Darüber hinaus benötigt die Identitätsrichtlinie des Aufrufers in AWS-Konto A eine `StartAudienceGenerationJob` entsprechende Genehmigung. `arn:aws:cleanrooms-ml:us-west-1:AccountA:audience-generation-job/*` Es gibt also drei IAM-Ressourcen für Aktionen`StartAudienceGenerationJob`: den AWS-Konto A-Job, den AWS-Konto B-Job und den AWS-Konto B-Job. `ConfiguredAudienceModel`

> **Warning**
>
> Derjenige AWS-Konto , der den Job gestartet hat, erhält ein AWS CloudTrail Audit-Log-Ereignis über den Job. AWS-Konto Derjenige, dem der gehört, empfängt `ConfiguredAudienceModel` kein AWS CloudTrail Überwachungsprotokollereignis.

Jobs taggen

Wenn Sie den `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` Parameter von festlegen`CreateConfiguredAudienceModel`, haben alle Jobs zur Generierung von Lookalike-

Segmenten in Ihrem Konto, die anhand dieses konfigurierten Lookalike-Modells erstellt wurden, standardmäßig dieselben Tags wie das konfigurierte Lookalike-Modell. Das konfigurierte Lookalike-Modell ist das übergeordnete Modell und der Job zur Generierung von Lookalike-Segmenten ist das untergeordnete Modell.

Wenn Sie einen Job in Ihrem eigenen Konto erstellen, überschreiben die Anforderungs-Tags des Jobs die übergeordneten Tags. Jobs, die von anderen Konten erstellt wurden, erzeugen niemals Stichwörter in Ihrem Konto. Wenn Sie einen Job einrichten `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` und ein anderer Account erstellt, gibt es zwei Kopien des Jobs. Die Kopie in Ihrem Konto enthält die übergeordneten Ressourcen-Tags und die Kopie im Konto des Jobeinreichers enthält Stichwörter aus der Anfrage.

Mitarbeiter werden validiert

Wenn Sie anderen Mitgliedern einer AWS Clean Rooms Kollaboration Berechtigungen gewähren, sollte die Ressourcenrichtlinie den Bedingungsschlüssel enthalten. `cleanrooms-ml:CollaborationId` Dadurch wird erzwungen, dass der `collaborationId` Parameter in der StartAudienceGenerationJobAnfrage enthalten ist. Wenn der `collaborationId` Parameter in der Anfrage enthalten ist, überprüft Clean Rooms ML, ob die Kollaboration existiert, dass der Jobeinreicher ein aktives Mitglied der Kollaboration ist und der Besitzer des konfigurierten Lookalike-Modells ein aktives Mitglied der Kollaboration ist.

Wenn Ihre konfigurierte Ressourcenrichtlinie für das Lookalike-Modell AWS Clean Rooms verwaltet wird (der `manageResourcePolicies` Parameter ist CreateConfiguredAudienceModelAssociation angefordert), wird dieser Bedingungsschlüssel `TRUE` in der Ressourcenrichtlinie festgelegt. Daher müssen Sie den `collaborationId` in StartAudienceGenerationJobangeben.

Kontoübergreifender Zugriff

`StartAudienceGenerationJob`Kann nur kontenübergreifend aufgerufen werden. Alle anderen Clean Rooms ML-APIs können nur mit Ressourcen in Ihrem eigenen Konto verwendet werden. Dadurch wird sichergestellt, dass Ihre Trainingsdaten, die Konfiguration eines Lookalike-Modells und andere Informationen vertraulich bleiben.

Clean Rooms ML gibt niemals Amazon S3 oder AWS Glue Standorte für mehrere Konten preis. Der Speicherort der Trainingsdaten, der konfigurierte Speicherort für die Ausgabe eines Lookalike-Modells und der Standort der Jobstartdaten für die Lookalike-Segmentgenerierung sind nicht für alle Konten sichtbar. Wenn es sich `Get` um einen Job zur Zielgruppengenerierung handelt, der von einem anderen Account eingereicht wurde, zeigt der Service den Ausgangsort nicht an.

Überprüfung der Einhaltung der Vorschriften für AWS Clean Rooms

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in AWS Clean Rooms

Die AWS globale Infrastruktur basiert auf AWS Regionen und Verfügbarkeitszonen. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Sicherheit der Infrastruktur in AWS Clean Rooms

Als verwalteter Dienst AWS Clean Rooms ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS Clean Rooms über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Netzwerksicherheit

Wenn während der Abfrageausführung aus Ihrem S3-Bucket AWS Clean Rooms gelesen wird, wird der Datenverkehr zwischen Amazon S3 AWS Clean Rooms und Amazon S3 sicher durch das AWS private Netzwerk geleitet. Eingehender Datenverkehr wird mit dem Amazon Signature Version 4-Protokoll (SIGv4) signiert und mit HTTPS verschlüsselt. Dieser Datenverkehr wird auf der Grundlage der IAM-Servicerolle autorisiert, die Sie für Ihre konfigurierte Tabelle eingerichtet haben.

Sie können programmgesteuert eine Verbindung AWS Clean Rooms über einen Endpunkt herstellen. Eine Liste der Dienstendpunkte finden Sie unter AWS Clean Rooms Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

Alle Dienstendpunkte sind nur für HTTPS verfügbar. Sie können Amazon Virtual Private Cloud (VPC) -Endpunkte verwenden, falls Sie AWS Clean Rooms von Ihrer VPC aus eine Verbindung herstellen möchten und keine Internetverbindung haben möchten. Weitere Informationen finden Sie unter Access AWS services through AWS PrivateLink im Handbuch.AWS PrivateLink

Sie können Ihren IAM-Prinzipalen IAM-Richtlinien zuweisen, die die SourceVpce aws:-Kontextschlüssel verwenden, um Ihren IAM-Prinzipal darauf zu beschränken, Anrufe nur AWS Clean Rooms über einen VPC-Endpunkt und nicht über das Internet tätigen zu können.

Zugriff AWS Clean Rooms oder AWS Clean Rooms ML über einen Schnittstellen-Endpunkt ()AWS PrivateLink

Sie können AWS PrivateLink es verwenden, um eine private Verbindung zwischen Ihrer Virtual Private Cloud (VPC) AWS Clean Rooms und/oder AWS Clean Rooms ML herzustellen. Sie können auf AWS Clean Rooms oder AWS Clean Rooms ML zugreifen, als ob es in Ihrer VPC wäre, ohne ein

Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung verwenden zu müssen. Instances in Ihrer VPC benötigen für den Zugriff AWS Clean Rooms keine öffentlichen IP-Adressen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Hierbei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Eingangspunkt für den Datenverkehr dienen, der für AWS Clean Rooms bestimmt ist.

Weitere Informationen finden Sie unter Zugriff auf AWS-Services über AWS PrivateLink im AWS PrivateLink -Leitfaden.

Überlegungen zu AWS Clean Rooms

Bevor Sie einen Schnittstellen-Endpunkt für einrichten AWS Clean Rooms, lesen Sie die Überlegungen im AWS PrivateLink Handbuch.

AWS Clean Rooms und AWS Clean Rooms ML unterstützen das Aufrufen all ihrer API-Aktionen über den Schnittstellenendpunkt.

VPC-Endpunktrichtlinien werden für AWS Clean Rooms oder AWS Clean Rooms ML nicht unterstützt. Standardmäßig ist Vollzugriff auf AWS Clean Rooms und AWS Clean Rooms ML über den Schnittstellenendpunkt zulässig. Alternativ können Sie den Endpunkt-Netzwerkschnittstellen eine Sicherheitsgruppe zuordnen, um den Datenverkehr zum AWS Clean Rooms oder AWS Clean Rooms ML über den Schnittstellenendpunkt zu steuern.

Erstellen Sie einen Schnittstellenendpunkt für AWS Clean Rooms

Sie können einen Schnittstellenendpunkt für AWS Clean Rooms oder AWS Clean Rooms ML entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen Schnittstellenendpunkt für die AWS Clean Rooms Verwendung des folgenden Servicenamens.

```
com.amazonaws.region.cleanrooms
```

Erstellen Sie einen Schnittstellenendpunkt für AWS Clean Rooms ML mit dem folgenden Dienstnamen.

```
com.amazonaws.region.cleanrooms-ml
```

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anfragen an die AWS Clean Rooms Verwendung des standardmäßigen regionalen DNS-Namens stellen. Zum Beispiel , ., `cleanrooms-ml.us-east-1.amazonaws.com`.

Überwachung AWS Clean Rooms

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Clean Rooms anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, mit denen Sie beobachten AWS Clean Rooms, melden können, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen ergreifen können:

- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von Amazon EC2 EC2-Instances und anderen Quellen überwachen AWS CloudTrail, speichern und darauf zugreifen. Amazon CloudWatch Logs kann Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.

  Clean Rooms ML ermöglicht kontoübergreifende Jobs für bestimmte API-Aktionen. Derjenige AWS-Konto , der den Job gestartet hat, erhält das AWS CloudTrail Audit-Log-Ereignis für den Job. Weitere Informationen finden Sie unter IAM-Verhalten für ML AWS Clean Rooms.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Protokollieren von AWS Clean Rooms-API-Aufrufen mithilfe von AWS CloudTrail

AWS Clean Roomsist in integriertAWS CloudTrail, einem Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einemAWS-Service durchgeführten Aktionen bereitstelltAWS Clean Rooms. CloudTrail erfasst alle API-Aufrufe fürAWS Clean Rooms als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Clean Rooms-Konsole und Code-Aufrufe der AWS Clean Rooms-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket, einschließlich Ereignissen fürAWS Clean Rooms Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail Konsole trotzdem in Ereignisverlauf anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an gestellte AnfrageAWS Clean Rooms, die IP-Adresse, von der die

Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und weitere Angaben bestimmen.

Weitere Informationen CloudTrail finden Sie im AWS CloudTrailBenutzerhandbuch.

AWS Clean RoomsInformationen in CloudTrail

CloudTrail wirdAWS-Konto beim Erstellen Ihres für Sie aktiviert. Wenn eine Aktivität auftrittAWS Clean Rooms, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderenAWS-Service Ereignissen in Ereignisverlauf protokolliert. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS Clean Rooms, erstellen Sie einen Trail. Ein Trail CloudTrail ermöglicht es Protokolldateien in einem Amazon S3 S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere konfigurieren,AWS-Services um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen
- Empfangen von CloudTrail Protokolldateien von mehreren Konten

AlleAWS Clean Rooms Aktionen werden von der AWS Clean RoomsAPI-Referenz protokolliert CloudTrail und sind in dieser dokumentiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Stammbenutzers oder des IAM-Benutzers gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.

- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlagen zu AWS Clean Rooms-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Beispiele fürAWS Clean Rooms CloudTrail Ereignisse

Die folgenden Beispiele veranschaulichen CloudTrail Ereignisse für

Themen

- StartProtectedQuery (erfolgreich)
- StartProtectedQuery(gescheitert)

StartProtectedQuery (erfolgreich)


```
{
    "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(gescheitert)

```
{
    "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"
}
```

AWS Clean Rooms Ressourcen erstellen mit AWS CloudFormation

AWS Clean Rooms ist in einen Service integriert AWS CloudFormation, der Sie bei der Modellierung und Einrichtung Ihrer AWS Ressourcen unterstützt. Dank dieser Integration müssen Sie weniger Zeit für die Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur aufwenden. Sie erstellen eine Vorlage, die alle gewünschten AWS Ressourcen beschreibt und diese Ressourcen für Sie AWS CloudFormation bereitstellt und konfiguriert. Zu den Ressourcen gehören beispielsweise Kollaborationen, konfigurierte Tabellen, konfigurierte Tabellenzuordnungen und Mitgliedschaften.

Wenn Sie Ihre Vorlage verwenden AWS CloudFormation, können Sie sie wiederverwenden, um Ihre AWS Clean Rooms Ressourcen einheitlich und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen immer wieder mehrfach AWS-Konten bereit AWS-Regionen.

AWS Clean Rooms und AWS CloudFormation Vorlagen

Um Ressourcen für und zugehörige Dienste bereitzustellen AWS Clean Rooms und zu konfigurieren, müssen Sie sich mit AWS CloudFormation Vorlagen auskennen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie AWS CloudFormation Designer verwenden, um Ihnen die ersten Schritte mit Vorlagen zu erleichtern. AWS CloudFormation Weitere Informationen finden Sie unter Was ist AWS CloudFormation -Designer? im AWS CloudFormation -Benutzerhandbuch.

AWS Clean Rooms unterstützt das Erstellen von Kollaborationen, konfigurierten Tabellen, konfigurierten Tabellenzuordnungen und Mitgliedschaften in. AWS CloudFormationWeitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für Kollaborationen, konfigurierte Tabellen, konfigurierte Tabellenzuordnungen und Mitgliedschaften, finden Sie in der Referenz zum AWS Clean Rooms Ressourcentyp im Benutzerhandbuch.AWS CloudFormation

Die folgenden Vorlagen sind verfügbar:

- Vorlage für eine Analyse

  Geben Sie eine AWS Clean Rooms Analysevorlage an, einschließlich eines Namens, einer Beschreibung, eines Formats, einer Quelle, Parametern und Tags.

Weitere Informationen finden Sie unter den folgenden Themen:

AWS::CleanRooms::AnalysisTemplate im AWS Clean Rooms -Benutzerhandbuch

CreateAnalysisTemplate in der AWS Clean Rooms -API-Referenz

- Zusammenarbeit

  Geben Sie eine AWS Clean Rooms Kollaboration an, einschließlich eines Namens, einer Beschreibung, eines Typs, von Parametern und Tags.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::CleanRooms::Collaboration im AWS CloudFormation -Benutzerhandbuch

  CreateCollaboration in der AWS Clean Rooms -API-Referenz

- Konfigurierte Tabelle

  Geben Sie eine konfigurierte Tabelle in an AWS Clean Rooms, einschließlich der zulässigen Spalten, der Analysemethode, der Beschreibung, des Namens, der Tabellenreferenz, des Datenschutzbudgets und der Tags. Konfigurierte Tabellen stellen einen Verweis auf eine bestehende Tabelle in dar AWS Glue Data Catalog , die für die Verwendung in konfiguriert wurde AWS Clean Rooms. Eine konfigurierte Tabelle enthält eine Analyseregel, die bestimmt, wie die Daten verwendet werden können.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::CleanRooms::ConfiguredTable im AWS CloudFormation -Benutzerhandbuch

  CreateConfiguredTable in der AWS Clean Rooms -API-Referenz

- Konfigurierte Tabellenverknüpfung

  Geben Sie eine konfigurierte AWS Clean Rooms Tabellenverknüpfung an, einschließlich ID, Beschreibung, Mitglieds-ID, Name, Rolle, Amazon-Ressourcenname (ARN) und Tags. Eine konfigurierte Tabellenzuordnung verknüpft eine konfigurierte Tabelle mit einer Kollaboration.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::CleanRooms::ConfiguredTableAssociation im AWS CloudFormation -Benutzerhandbuch

  CreateConfiguredTableAssociation in der AWS Clean Rooms -API-Referenz

- Mitgliedschaft

  Geben Sie die Mitgliedschaft für eine bestimmte Kollaborations-ID an und treten Sie der Kollaboration bei AWS Clean Rooms.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::CleanRooms::Membership im AWS CloudFormation -Benutzerhandbuch

  CreateMembership in der AWS Clean Rooms -API-Referenz

- Vorlage für ein Datenschutzbudget

  Geben Sie eine Vorlage für ein AWS Clean Rooms Datenschutzbudget an, einschließlich eines Datenschutzbudgets, zusätzlicher Datenvolumen pro Anfrage und einer monatlichen Aktualisierung des Datenschutzbudgets.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::CleanRooms::PrivacyBudgetTemplate im AWS CloudFormation -Benutzerhandbuch

  CreatePrivacyBudgetTemplate in der AWS Clean Rooms -API-Referenz

- Trainingsdatensatz erstellen

  Geben Sie einen Trainingsdatensatz für ein Clean Rooms-ML-Modell aus einer AWS Glue Tabelle an.

  Weitere Informationen finden Sie unter den folgenden Themen:

  AWS::CleanRoomsML::TrainingDataset im AWS CloudFormation -Benutzerhandbuch

  CreateTrainingDatasetin der Clean Rooms ML API-Referenz

Erfahren Sie mehr über AWS CloudFormation

Weitere Informationen AWS CloudFormation dazu finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- AWS CloudFormation API Reference

- AWS CloudFormation -Benutzerhandbuch für die Befehlszeilenschnittstelle

Kontingente für AWS Clean Rooms

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jedes Kontingent AWS-Service. Sofern nicht anders angegeben, ist jedes Kontingent spezifisch für ein AWS-Region. Sie können für einige Kontingente eine Erhöhung beantragen, während andere Kontingente nicht erhöht werden können.

Um die Kontingente für anzuzeigen AWS Clean Rooms, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS-Services aus und wählen Sie AWS Clean Rooms.

Informationen zum Beantragen einer Kontingenterhöhung finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch. Wenn das Kontingent noch nicht unter Servicekontingente verfügbar ist, verwenden Sie das Formular zur Erhöhung des Servicelimits.

Ihr AWS-Konto hat die folgenden Kontingente im Zusammenhang mit AWS Clean Rooms.

Ressource	Standard	Beschreibung
Pro Zusammenarbeit eingeladene Mitglieder	5	Maximale Anzahl eingeladener Mitglieder pro Kollaboration
Mitgliedschaften pro Konto	100	Maximale Anzahl von Mitgliedschaften für ein Konto
Pro Konto erstellte Zusammenarbeiten	10	Maximale Anzahl von Kollaborationen, die pro Konto erstellt wurden
Konfigurierte Tabellen pro Konto	60	Maximale Anzahl konfiguri erter Tabellen, die von einem Konto erstellt werden können
Tabellenzuordnungen pro Mitgliedschaft	25	Maximale Anzahl von Tabellen, die pro aktiver Mitgliedschaft verknüpft sind
Gleichzeitig laufende Anfragen pro Mitgliedschaft	5	Maximale Anzahl gleichzei tiger laufender Abfragen pro Mitgliedschaft

Ressource	Standard	Beschreibung
Spalten pro konfigurierter Tabellenzulassungsliste	100	Maximale Anzahl von Spalten, die pro konfigurierter Tabelle auf die Zulassungsliste gesetzt werden können
Konfigurierte Tabellen pro geschützter Abfrage	15	Maximale Anzahl konfiguri erter Tabellen in einer geschützten Abfrage
Analysevorlagen pro Mitglieds chaft	25	Maximale Anzahl von Analysevorlagen pro Mitglieds chaft
Konfigurierte Verknüpfungen im Lookalike-Modell (Zielgrup penmodell) pro Mitgliedschaft	5	Maximale Anzahl konfiguri erter Lookalike-Modell-A ssoziationen pro Mitglieds chaft.

Grenzwerte für Ressourcenparameter

Ressource	Standard	Beschreibung
Größe der Analyseregeln	100 KB	Maximale JSON-Größe für eine Analyseregel
Länge des Abfragetexts	90 KB (8 KB für differenzielle Datenschutzabfragen)	Maximale Textlänge für eine SQL-Abfrageanweisung
Laufzeit der Abfrage	12 Stunden	Maximale Dauer, für die eine Abfrage vor dem Timeout ausgeführt wird
Ausgabegröße der Datendatei abfragen	6,2 GB	Maximale Größe einer Ausgabedatei aus einer geschützten Abfrage

Ihr Konto AWS-Konto verfügt über die folgenden Kontingente für API-Transaktionen pro Sekunde (TPS) pro Konto und Endpunkt.

API-Drosselungskontingente

Ressource	Ratenlimit	Beschreibung
Rate der Anfragen `BatchGetCollaborationAnalysisTemplate`	5 TPS	Maximale Anzahl von `BatchGetCollaborationAnalysisTemplate` API-Aufrufen pro Sekunde
Rate der `BatchGetSchema` Anfragen	5 TPS	Maximale Anzahl von `BatchGetSchema` API-Aufrufen pro Sekunde
Rate der `CreateAnalysisTemplate` Anfragen	5 TPS	Maximale Anzahl von `CreateAnalysisTemplate` API-Aufrufen pro Sekunde
Rate der `CreateCollaboration` Anfragen	5 TPS	Maximale Anzahl von `CreateCollaboration` API-Aufrufen pro Sekunde
Rate der `CreateConfiguredAudienceModelAssociation` Anfragen	5 TPS	Maximale Anzahl von `CreateConfiguredAudienceModelAssociation` -Aufrufen pro Sekunde
Rate der `CreateConfiguredTable` Anfragen	5 TPS	Maximale Anzahl von `CreateConfiguredTable` -Aufrufen pro Sekunde
Rate der `CreateConfiguredTableAnalysisRule` Anfragen	5 TPS	Maximale Anzahl von `CreateConfiguredTableAnalysisRule` -Aufrufen pro Sekunde

Ressource	Ratenlimit	Beschreibung
Rate der `CreateConfiguredTableAssociation` Anfragen	5 TPS	Maximale Anzahl von `CreateConfiguredTableAssociation` -Aufrufen pro Sekunde
Rate der `CreateMembership` Anfragen	5 TPS	Maximale Anzahl von `CreateMembership` -Aufrufen pro Sekunde
Rate der `CreatePrivacyBudgetTempate` Anfragen	5 TPS	Maximale Anzahl von `CreatePrivacyBudgetTemplate` -Aufrufen pro Sekunde
Rate der `DeleteAnalysisTemplate` Anfragen	5 TPS	Maximale Anzahl von `DeleteAnalysisTemplate` -Aufrufen pro Sekunde
Rate der `DeleteCollaboration` Anfragen	5 TPS	Maximale Anzahl von `DeleteCollaboration` -Aufrufen pro Sekunde
Rate der `DeleteConfiguredAudienceModelAssociation` Anfragen	5 TPS	Maximale Anzahl von `DeleteConfiguredAudienceModelAssociation` -Aufrufen pro Sekunde
Rate der `DeleteConfiguredTable` Anfragen	5 TPS	Maximale Anzahl von `DeleteConfiguredTable` -Aufrufen pro Sekunde
Rate der `DeleteConfiguredTableAnalysisRule` Anfragen	5 TPS	Maximale Anzahl von `DeleteConfiguredTableAnalysisRule` -Aufrufen pro Sekunde

Ressource	Ratenlimit	Beschreibung
Rate der `DeleteConfiguredTableAssociation` Anfragen	5 TPS	Maximale Anzahl von `DeleteConfiguredTableAssociation` -Aufrufen pro Sekunde
Rate der `DeleteMember` Anfragen	5 TPS	Maximale Anzahl von `DeleteMember` -Aufrufen pro Sekunde
Rate der `DeleteMembership` Anfragen	5 TPS	Maximale Anzahl von `DeleteMembership` -Aufrufen pro Sekunde
Rate der `DeletePrivacyBudgetTemplate` Anfragen	5 TPS	Maximale Anzahl von `DeletePrivacyBudgetTemplate` -Aufrufen pro Sekunde
Rate der `GetAnalysisTemplate` Anfragen	5 TPS	Maximale Anzahl von `GetAnalysisTemplate` -Aufrufen pro Sekunde
Rate der `GetCollaboration` Anfragen	5 TPS	Maximale Anzahl von `GetCollaboration` -Aufrufen pro Sekunde
Rate der `GetCollaborationConfiguredAudienceModelAssociation` Anfragen	5 TPS	Maximale Anzahl von `GetCollaborationConfiguredAudienceModelAssociation` -Aufrufen pro Sekunde
Rate der `GetCollaborationPrivacyBudgetTemplate` Anfragen	5 TPS	Maximale Anzahl von `GetCollaborationPrivacyBudgetTemplate` -Aufrufen pro Sekunde

Ressource	Ratenlimit	Beschreibung
Rate der `GetConfiguredAudienceModelAssociation` Anfragen	5 TPS	Maximale Anzahl von `GetConfiguredAudienceModelAssociation` -Aufrufen pro Sekunde
Rate der `GetConfiguredTable` Anfragen	5 TPS	Maximale Anzahl von `GetConfiguredTable` -Aufrufen pro Sekunde
Rate der `GetConfiguredTableAnalysisRule` Anfragen	5 TPS	Maximale Anzahl von `GetConfiguredTableAnalysisRule` -Aufrufen pro Sekunde
Rate der `GetConfiguredTableAssociation` Anfragen	20 TPS	Maximale Anzahl von `GetConfiguredTableAssociation` -Aufrufen pro Sekunde
Rate der `GetMembership` Anfragen	5 TPS	Maximale Anzahl von `GetMembership` -Aufrufen pro Sekunde
Rate der `GetPrivacyBudgetTemplate` Anfragen	5 TPS	Maximale Anzahl von `GetPrivacyBudgetTemplate` -Aufrufen pro Sekunde
Rate der `GetProtectedQuery` Anfragen	20 TPS	Maximale Anzahl von `GetProtectedQuery` -Aufrufen pro Sekunde
Rate der `GetSchema` Anfragen	5 TPS	Maximale Anzahl von `GetSchema` -Aufrufen pro Sekunde

Ressource	Ratenlimit	Beschreibung
Rate der `GetSchemaAnalysisRule` Anfragen	5 TPS	Maximale Anzahl von `GetSchemaAnalysisRule` -Aufrufen pro Sekunde
Rate der `ListAnalysisTemplates` Anfragen	5 TPS	Maximale Anzahl von `ListAnalysisTemplates` -Aufrufen pro Sekunde
Rate der `ListCollaborationConfiguredAudienceModelAssociations` Anfragen	5 TPS	Maximale Anzahl von `ListCollaborationConfiguredAudienceModelAssociations` -Aufrufen pro Sekunde
Rate der `ListCollaborationPrivacyBudgets` Anfragen	5 TPS	Maximale Anzahl von `ListCollaborationPrivacyBudgets` -Aufrufen pro Sekunde
Rate der `ListCollaborationPrivacyBudgetTemplates` Anfragen	5 TPS	Maximale Anzahl von `ListCollaborationPrivacyBudgetTemplates` -Aufrufen pro Sekunde
Rate der `ListCollaborations` Anfragen	5 TPS	Maximale Anzahl von `ListCollaborations` -Aufrufen pro Sekunde
Rate der `ListConfiguredAudienceModelAssociations` Anfragen	5 TPS	Maximale Anzahl von `ListConfiguredAudienceModelAssociations` -Aufrufen pro Sekunde

Ressource	Ratenlimit	Beschreibung
Rate der `ListConfiguredTableAssociations` Anfragen	5 TPS	Maximale Anzahl von `ListConfiguredTableAssociations` -Aufrufen pro Sekunde
Rate der `ListConfiguredTables` Anfragen	5 TPS	Maximale Anzahl von `ListConfiguredTables` -Aufrufen pro Sekunde
Rate der `ListMembers` Anfragen	5 TPS	Maximale Anzahl von `ListMembers` -Aufrufen pro Sekunde
Rate der `ListMemberships` Anfragen	5 TPS	Maximale Anzahl von `ListMemberships` -Aufrufen pro Sekunde
Rate der `ListPrivacyBudgets` Anfragen	5 TPS	Maximale Anzahl von `ListPrivacyBudgets` -Aufrufen pro Sekunde
Rate der `ListPrivacyBudgetTemplates` Anfragen	5 TPS	Maximale Anzahl von `ListPrivacyBudgetTemplates` -Aufrufen pro Sekunde
Rate der `ListProtectedQueries` Anfragen	5 TPS	Maximale Anzahl von `ListProtectedQueries` -Aufrufen pro Sekunde
Rate der `ListSchemas` Anfragen	5 TPS	Maximale Anzahl von `ListSchemas` -Aufrufen pro Sekunde

Ressource	Ratenlimit	Beschreibung
Rate der `StartProtectedQuery` Anfragen	5 TPS	Maximale Anzahl von `StartProtectedQuery` -Aufrufen pro Sekunde
Rate der `UpdateAnalysisTemplate` Anfragen	5 TPS	Maximale Anzahl von `UpdateAnalysisTemplate` -Aufrufen pro Sekunde
Rate der `UpdateCollaboration` Anfragen	5 TPS	Maximale Anzahl von `UpdateCollaboration` -Aufrufen pro Sekunde
Rate der `UpdateConfiguredAudienceModelAssociation` Anfragen	5 TPS	Maximale Anzahl von `UpdateConfiguredAudienceModelAssociation` -Aufrufen pro Sekunde
Rate der `UpdateConfiguredTable` Anfragen	5 TPS	Maximale Anzahl von `UpdateConfiguredTable` -Aufrufen pro Sekunde
Rate der `UpdateConfiguredTableAnalysisRule` Anfragen	5 TPS	Maximale Anzahl von `UpdateConfiguredTableAnalysisRule` -Aufrufen pro Sekunde
Rate der `UpdateConfiguredTableAssociation` Anfragen	5 TPS	Maximale Anzahl von `UpdateConfiguredTableAssociation` -Aufrufen pro Sekunde
Rate der `UpdatePrivacyBudgetTemplate` Anfragen	5 TPS	Maximale Anzahl von `UpdatePrivacyBudgetTemplate` -Aufrufen pro Sekunde

AWS Clean Rooms Drosselung der Kontingente durch die ML-API

Ressource	Ratenlimit	Beschreibung
Rate der Anfragen `CreateAudienceModel`	1 TPS-Rate, 3 TPS-Burst	Maximale Anzahl von `CreateAudienceModel` API-Aufrufen pro Sekunde
Rate der `CreateConfiguredAudienceModel` Anfragen	10 TPS	Maximale Anzahl von `CreateConfiguredAudienceModel` API-Aufrufen pro Sekunde
Rate der `CreateTrainingDataset` Anfragen	10 TPS	Maximale Anzahl von `CreateTrainingDataset` API-Aufrufen pro Sekunde
Rate der `DeleteAudienceGenerationJob` Anfragen	Geschwindigkeit von 2 TPS, Burst von 10 TPS	Maximale Anzahl von `DeleteAudienceGenerationJob` API-Aufrufen pro Sekunde
Rate der `DeleteAudienceModel` Anfragen	Geschwindigkeit von 2 TPS, Burst von 10 TPS	Maximale Anzahl von `DeleteAudienceModel` API-Aufrufen pro Sekunde
Rate der `DeleteConfiguredAudienceModel` Anfragen	10 TPS	Maximale Anzahl von `DeleteConfiguredAudienceModel` API-Aufrufen pro Sekunde
Rate der `DeleteConfiguredAudienceModelPolicy` Anfragen	25 TPS	Maximale Anzahl von `DeleteConfiguredAudienceModelPolicy` API-Aufrufen pro Sekunde
Rate der `DeleteTrainingDataset` Anfragen	10 TPS	Maximale Anzahl von `DeleteTrainingData`

Ressource	Ratenlimit	Beschreibung
		`set` API-Aufrufen pro Sekunde
Rate der `GetAudienceGenerationJob` Anfragen	50 TPS	Maximale Anzahl von `GetAudienceGenerationJob` API-Aufrufen pro Sekunde
Rate der `GetAudienceModel` Anfragen	50 TPS	Maximale Anzahl von `GetAudienceModel` API-Aufrufen pro Sekunde
Rate der `GetConfiguredAudienceModel` Anfragen	50 TPS	Maximale Anzahl von `GetConfiguredAudienceModel` API-Aufrufen pro Sekunde
Rate der `GetConfiguredAudienceModelPolicy` Anfragen	50 TPS	Maximale Anzahl von `GetConfiguredAudienceModelPolicy` API-Aufrufen pro Sekunde
Rate der `GetTrainingDataset` Anfragen	50 TPS	Maximale Anzahl von `GetTrainingDataset` API-Aufrufen pro Sekunde
Rate der `ListAudienceExportJobs` Anfragen	50 TPS	Maximale Anzahl von `ListAudienceExportJobs` API-Aufrufen pro Sekunde
Rate der `ListAudienceGenerationJobs` Anfragen	50 TPS	Maximale Anzahl von `ListAudienceGenerationJobs` API-Aufrufen pro Sekunde

Ressource	Ratenlimit	Beschreibung
Rate der `ListAudienceModels` Anfragen	50 TPS	Maximale Anzahl von `ListAudienceModels` API-Aufrufen pro Sekunde
Rate der `ListConfiguredAudienceModels` Anfragen	50 TPS	Maximale Anzahl von `ListConfiguredAudienceModels` API-Aufrufen pro Sekunde
Rate der `ListTagsForResource` Anfragen	50 TPS	Maximale Anzahl von `ListTagsForResource` API-Aufrufen pro Sekunde
Rate der `ListTrainingDatasets` Anfragen	50 TPS	Maximale Anzahl von `ListTrainingDatasets` API-Aufrufen pro Sekunde
Rate der `PutConfiguredAudienceModelPolicy` Anfragen	25 TPS	Maximale Anzahl von `PutConfiguredAudienceModelPolicy` API-Aufrufen pro Sekunde
Rate der `StartAudienceExportJob` Anfragen	1 TPS-Rate, 3 TPS-Burst	Maximale Anzahl von `StartAudienceExportJob` API-Aufrufen pro Sekunde
Rate der `StartAudienceGenerationJob` Anfragen	1 TPS-Rate, 5 TPS-Burst	Maximale Anzahl von `StartAudienceGenerationJob` API-Aufrufen pro Sekunde
Rate der `TagResource` Anfragen	10 TPS	Maximale Anzahl von `TagResource` API-Aufrufen pro Sekunde

Ressource	Ratenlimit	Beschreibung
Rate der `UntagResource` Anfragen	50 TPS	Maximale Anzahl von `UntagResource` API-Aufrufen pro Sekunde
Rate der `UpdateConfiguredAudienceModel` Anfragen	10 TPS	Maximale Anzahl von `UpdateConfiguredAudienceModel` API-Aufrufen pro Sekunde

Name	Standard	Anpas	Beschreibung
Aktive Zielgruppen-Exportaufträge pro Auftrag zur Zielgruppengenerierung	Jede unterstützte Region: 25	Nein	Die maximale Anzahl von aktiven Zielgruppen-Exportaufträgen für einen Job zur Zielgruppengenerierung
Ausstehende/laufende Zielgruppenexportaufträge pro Kunde	Jede unterstützte Region: 20	Nein	Die maximale Anzahl von ausstehenden/laufenden Zielgruppen-Exportaufträgen pro Kunde
Ausstehende/laufende Jobs zur Zielgruppengenerierung pro Kunde	Jede unterstützte Region: 10	Yes (Ja)	Die maximale Anzahl ausstehender oder laufender Jobs zur Zielgruppengenerierung pro Kunde
Ausstehende oder in Bearbeitung befindliche Zielgruppenmodelle pro Kunde	Jede unterstützte Region: 2	Ja	Die maximale Anzahl von ausstehenden/laufenden Schulungsaufträgen für Zielgruppenmodelle pro Kunde

ML-Kontingente für saubere Räume

Ressource	Standard	Beschreibung
Datensätze	pro Job	
Maximale Anzahl von Interaktionen	20 Milliarden	Maximale Anzahl von Interaktionen, die in Trainingsdaten zulässig sind. Größere Eingaben werden abgetastet.
Minimale Anzahl von Interaktionen	1 Mio.	
Maximale Anzahl verschiedener Benutzer für das Training mit ähnlichen Modellen	1 Mio.	Wenn mehr berücksichtigt werden, werden nur die besten 100 Millionen verwendet, geordnet nach der Anzahl der Interaktionen.
Mindestanzahl verschiedener Benutzer für das Training mit einem ähnlichen Modell	100 000	
Maximale Anzahl von Benutzern für den Export eines Jobs mit einem ähnlichen Segment (Zielgruppe)	10.000	
Maximale Anzahl verschiedener Elemente, die für das Modelltraining verwendet werden.	1 Mio.	Sie können bis zu 50 Millionen Elemente hinzufügen, es werden jedoch nur die beliebtesten 1 Million verwendet.
Maximale Anzahl von Feature-Spalten im Trainingsdatensatz.	10	

Ressource	Standard	Beschreibung
Mindestanzahl unterschiedlicher Elemente pro Benutzer	2	AWS Clean Rooms ML erfordert, dass jede Zeile oder jeder Benutzer zwei oder mehr Elemente enthält, einschließlich sich wiederholender Elemente.
Maximale Größe der Stammzielgruppe	500 000	
Mindestgröße des Startpublikums	500	Der Anbieter von Trainingsdaten kann diesen Wert auf einen niedrigen Wert von 25 festlegen.
APIs	pro Kunde	
Gesamtzahl der aktiven Trainingsdatensätze	500	
Gesamtzahl der aktiven Lookalike-Modelle (Zielgruppenmodelle)	500	
Gesamtzahl der aktiven konfigurierten Lookalike-Modelle (Zielgruppenmodelle)	10.000	
Gesamtzahl der abgeschlossenen Jobs zur Generierung von Lookalike-Segmenten (Audience)	Kein Limit	
Gesamtzahl der abgeschlossenen Aufträge für den Export von Lookalike-Segmenten (Audience)	Kein Limit	

Ressource	Standard	Beschreibung
Maximale Dauer eines Jobs zur Generierung eines Lookalike-Modells (Zielgrup penmodell)	1 Tag (24 Stunden)	
Maximale Dauer eines Jobs zur Generierung eines Lookalike-Segments (Audience)	10 Stunden	Nachdem Sie einen Seed bereitgestellt haben, benötigt Clean Rooms ML maximal 10 Stunden, um ein ähnliches Segment zu generieren.
Mindestprozentsatz für die Größe eines Segments (Zielgruppe)	1%	
Maximaler Prozentsatz für einen Bereich mit Segmentgr öße (Zielgruppe)	20 %	
Absolute Mindestgröße für einen Bereich mit Segmentgr öße (Zielgruppengröße)	1% der Anzahl der einzelnen Benutzer	
Maximale absolute Größe für ein Segment (Zielgrup pengröße)	20% der Anzahl der einzelnen Benutzer	

Dokumentenverlauf für das AWS Clean Rooms Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für beschrieben AWS Clean Rooms.

Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie den RSS-Feed abonnieren. Um RSS-Updates abonnieren zu können, muss für den von Ihnen verwendeten Browser ein RSS-Plug-In aktiviert sein.

Änderung	Beschreibung	Datum
Aktualisieren Sie die bestehende Richtlinie	Die folgende neue Berechtigung wurde der `AWSCleanRoomsFullAccessNoQuerying` verwalteten Richtlinie hinzugefügt:`cleanrooms:BatchGetSchemaAnalysisRule` .	13. Mai 2024
AWS Clean Rooms ML ist jetzt vollständig verfügbar	AWS Clean Rooms ML bietet eine Methode zur Verbesserung der Privatsphäre, mit der zwei Parteien ähnliche Benutzer in ihren Daten identifizieren können, ohne ihre Daten miteinander teilen zu müssen.	3. April 2024
Aktualisierung der bestehenden Richtlinie	Die Statement ID in der `AWSCleanRoomsFullAccess` verwalteten Richtlinie wurde von ConsolePickQueryResultsBucket bis aktualisiertSetQueryResultsBucket, um die Berechtig	21. März 2024

	ungen seit den Berechtig ungen besser darzustellen.	
Neue verwaltete Richtlinien für AWS Clean Rooms ML	Zwei neue verwaltet e Richtlinien wurden hinzugefügt: `AWSCleanR oomsMLReadOnlyAcce ss` und `AWSCleanR oomsMLFullAccess` .	29. November 2023
AWS Clean Rooms ML (Vorschau)	AWS Clean Rooms ML bietet eine Methode zur Verbesser ung des Datenschutzes, mit der zwei Parteien ähnliche Benutzer in ihren Daten identifizieren können, ohne ihre Daten miteinander teilen zu müssen.	29. November 2023
AWS Clean Rooms Differenz ierter Datenschutz (Vorschau)	Kunden können jetzt AWS Clean Rooms Differential Privacy verwenden, um die Privatsphäre ihrer Benutzer zu schützen.	29. November 2023
Konfiguration der Zahlung	Der Kollaborationserst eller kann nun entweder das Mitglied, das Abfragen ausführen kann, oder ein anderes Mitglied der Kollabora tion so konfigurieren, dass ihm die Rechenkosten für Abfragen in Rechnung gestellt werden.	14. November 2023

Laufzeit der Abfrage — Aktualisierung	Die maximale Dauer der Ausführung einer Abfrage vor dem Timeout wurde von 4 Stunden auf 12 Stunden aktualisiert.	06. Oktober 2023
AWS CloudFormation Ressourcen — aktualisieren	AWS Clean Rooms hat die folgenden neuen Ressourcen hinzugefügt: `AWS::CleanRooms::Membership` `ProtectedQueryOutputConfiguration` `AWS::CleanRooms::MembershipProtectedQueryResultConfiguration` , und`AWS::CleanRooms::Membership` `ProtectedQueryS3OutputConfiguration` .	07. September 2023
AWS CloudFormation Ressourcen — aktualisieren	AWS Clean Rooms hat die folgenden neuen Ressourcen hinzugefügt: `AWS::CleanRooms::AnalysisTemplate` und`AWS::CleanRooms::ConfiguredTable` `AnalysisRuleCustom` .	31. August 2023

Separate Fähigkeiten der Mitglieder	Der Ersteller der Kollaboration kann jetzt ein Mitglied als das Mitglied bestimmen, das Abfragen durchführen kann, und ein anderes Mitglied als das Mitglied, das Ergebnisse erhalten kann. Dadurch kann der Kollaborationsersteller sicherstellen, dass das Mitglied, das Abfragen durchführen kann, keinen Zugriff auf die Abfrageergebnisse hat.	30. August 2023
AWS Clean Rooms Glossar	Aktualisierung nur für die Dokumentation, um ein Glossar mit Begriffen hinzuzufügen. AWS Clean Rooms	30. August 2023
Support für Apache Iceberg Tabellen (Vorschau)	AWS Clean Rooms unterstützt jetzt Apache Iceberg Tabellen (Vorschau).	25. August 2023
Aktualisierung der Kontingente	Der Abschnitt Kontingente wurde aktualisiert, um das neue Standardkontingent für Mitgliedschaften pro Konto widerzuspiegeln.	9. August 2023

Aktualisierung der bestehenden Richtlinie	Die folgenden neuen Berechtigungen wurden der `AWSCleanRoomsFullAccessNoQuerying` verwalteten Richtlinie hinzugefügt:`cleanrooms:CreateAnalysisTemplate`, `cleanrooms:GetAnalysisTemplate`, `cleanrooms:UpdateAnalysisTemplate`, `cleanrooms:DeleteAnalysisTemplate`, `cleanrooms:ListAnalysisTemplates`, `cleanrooms:GetCollaborationAnalysisTemplate`, `cleanrooms:BatchGetCollaborationAnalysisTemplate`, und `cleanrooms:ListCollaborationAnalysisTemplates`.	31. Juli 2023

Analysevorlagen und benutzerdefinierte Analyseregel	AWS Clean Rooms unterstützt jetzt Analysevorlagen und die benutzerdefinierte Analyseregel. Analysevorlagen ermöglichen es Mitarbeitern, ihre eigene benutzerdefinierte SQL-Abfrage zu erstellen oder zu importieren, um sie in der Zusammenarbeit zu verwenden. Mit der benutzerdefinierten Analyseregel kann der Tabellenbesitzer benutzerdefinierte SQL-Abfragen für seine konfigurierten Tabellen genehmigen.	31. Juli 2023
Analyseregeln unterstützen die `OR` logische Bedingung	AWS Clean Rooms Analyseregeln unterstützen jetzt die `OR` logische Bedingung in der JOIN Klausel.	29. Juni 2023
CloudFormation Integration	AWS Clean Rooms integriert sich jetzt mit AWS CloudFormation.	15. Juni 2023
Analyse-Builder	Mitglieder, die Ergebnisse abfragen und empfangen können, können nun mithilfe der Benutzeroberfläche von Analysis Builder Abfragen für einige Tabellen ausführen, ohne SQL-Code schreiben zu müssen.	15. Juni 2023

SQL-Funktionen	Rein dokumentationsbezogenes Update zur Erläuterung der unterstützten SQL-Funktionen.	5. Mai 2023
Fehlersuche	Rein dokumentationsbezogenes Update, um einen Abschnitt zur Fehlerbehebung für häufig auftretende Probleme hinzuzufügen.	27. April 2023
Unterstützte Datentypen für AWS Clean Rooms	Update nur für die Dokumentation, um einen neuen Abschnitt hinzuzufügen, der die unterstützten AWS Glue Data Catalog Datentypen auflistet.	26. April 2023
Beispiele für AWS CloudTrail Ereignisse	Update nur für die Dokumentation, um Beispiele für CloudTrail Ereignisse für StartProtectedQuery (erfolgreich) und StartProtectedQuery (fehlgeschlagen) hinzuzufügen.	20. April 2023
Aktualisierung der bestehenden Richtlinie	Die folgenden neuen Berechtigungen wurden der `AWSCleanRoomsFullAccessNoQuerying` verwalteten Richtlinie hinzugefügt: `cleanrooms:ListTagsForResource` `cleanrooms:UntagResource`, und`cleanrooms:TagResource`. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien.	21. März 2023

Allgemeine Verfügbarkeit	AWS Clean Rooms ist jetzt allgemein verfügbar.	21. März 2023
Vorschau-Version	Vorschauversion des AWS Clean Rooms Benutzerh andbuchs	12. Januar 2023

AWS Clean Rooms Glossar

Konsultieren Sie dieses Glossar, um sich mit der verwendeten Terminologie vertraut zu machen. AWS Clean Rooms

Regel für die Aggregationsanalyse

Die Abfrageeinschränkung, die Abfragen ermöglicht, bei denen Analysen mithilfe vonCOUNT, oder aggregiert werdenSUM, und AVG zwar entlang optionaler Dimensionen. Diese Abfragen geben keine Informationen auf Zeilenebene preis.

Unterstützt Anwendungsfälle wie Kampagnenplanung, Messung der Medienreichweite, Häufigkeit und Konversionsmessung.

Andere Arten von Analyseregeln sind benutzerdefinierte Regeln und Listenregeln.

Regeln für die Analyse

Die Abfrageeinschränkungen, die einen bestimmten Abfragetyp autorisieren.

Der Analyseregeltyp bestimmt, welche Art von Analyse für die konfigurierte Tabelle ausgeführt werden kann. Jeder Typ hat eine vordefinierte Abfragestruktur. Über die Abfragesteuerelemente steuern Sie, wie Ihre Tabellenspalten in der Struktur verwendet werden können.

Die Arten von Analyseregeln sind Aggregation, Liste und Benutzerdefiniert.

Analysevorlage

Eine für die Zusammenarbeit spezifische, vorab genehmigte Abfrage, die wiederverwendet werden kann.

Unterstützt benutzerdefinierte SQL-Abfragen, die in unterstützt werden. AWS Clean Rooms

Kann überall dort Parameter enthalten, wo ein Literalwert normalerweise in einer SQL-Abfrage vorkommen könnte. Weitere Informationen zu unterstützten Parametertypen finden Sie unter Datentypen in der AWS Clean Rooms SQL-Referenz.

Analysevorlagen funktionieren nur mit der benutzerdefinierten Analyseregel.

C3R-Verschlüsselungsclient

Der Verschlüsselungsclient von Cryptographic Computing for Clean Rooms (C3R).

C3R ist ein clientseitiges Verschlüsselungs-SDK mit einer Befehlszeilenschnittstelle, das zum Verschlüsseln und Entschlüsseln von Daten verwendet wird.

Spalte mit klarem Text

Eine Spalte, die weder für ein noch für ein JOIN SQL-Konstrukt kryptografisch geschützt ist. SELECT

Klartextspalten können in jedem Teil der SQL-Abfrage verwendet werden.

Zusammenarbeit

Eine sichere logische Grenze, innerhalb AWS Clean Rooms derer Mitglieder SQL-Abfragen an konfigurierten Tabellen ausführen können.

Kollaborationen werden vom Ersteller der Kollaboration erstellt.

Nur Mitglieder, die zu der Kollaboration eingeladen wurden, können der Kollaboration beitreten.

Eine Kollaboration kann nur aus einem Mitglied bestehen, das Daten abfragen kann, einem Mitglied, das Ergebnisse erhalten kann, und einem Mitglied, das die Kosten für die Datenabfrage bezahlt.

Alle Mitglieder können die Liste der eingeladenen Teilnehmer der Kollaboration sehen, bevor sie der Kollaboration beitreten.

Ersteller der Kollaboration

Das Mitglied, das eine Kollaboration erstellt.

Pro Kollaboration gibt es nur einen Kollaborationsersteller.

Nur der Ersteller der Kollaboration kann Mitglieder aus der Kollaboration entfernen oder die Kollaboration löschen.

Konfigurierte Tabelle

Jede konfigurierte Tabelle stellt einen Verweis auf eine bestehende Tabelle in dar AWS Glue Data Catalog , die für die Verwendung in konfiguriert wurde. AWS Clean Rooms Eine konfigurierte Tabelle enthält eine Analyseregel, die bestimmt, wie die Daten verwendet werden können.

AWS Clean Rooms Unterstützt derzeit das Zuordnen von Daten, die in Amazon Simple Storage Service (Amazon S3) gespeichert sind und über katalogisiert wurden. AWS Glue

Weitere Informationen AWS Glue dazu finden Sie im AWS Glue Entwicklerhandbuch.

Konfigurierte Tabellen können einer oder mehreren Kollaborationen zugeordnet werden.

> **Note**
>
> AWS Clean Rooms unterstützt derzeit keine Amazon S3 S3-Bucket-Standorte, bei denen registriert ist AWS Lake Formation.

Benutzerdefinierte Analyseregel

Die Abfrageeinschränkung, die einen bestimmten Satz vorab genehmigter Abfragen (Analysevorlagen) oder eine bestimmte Gruppe von Konten zulässt, die Abfragen bereitstellen können, die Ihre Daten verwenden.

Unterstützt Anwendungsfälle wie First-Touch-Attribution, inkrementelle Analysen und Analysen zur Zielgruppenfindung.

Unterstützt differenziellen Datenschutz.

Entschlüsselung

Der Prozess der Rücktransformation verschlüsselter Daten in ihre ursprüngliche Form. Die Entschlüsselung kann nur durchgeführt werden, wenn Sie Zugriff auf den geheimen Schlüssel haben.

Differenzielle Privatsphäre

Eine mathematisch strenge Technik, die die Kollaborationsdaten vor Mitgliedern schützt, die Ergebnisse erhalten können, wenn sie mehr über eine bestimmte Person erfahren.

Verschlüsselung

Der Prozess, bei dem Daten mithilfe eines geheimen Werts, eines sogenannten Schlüssels, in eine Form kodiert werden, die zufällig erscheint. Ohne Zugriff auf den Schlüssel ist es unmöglich, den ursprünglichen Klartext zu ermitteln.

Spalte „Fingerabdruck“

Eine Spalte, die für ein JOIN SQL-Konstrukt kryptografisch geschützt ist.

Regel für die Listenanalyse

Die Abfrageeinschränkung, die Abfragen ermöglicht, die eine Attributanalyse der Überschneidung zwischen dieser Tabelle und den Tabellen des Mitglieds, das Abfragen durchführen kann, auf Zeilenebene ausgeben.

Unterstützt Anwendungsfälle wie Bereicherung und Zielgruppenbildung oder -unterbindung.

Mitglied

Ein AWS Kunde, der an einer Zusammenarbeit teilnimmt.

Ein Mitglied wird anhand seines identifiziert AWS-Konto.

Alle Mitglieder können Daten beitragen.

Mitglied, das Abfragen durchführen kann

Das Mitglied, das Daten in der Kollaboration abfragen kann.

Es gibt nur ein Mitglied, das Abfragen pro Kollaboration durchführen kann, und dieses Mitglied ist unveränderlich.

Ein Administratorbenutzer kann mithilfe von AWS Identity and Access Management (IAM-) Berechtigungen steuern, welche seiner IAM-Prinzipale (z. B. Benutzer oder Rollen) Daten in der Kollaboration abfragen können. Weitere Informationen finden Sie unter Erstellen Sie eine Servicerolle zum Lesen von Daten.

Mitglied, das Ergebnisse erhalten kann

Das Mitglied, das Abfrageergebnisse erhalten kann. Das Mitglied, das Ergebnisse erhalten kann, legt die Einstellungen für die Abfrageergebnisse für das Amazon S3 S3-Ziel und das Format der Abfrageergebnisse fest.

Es gibt nur ein Mitglied, das Ergebnisse pro Zusammenarbeit erhalten kann, und dieses Mitglied ist unveränderlich.

Das Mitglied zahlt die Kosten für die Berechnung von Abfragen

Das Mitglied, das für die Bezahlung der Kosten für die Query Compute verantwortlich ist.

Es gibt nur ein Mitglied, das für die Bezahlung der Abfrageberechnungskosten pro Zusammenarbeit verantwortlich ist, und dieses Mitglied ist unveränderlich.

Wenn der Ersteller der Kollaboration niemanden als das Mitglied angegeben hat, das die Kosten für die Abfrageverarbeitung bezahlt, ist das Mitglied, das Abfragen durchführen kann, der Standardzahler.

Das Mitglied, das die Kosten für die Query-Compute bezahlt, erhält eine Rechnung für die Abfragen, die im Rahmen der Kollaboration ausgeführt wurden.

Mitgliedschaften

Eine Ressource, die erstellt wird, wenn ein Mitglied einer Kollaboration beitritt.

Alle Ressourcen, die das Mitglied einer Kollaboration zuordnet, sind Teil der Mitgliedschaft oder mit der Mitgliedschaft verknüpft.

Nur das Mitglied, dem die Mitgliedschaft gehört, kann Ressourcen in dieser Mitgliedschaft hinzufügen, entfernen oder bearbeiten.

Versiegelte Spalte

Eine Spalte, die für ein SELECT SQL-Konstrukt kryptografisch geschützt ist.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.