aws

Guida per l'utente

AWS Clean Rooms

AWS Clean Rooms: Guida per l'utente

Table of Contents

Che cos'è AWS Clean Rooms?

AWS Clean Rooms aiuta te e i tuoi partner ad analizzare e collaborare sui set di dati collettivi per ottenere nuove informazioni senza rivelare i dati sottostanti gli uni agli altri. Puoi utilizzare AWS Clean Rooms uno spazio di lavoro collaborativo sicuro per creare le tue camere bianche in pochi minuti e iniziare ad analizzare i tuoi set di dati collettivi con pochi passaggi. Puoi scegliere i partner con cui collaborare, selezionare i relativi set di dati e configurare le restrizioni per i partecipanti.

Con AWS Clean Rooms, puoi collaborare con migliaia di aziende che già lo utilizzano. AWS La collaborazione non richiede lo spostamento AWS o il caricamento dei dati su un'altra piattaforma. Quando esegui query, AWS Clean Rooms legge i dati dalla loro posizione originale e applica regole di analisi integrate per aiutarti a mantenere il controllo sui dati.

AWS Clean Rooms fornisce controlli integrati per l'accesso ai dati e controlli di supporto all'audit che è possibile configurare. Questi controlli includono:

- Regole di analisi per limitare le query SQL e fornire vincoli di output
- Elaborazione crittografica per Clean Rooms mantenere i dati crittografati, anche durante l'elaborazione delle query, per rispettare rigorose politiche di gestione dei dati
- Registri di interrogazione per esaminare le domande e supportare gli audit
- Privacy differenziale per la protezione dai tentativi di identificazione degli utenti. AWS Clean Rooms Differential Privacy è una funzionalità completamente gestita che protegge la privacy degli utenti con tecniche basate su basi matematiche e controlli intuitivi che puoi applicare con pochi clic.
- AWS Clean Rooms ML per consentire a due parti di identificare utenti simili nei propri dati senza la necessità di condividere i propri dati tra loro. La prima parte crea e configura un modello simile a partire dai propri dati di addestramento. La seconda parte utilizza i propri dati iniziali per una collaborazione e crea un segmento simile a quello dei dati di addestramento.

Il video seguente spiega di più su. AWS Clean Rooms

AWS Clean Rooms

Sei un AWS Clean Rooms utente alle prime armi?

Se sei un utente principiante di AWS Clean Rooms, ti consigliamo di iniziare leggendo le seguenti sezioni:

Come funziona AWS Clean Rooms

Il seguente flusso di lavoro presuppone che:

- Il membro della collaborazione ha già caricato le proprie tabelle di dati su Amazon S3 e creato una AWS Glue tabella.
- (Facoltativo) Solo per le tabelle di dati crittografate, il membro della collaborazione ha già preparato tabelle di dati crittografate utilizzando il client di crittografia C3R.

In sintesi, il flusso di lavoro per AWS Clean Rooms è il seguente:

1. Il creatore della collaborazione svolge le seguenti attività:
   - Crea una collaborazione.
   - Invita uno o più membri alla collaborazione.
   - Assegna abilità ai membri, ad esempio il membro che può eseguire interrogazioni e il membro che può ricevere risultati.

     Se il creatore della collaborazione è anche il membro che può ricevere i risultati, specifica la destinazione e il formato dei risultati della query. Forniscono inoltre un ruolo di servizio Amazon Resource Name (ARN) per scrivere i risultati nella destinazione dei risultati della query.
   - Configura quale membro è responsabile del pagamento dei costi di elaborazione delle query nell'ambito della collaborazione.
2. Il membro invitato si unisce alla collaborazione creando una risorsa di appartenenza.

   Se il membro invitato è il membro che può ricevere i risultati, specifica la destinazione e il formato dei risultati della query. Forniscono inoltre un ruolo di servizio ARN da scrivere nella destinazione dei risultati della query.

Se il membro invitato è il membro responsabile del pagamento dei costi di elaborazione delle query, accetta le proprie responsabilità di pagamento prima di aderire alla collaborazione.

3. Il membro configura una AWS Glue tabella esistente da utilizzare in. AWS Clean Rooms(Questo passaggio può essere eseguito prima o dopo l'adesione a una collaborazione, a meno che non si utilizzi Cryptographic Computing forClean Rooms.)

> **Note**
>
> AWS Clean Rooms supporta AWS Glue tabelle. Per ulteriori informazioni sull'inserimento dei dati AWS Glue, consultaFase 3: carica la tabella di dati su Amazon S3.

   1. Il membro assegna un nome alla tabella configurata e sceglie quali colonne utilizzare nella collaborazione.
   2. Il membro configura una delle seguenti regole di analisi nella tabella configurata:
      - Regola di analisi di aggregazione o regola di analisi dell'elenco: per controllare il tipo di analisi che può essere eseguita sulla tabella.
      - Regola di analisi personalizzata: consente un set specifico di query preapprovate o un set specifico di account in grado di fornire query che utilizzano i dati dell'utente. Consente al membro di attivare la privacy differenziale per proteggersi dai tentativi di identificazione dell'utente.

> **Note**
>
> Il membro può configurare la regola di analisi in qualsiasi momento prima di associare le tabelle configurate alla collaborazione.

4. Il membro associa le tabelle configurate alla collaborazione e assegna AWS Clean Rooms un ruolo di servizio per accedere alle proprie AWS Glue tabelle.

> **Note**
>
> Questo ruolo di servizio dispone delle autorizzazioni per le tabelle. Il ruolo di servizio può essere assunto solo eseguendo AWS Clean Rooms le query consentite per conto del membro che può eseguire le query. Nessun membro della collaborazione (diverso dal proprietario dei dati) ha accesso alle tabelle sottostanti della collaborazione. Il

proprietario dei dati può attivare la privacy differenziale per rendere le proprie tabelle disponibili per l'interrogazione da parte di altri membri.

5. Il membro che può eseguire le query esegue le query SQL sulle tabelle configurate.

   Le query possono essere eseguite solo se il membro responsabile del pagamento dei costi di elaborazione delle query ha aderito alla collaborazione come membro attivo.

   Le regole di analisi e i vincoli di output vengono applicati automaticamente. AWS Clean Rooms restituisce solo i risultati conformi alle regole di analisi definite nel passaggio 3.b.

   Per le interrogazioni su dati crittografati, il membro che può ricevere risultati riceve l'output crittografato da AWS Clean Rooms cui deve essere decrittografato (vedere il passaggio 8).

6. Il membro che può ricevere risultati esamina i risultati nella AWS Clean Rooms console o nel bucket Amazon S3 specificato.
7. Al membro che paga i costi di elaborazione delle query viene addebitato il costo delle query eseguite nell'ambito della collaborazione.
8. (Facoltativo) Solo per le tabelle di dati crittografate, il membro che può ricevere i risultati decrittografa i risultati della query eseguendo il client di crittografia C3R in modalità di decrittografia.

Servizi correlati

Quanto segue è correlato a: Servizi AWS AWS Clean Rooms

- Amazon S3

  I membri della collaborazione possono archiviare i dati che inseriscono AWS Clean Rooms in Amazon S3.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  Preparazione delle tabelle di dati per le interrogazioni in AWS Clean Rooms

  Che cos'è Amazon S3? nella Guida per l'utente di Amazon Simple Storage Service
- AWS Glue

I membri della collaborazione possono creare AWS Glue tabelle dai propri dati in Amazon S3 da utilizzare in. AWS Clean Rooms

Per ulteriori informazioni, consulta i seguenti argomenti:

Preparazione delle tabelle di dati per le interrogazioni in AWS Clean Rooms

Che cos'è AWS Glue? nella Guida per gli sviluppatori di AWS Glue

- AWS CloudFormation

  Crea le seguenti risorse in AWS CloudFormation: collaborazioni, tabelle configurate, associazioni di tabelle configurate e appartenenze

  Per ulteriori informazioni, consulta Creazione di AWS Clean Rooms risorse con AWS CloudFormation.

- AWS CloudTrail

  Utilizzalo AWS Clean Rooms con CloudTrail i log per migliorare l'analisi delle attività. Servizio AWS

  Per ulteriori informazioni, consulta Registrazione di chiamate API AWS Clean Rooms con AWS CloudTrail.

Accesso AWS Clean Rooms

È possibile accedere AWS Clean Rooms tramite le seguenti opzioni:

- Direttamente tramite la AWS Clean Rooms console all'indirizzo https://console.aws.amazon.com/cleanrooms/.
- A livello di codice tramite l'API. AWS Clean Rooms Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS Clean Rooms .

Prezzi per AWS Clean Rooms

Per informazioni sui prezzi, consulta Prezzi di AWS Clean Rooms.

Fatturazione per AWS Clean Rooms

AWS Clean Rooms offre al creatore della collaborazione la possibilità di configurare quale membro paga i costi di elaborazione delle query nell'ambito della collaborazione.

Nella maggior parte dei casi, il membro che può eseguire le query e il membro che paga i costi di elaborazione delle query sono gli stessi. Tuttavia, se il membro che può eseguire le query e il membro che paga i costi di elaborazione delle query sono diversi, quando il membro che può eseguire le query esegue le query sulla propria risorsa di appartenenza, viene fatturata la risorsa di appartenenza del membro che paga i costi di calcolo delle query.

Il membro che paga i costi di calcolo delle query non vede alcun evento relativo alle query eseguite nella propria cronologia CloudTrail degli eventi perché il pagatore non è né colui che esegue le query né il proprietario della risorsa su cui vengono eseguite le query. Tuttavia, il pagatore vede le fatture generate sulla propria risorsa di iscrizione per tutte le domande eseguite dal membro che può eseguire le query nell'ambito della collaborazione.

Per ulteriori informazioni su come creare una collaborazione e configurare il pagamento dei costi di calcolo delle query da parte del membro, consulta. Crea una collaborazione

Regole di analisi in AWS Clean Rooms

Per abilitare una tabella da utilizzare AWS Clean Rooms per l'analisi collaborativa, il membro della collaborazione deve configurare una regola di analisi.

Una regola di analisi è un controllo che migliora la privacy che ogni proprietario dei dati imposta su una tabella configurata. Una regola di analisi determina in che modo la tabella configurata può essere analizzata.

La regola di analisi è un controllo a livello di account sulla tabella configurata (una risorsa a livello di account) e viene applicata in qualsiasi collaborazione in cui è associata la tabella configurata. Se non è configurata alcuna regola di analisi, la tabella configurata può essere associata alle collaborazioni ma non può essere interrogata. Le query possono fare riferimento solo a tabelle configurate con lo stesso tipo di regola di analisi.

Per configurare una regola di analisi, è necessario innanzitutto selezionare un tipo di analisi e quindi specificare la regola di analisi. Per entrambi i passaggi, è necessario considerare il caso d'uso che si desidera abilitare e il modo in cui si desidera proteggere i dati sottostanti.

AWS Clean Rooms applica i controlli più restrittivi su tutte le tabelle configurate a cui fa riferimento una query.

Gli esempi seguenti illustrano i controlli restrittivi.

Example Controllo restrittivo: vincolo di output

- Il collaboratore A ha un vincolo di output sulla colonna identifier di 100.
- Il collaboratore B ha un vincolo di output sulla colonna identifier pari a 150.

  Una query di aggregazione che fa riferimento a entrambe le tabelle configurate richiede almeno 150 valori distinti di identifier all'interno di una riga di output per essere visualizzata nell'output della query. L'output della query non indica che i risultati siano stati rimossi a causa del vincolo di output.

Example Controllo restrittivo: modello di analisi non approvato

- Collaborator A ha consentito un modello di analisi con una query che fa riferimento alle tabelle configurate di Collaborator A e Collaborator B nelle relative regole di analisi personalizzate.
- Il collaboratore B non ha consentito il modello di analisi.

Poiché il Collaboratore B non ha consentito il modello di analisi, il membro che può eseguire la query non può eseguire quel modello di analisi.

Tipi di regole di analisi

Esistono tre tipi di regole di analisi: aggregazione, elenco e personalizzata. Le tabelle seguenti confrontano i tipi di regole di analisi. Ogni tipo ha una sezione separata che descrive la specificazione della regola di analisi.

Le tabelle seguenti mostrano un riepilogo di confronto dei tipi di regole di analisi.

Casi di utilizzo supportati

Le tabelle seguenti mostrano un riepilogo di confronto dei casi d'uso supportati per ogni tipo di regola di analisi.

Caso d'uso	Aggregazione	Elenco	Personalizza
Analisi supportate	Query che aggregano le statistiche utilizzando le funzioni COUNT, SUM e AVG in dimensioni opzionali	Query che generano elenchi a livello di riga delle sovrapposizioni tra più tabelle	Qualsiasi analisi personalizzata purché il modello di analisi o il creatore dell'analisi siano stati esaminati e consentiti
Casi d'uso comuni	Analisi, misurazione, attribuzione dei segmenti	Arricchimento, costruzione di segmenti	Attribuzione immediata, analisi incrementali,

Caso d'uso	Aggregazione	Elenco	Personalizza
			scoperta del pubblico
Costrutti SQL	• Istruzioni JOIN: INNER JOIN • Funzioni aggregate: COUNT/ COUNT DISTINCT, SUM/ SUM DISTINCT e AVG • Funzioni scalari: sottoinsieme limitato	• Istruzioni JOIN: INNER JOIN • Funzioni scalari: nessuna	La maggior parte delle funzioni SQL e dei costrutti SQL sono disponibili con il comando SELECT
Sottoquery ed espressioni di tabella comuni (CTE)	No	No	Sì
Modelli di analisi	No	No	Sì

Controlli supportati

Le tabelle seguenti mostrano un riepilogo di confronto del modo in cui ogni tipo di regola di analisi protegge i dati sottostanti.

Controllo	Aggregazione	Elenco	Personalizza
Meccanismo di controllo	Controlla come i dati della tabella possono essere utilizzati in una query (Ad esempio, consenti COUNT e SUM della colonna hashed_email.)	Controlla come i dati della tabella possono essere utilizzati in una query (Ad esempio, consenti l'uso della colonna hashed_email solo per l'unione.)	Controlla quali interrogazioni possono essere eseguite sulla tabella (Ad esempio, consenti solo le interrogazioni definite nei modelli di analisi «Query personalizzata 1".)
Tecniche integrate di miglioramento della privacy	• Fiammifero cieco • Aggregazione richiesta • Soglia minima di	• Partita alla cieca • Sovrapposizione richiesta • Struttura di	Privacy differenziale

Controllo	Aggregazione	Elenco	Personalizza
	aggregazione >= • 2 Struttura di interrogazione predefinita	interrogazione predefinita	
Esamina la query prima che possa essere eseguita	No	No	Sì, utilizzando modelli di analisi

Per ulteriori informazioni sulle regole di analisi disponibili in AWS Clean Rooms, consultate i seguenti argomenti.

- Regola di analisi di aggregazione
- Regola di analisi delle liste
- Regola di analisi personalizzata in AWS Clean Rooms

Regola di analisi di aggregazione

InAWS Clean Rooms, una regola di analisi di aggregazione genera statistiche aggregate utilizzando le funzioni COUNT, SUM e/o AVG insieme a dimensioni opzionali. Quando la regola di analisi di aggregazione viene aggiunta a una tabella configurata, consente al membro che può eseguire query sulla tabella configurata.

La regola di analisi di aggregazione supporta casi d'uso come la pianificazione delle campagne, la copertura dei media, la misurazione della frequenza e l'attribuzione.

La struttura e la sintassi delle query supportate sono definite in. Struttura e sintassi delle interrogazioni di aggregazione

I parametri della regola di analisi, definita inRegola di analisi dell'aggregazione: controlli di interrogazione, includono i controlli di interrogazione e i controlli dei risultati delle query. I suoi controlli di interrogazione includono la possibilità di richiedere che una tabella configurata sia aggiunta ad almeno una tabella configurata di proprietà del membro che può eseguire query, direttamente o in modo transitivo. Questo requisito ti consente di garantire che la query venga eseguita sull'intersezione (INNERJOIN) della tua tabella e della loro.

Struttura e sintassi delle interrogazioni di aggregazione

Le query su tabelle che dispongono di una regola di analisi di aggregazione devono rispettare la sintassi seguente.

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

Nella tabella seguente vengono illustrate tutte le espressioni elencate nella sintassi precedente.

Expression	Definizione	Esempi
select_aggregate_function_expression	Un elenco separato da virgole contenente le seguenti espressioni: • select_aggregation_function_expression • select_aggregate_expression **Note** Deve essercene almeno una select_aggregation_function_expression in. select_aggregate_expression	SELECT SUM(PRICE), user_segment
select_aggregation_function_expression	Una o più funzioni di aggregazione supportate applicate a una o più colonne. Sono consentite solo le colonne come argomenti delle funzioni di aggregazione. **Note** Deve essercene almeno uno select_ag	AVG(PRICE) COUNT(DISTINCT user_id)

Expression	Definizione	Esempi
	`gregation _function _expression` in. `select_ag gregate_e xpression`	

`select_grouping_co lumn_expression`	Un'espressione che può contenere qualsiasi espressio ne utilizzando quanto segue:
	• Nomi di colonna delle tabelle
	• Funzioni scalari supportate
	• Stringhe letterali
	• Letterali numerici
	
	Note
	`select_ag gregate_e xpression` può assegnare un alias alle colonne con o senza il parametro. `AS` Per ulteriori informazi oni, vedere AWS Clean RoomsSQL Reference.
		`TRUNC(timestampCol umn)`
		
		`UPPER(campaignName)`

Expression	Definizione	Esempi
table_expression	Una tabella, o unione di tabelle, che collega espressioni condizionali di join con `join_condition` . `join_condition` restituisce un valore booleano. I `table_expression` supporti: • Un JOIN tipo specifico (INNERJOIN) • La condizione di confronto dell'uguaglianza all'interno di a `join_condition` (=) • Operatori logici (AND,0R).	`FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2`

Expression	Definizione	Esempi
where_expression	Un'espressione condizionale che restituisce un valore booleano. Può essere composta dai seguenti elementi: • Nomi di colonna delle tabelle • Funzioni scalari supportate • Operatori matematici • Stringhe letterali • Letterali numerici Le condizioni di confronto supportate sono ()=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL. Gli operatori logici supportati sono (AND, OR). where_expression È facoltativo.	WHERE where_condition WHERE price > 100 WHERE TRUNC(timestampColumn) = '1/1/2022' WHERE timestampColumn = timestampColumn2 - 14
group_by_expression	Un elenco di espressioni separate da virgole che soddisfano i requisiti per. select_grouping_column_expression	GROUP BY TRUNC(timestampColumn), UPPER(campaignName), segment

Expression	Definizione	Esempi
having_expression	Un'espressione condizionale che restituisce un valore booleano. Hanno una funzione di aggregazione supportata applicata a una singola colonna (ad esempio`SUM(price)`) e vengono confrontati con un valore letterale numerico. Le condizioni supportate sono (). `=, >, <, <=, >=, <>, !=` Gli operatori logici supportati sono (`AND, OR`). `having_expression` È facoltativo.	`HAVING SUM(SALES) > 500`

Expression	Definizione	Esempi
order_by_expression	Un elenco di espressioni separate da virgole compatibili con gli stessi requisiti definiti in `select_aggregate_expression` precedenza. È `order_by_expression` facoltativo. **Note** `order_by_expression` permessi `ASC` e `DESC` parametri. Per ulteriori informazioni, vedere i parametri ASC DESC nel AWS Clean Rooms riferimento SQL.	`ORDER BY SUM(SALES), UPPER(campaignName)`

Per quanto riguarda la struttura e la sintassi delle query di aggregazione, tieni presente quanto segue:

- I comandi SQL diversi da quelli non SELECT sono supportati.
- Le sottoquery e le espressioni di tabella comuni (ad esempioWITH) non sono supportate.
- Gli operatori che combinano più interrogazioni (ad esempioUNION) non sono supportati.
- TOPLIMIT, e OFFSET i parametri non sono supportati.

Regola di analisi dell'aggregazione: controlli di interrogazione

Con i controlli di interrogazione di aggregazione, puoi controllare come le colonne della tabella vengono utilizzate per interrogare la tabella. Ad esempio, è possibile controllare quale colonna viene

utilizzata per l'unione, quale colonna può essere contata o quale colonna può essere utilizzata nelle WHERE istruzioni.

Nelle sezioni seguenti viene illustrato ogni controllo.

Argomenti

Controlli di aggregazione

Utilizzando i controlli di aggregazione, è possibile definire quali funzioni di aggregazione consentire e a quali colonne devono essere applicate. Le funzioni di aggregazione possono essere utilizzate nelle espressioni SELECTHAVING, e. ORDER BY

Controllo	Definizione	Utilizzo
`aggregateColumns`	Colonne di colonne di tabella configurate che è possibile utilizzare all'interno delle funzioni di aggregazione.	`aggregateColumns` può essere utilizzato all'interno di una funzione di aggregazi one nelle SELECT espressio niHAVING, e ORDERBY. Alcuni `aggregateColumns` possono anche essere classificati come `joinColum n` (definiti in seguito). `aggregateColumn` Given non può anche essere classificato come `dimension Column` (definito in seguito).
`function`	Le funzioni COUNT, SUM e AVG consentite possono	`function`può essere applicato a qualsiasi

Controllo	Definizione	Utilizzo
	essere utilizzate in aggiunta a. `aggregateColumns`	`aggregateColumns` oggetto ad esso associato.

Unisci i controlli

Una `JOIN` clausola viene utilizzata per combinare righe di due o più tabelle, in base a una colonna correlata tra di esse.

È possibile utilizzare i controlli Join per controllare il modo in cui la tabella può essere unita ad altre tabelle in. `table_expression` AWS Clean Roomssupporta solo INNERJOIN. INNERJOINIe istruzioni possono utilizzare solo colonne che sono state classificate in modo esplicito come una delle regole di analisi, `joinColumn` in base ai controlli definiti dall'utente.

INNERJOINDevono operare su una `joinColumn` tabella configurata e su un'altra tabella configurata nella collaborazione. `joinColumn` Sei tu a decidere quali colonne della tabella possono essere utilizzate come`joinColumn`.

Ogni condizione di corrispondenza all'interno della ON clausola è richiesta per utilizzare la condizione di confronto di uguaglianza (=) tra due colonne.

Le condizioni di corrispondenza multiple all'interno di una ON clausola possono essere:

- Combinato utilizzando l'operatore logico `AND`
- Separato utilizzando l'operatore `OR` logico

> **Note**
>
> Tutte le JOIN condizioni di partita devono corrispondere a una riga su ciascun lato delJOIN. Anche tutti i condizionali collegati da un operatore logico `OR` o da un operatore `AND` logico devono rispettare questo requisito.

Di seguito è riportato un esempio di interrogazione con un operatore logico`AND`.

```
SELECT some_col, other_col
```

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

Di seguito è riportato un esempio di interrogazione con un operatore OR logico.

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

Controllo	Definizione	Utilizzo
`joinColumns`	Le colonne (se presenti) che si desidera consentire al membro che può eseguire la query di utilizzare nell'INNE RJOINistruzione.	Uno specifico `joinColumn` può anche essere classificato come `aggregateColumn` (vediControlli di aggregazione). La stessa colonna non può essere utilizzata sia come che come `joinColumn` `dimensionColumns` (vedi più avanti). A meno che non sia stata anche classificata come una`aggregateColumn` , a non `joinColumn` può essere utilizzata in altre parti della query diverse da. INNER JOIN
`joinRequired`	Controlla se hai bisogno di un messaggio INNER JOIN con una tabella configurata dal membro che può eseguire la query.	Se si abilita questo parametro , INNER JOIN è necessari o un. Se non abiliti questo parametro, an INNER JOIN è facoltativo.

Controllo	Definizione	Utilizzo
		Supponendo che questo parametro sia abilitato, il membro che può eseguire la query deve includere una tabella di sua proprietà in. INNER JOIN Devono unire JOIN la propria tabella alla propria, direttamente o transitivamente (ossia, unire la propria tabella a un'altra tabella, che a sua volta è unita al tavolo dell'utente).

Di seguito è riportato un esempio di transitività.

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

> **Note**
>
> Il membro che può eseguire la query può anche utilizzare il `joinRequired` parametro. In tal caso, la query deve unire la propria tabella ad almeno un'altra tabella.

Controlli dimensionali

I controlli delle dimensioni controllano la colonna lungo la quale le colonne di aggregazione possono essere filtrate, raggruppate o aggregate.

Controllo	Definizione	Utilizzo
`dimensionColumns`	Le colonne (se presenti) che consenti al membro che può	A `dimensionColumn` può essere usato in

Controllo	Definizione	Utilizzo
	eseguire la query di utilizzare inSELECT,, WHERE e. GROUP BY ORDER BY	SELECT (`select_grouping_column_expression`)WHERE, GROUPBY, e ORDERBY. La stessa colonna non può essere sia a `dimensionColumn` che a `joinColumn` e/o a `anaggregateColumn` .

Funzioni scalari

Le funzioni scalari controllano quali funzioni scalari possono essere utilizzate nelle colonne dimensionali.

Controllo	Definizione	Utilizzo
`scalarFunctions`	Le funzioni scalari che possono essere utilizzate `dimensionColumns` nella query.	Speciifica le funzioni scalari (se presenti) su cui è possibile applicare (ad esempioCAST). `dimensionColumns` Le funzioni scalari non possono essere utilizzate sopra altre funzioni o all'interno di altre funzioni. Gli argomenti delle funzioni scalari possono essere colonne, stringhe letterali o letterali numerici.

Sono supportate le seguenti funzioni scalari:

- Funzioni matematiche: ABS, CEILING, FLOOR, LOG, LN, ROUND, SQRT

- Funzioni di formattazione dei tipi di dati — CAST, CONVERT, TO_CHAR, TO_DATE, TO_NUMBER, TO_TIMESTAMP
- Funzioni di stringa: LOWER, UPPER, TRIM, RTRIM, SUBSTRING
  - Per RTRIM, i set di caratteri personalizzati da tagliare non sono consentiti.
- Espressioni condizionali — COALESCE
- Funzioni di data: EXTRACT, GETDATE, CURRENT_DATE, DATEADD
- Altre funzioni: TRUNC

Per maggiori dettagli, consulta AWS Clean RoomsSQL Reference.

Regola di analisi di aggregazione: controlli dei risultati delle query

Con i controlli dei risultati delle query di aggregazione, è possibile controllare quali risultati vengono restituiti specificando una o più condizioni che ogni riga di output deve soddisfare per poter essere restituita. AWS Clean Roomssupporta vincoli di aggregazione sotto forma di. `COUNT (DISTINCT column) >= X` Questo modulo richiede che ogni riga aggreghi almeno X valori distinti di una scelta dalla tabella configurata (ad esempio, un numero minimo di valori distinti). `user_id` Questa soglia minima viene applicata automaticamente, anche se la query inviata stessa non utilizza la colonna specificata. Vengono applicate collettivamente a ogni tabella configurata nell'interrogazione effettuata dalle tabelle configurate di ciascun membro della collaborazione.

Ogni tabella configurata deve avere almeno un vincolo di aggregazione nella regola di analisi. I proprietari delle tabelle configurate possono aggiungerne di più `columnName` e associarle `minimum` e vengono applicate collettivamente.

Vincoli di aggregazione

I vincoli di aggregazione controllano quali righe dei risultati della query vengono restituite. Per essere restituita, una riga deve soddisfare il numero minimo specificato di valori distinti in ogni colonna specificata nel vincolo di aggregazione. Questo requisito si applica anche se la colonna non è menzionata esplicitamente nella query o in altre parti della regola di analisi.

Controllo	Definizione	Utilizzo
`columnName`	Il `aggregateColumn` that viene utilizzato nella condizion	Può essere qualsiasi colonna nella tabella configurata.

Controllo	Definizione	Utilizzo
	e che ogni riga di output deve soddisfare.	
`minimum`	Il numero minimo di valori distinti associati `aggregateColumn` che deve avere la riga di output (ad esempio, COUNT DISTINCT) per poter essere restituita nei risultati della query.	`minimum`Deve essere almeno il valore 2.

Struttura delle regole di analisi dell'aggregazione

L'esempio seguente mostra una struttura predefinita per una regola di analisi di aggregazione.

Nell'esempio seguente, *`MyTable`*fa riferimento alla tabella di dati. È possibile sostituire ogni *`segnaposto di input dell'utente`* con le proprie informazioni.

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

Regola di analisi dell'aggregazione: esempio

L'esempio seguente dimostra come due aziende possono collaborare AWS Clean Rooms utilizzando l'analisi di aggregazione.

L'azienda A dispone di dati sui clienti e sulle vendite. L'azienda A è interessata a comprendere l'attività di restituzione dei prodotti. La società B è uno dei rivenditori della società A e dispone di dati sui resi. La società B dispone inoltre di attributi di segmento relativi ai clienti utili all'azienda A (ad esempio, ha acquistato prodotti correlati, utilizza il servizio clienti del rivenditore). L'azienda B non desidera fornire dati sui resi dei clienti a livello di riga e informazioni sugli attributi. La società B desidera solo abilitare una serie di query per l'azienda A per ottenere statistiche aggregate sui clienti che si sovrappongono a una soglia minima di aggregazione.

La società A e la società B decidono di collaborare in modo che l'azienda A possa comprendere l'attività di restituzione dei prodotti e fornire prodotti migliori presso l'azienda B e altri canali.

Per creare la collaborazione ed eseguire un'analisi di aggregazione, le aziende eseguono le seguenti operazioni:

1. L'azienda A crea una collaborazione e crea un'iscrizione. La collaborazione ha l'azienda B come altro membro della collaborazione. La società A consente la registrazione delle interrogazioni nell'ambito della collaborazione e la registrazione delle interrogazioni nel proprio account.
2. L'azienda B crea un'appartenenza alla collaborazione. Consente la registrazione delle interrogazioni nel proprio account.
3. La società A crea una tabella configurata per le vendite.
4. La società A aggiunge la seguente regola di analisi di aggregazione alla tabella configurata per le vendite.

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

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

`aggregateColumns`— La società A desidera contare il numero di clienti unici nella sovrapposizione tra i dati di vendita e i dati sui resi. L'azienda A desidera inoltre sommare il numero di `purchases` prodotti da confrontare con il numero di`returns`.

`joinColumns`— La società A intende utilizzare questa tecnica `identifier` per abbinare i clienti provenienti dai dati di vendita ai clienti provenienti dai dati sui resi. Ciò aiuterà l'Azienda A ad abbinare i resi agli acquisti giusti. Inoltre, aiuta l'azienda A a segmentare i clienti che si sovrappongono.

`dimensionColumns`— La società A filtra in base `dimensionColumns` al prodotto specifico, confronta gli acquisti e i resi in un determinato periodo di tempo, assicura che la data

di restituzione sia successiva a quella del prodotto e aiuta a segmentare i clienti che si sovrappongono.

`scalarFunctions`— La società A seleziona la funzione `CAST` scalare per aiutare ad aggiornare i formati dei tipi di dati, se necessario, in base alla tabella configurata che la società A associa alla collaborazione. Aggiunge inoltre funzioni scalari per facilitare la formattazione delle colonne, se necessario.

`outputConstraints`— La società A stabilisce vincoli minimi di output. Non è necessario limitare i risultati perché all'analista è consentito visualizzare i dati a livello di riga dalla tabella delle vendite

> **Note**
>
> La società A non include `joinRequired` nella regola di analisi. Fornisce la flessibilità necessaria all'analista per interrogare solo la tabella delle vendite.

5. La società B crea una tabella configurata per i resi.
6. La società B aggiunge la seguente regola di analisi di aggregazione alla tabella configurata per i resi.

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

```
  "joinColumns": [
    "hashedemail"
  ],
  "joinRequired": [
    "QUERY_RUNNER"
  ],
  "dimensionColumns": [
    "state",
    "popularpurchases",
    "customerserviceuser",
    "productline",
    "returndate"
  ],
  "scalarFunctions": [
    "CAST",
    "LOWER",
    "UPPER",
    "TRUNC"
  ],
  "outputConstraints": [
    {
      "columnName": "hashedemail",
      "minimum": 100,
      "type": "COUNT_DISTINCT"
    },
    {
      "columnName": "producttype",
      "minimum": 2,
      "type": "COUNT_DISTINCT"
    }
  ]
}
```

`aggregateColumns`— La società B consente alla società A di effettuare una somma `returns` da confrontare con il numero di acquisti. Hanno almeno una colonna aggregata perché abilitano una query aggregata.

`joinColumns`— La società B consente alla società A di aderire per `identifier` abbinare i clienti provenienti dai dati di restituzione ai clienti dai dati di vendita. `identifier`i dati sono particolarmente sensibili e la loro presenza `joinColumn` garantisce che non vengano mai inseriti in una query.

`joinRequired`— L'azienda B richiede che le domande sui dati di restituzione vengano sovrapposte ai dati di vendita. Non vogliono consentire all'azienda A di interrogare tutte le persone nel loro set di dati. Hanno anche concordato tale restrizione nel loro accordo di collaborazione.

`dimensionColumns`— La società B consente alla società A di filtrare e raggruppare per `statepopularpurchases`, e `customerserviceuser` si tratta di attributi unici che potrebbero aiutare a effettuare l'analisi per la società A. La società B consente all'azienda A di utilizzare per filtrare l'output in base `returndate` a `returndate` ciò che si verifica successivamente`purchasedate`. Con questo filtraggio, l'output è più accurato per valutare l'impatto della modifica del prodotto.

`scalarFunctions`— L'azienda B consente quanto segue:

- TRUNC per le date
- LOWER e UPPER nel caso in `producttype` cui i dati siano immessi in un formato diverso
- CASTse la società A deve convertire i tipi di dati delle vendite in modo che corrispondano ai tipi di dati dei resi

La società A non abilita altre funzioni scalari perché non ritiene che siano necessarie per le query.

`outputConstraints`— L'azienda B stabilisce vincoli minimi di output `hashedemail` per contribuire a ridurre la capacità di reidentificare i clienti. Aggiunge inoltre un vincolo minimo di output `producttype` per ridurre la capacità di identificare nuovamente i prodotti specifici che sono stati restituiti. Alcuni tipi di prodotto potrebbero essere più dominanti in base alle dimensioni della produzione (ad esempio,). `state` I loro vincoli di output verranno sempre applicati indipendentemente dai vincoli di output aggiunti dalla società A ai propri dati.

7. La società A crea una tabella di vendita associata alla collaborazione.
8. La società B crea un'associazione tra tabelle di restituzione e collaborazione.
9. La società A esegue interrogazioni, come nell'esempio seguente, per comprendere meglio la quantità di resi nell'azienda B rispetto al totale degli acquisti per località nel 2022.

```
SELECT
  companyB.state,
  SUM(companyB.returns),
  COUNT(DISTINCT companyA.hashedemail)
FROM
  sales companyA
  INNER JOIN returns companyB ON companyA.identifier = companyB.identifier
```

```
WHERE
  companyA.purchasedate BETWEEN '2022-01-01' AND '2022-12-31' AND
  TRUNC(companyB.returndate) > companyA.purchasedate
GROUP BY
  companyB.state;
```

10. La Società A e la Società B esaminano i registri delle interrogazioni. La società B verifica che la richiesta sia in linea con quanto concordato nell'accordo di collaborazione.

Risoluzione dei problemi relativi alle regole di analisi di aggregazione

Utilizza queste informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni quando lavori con le regole di analisi di aggregazione.

Problemi

- La mia query non ha prodotto alcun risultato

La mia query non ha prodotto alcun risultato

Questo può accadere quando non ci sono risultati corrispondenti o quando i risultati corrispondenti non soddisfano una o più soglie minime di aggregazione.

Per ulteriori informazioni sulle soglie minime di aggregazione, consulta. Regola di analisi dell'aggregazione: esempio

Regola di analisi delle liste

InAWS Clean Rooms, una regola di analisi degli elenchi genera elenchi a livello di riga della sovrapposizione tra la tabella configurata a cui viene aggiunta e le tabelle configurate del membro che può eseguire la query. Il membro che può eseguire query esegue query che includono una regola di analisi dell'elenco.

Il tipo di regola di analisi degli elenchi supporta casi d'uso come l'arricchimento e la creazione di audience.

Per ulteriori informazioni sulla struttura e sulla sintassi delle query predefinite per questa regola di analisi, vedere. Struttura predefinita della regola di analisi delle liste

I parametri della regola di analisi degli elenchi, definita inRegola di analisi delle liste: controlli di interrogazione, dispongono di controlli di interrogazione. I suoi controlli di interrogazione includono la

possibilità di selezionare le colonne che possono essere elencate nell'output. La query deve avere almeno un join con una tabella configurata dal membro che può eseguire la query, direttamente o in modo transitivo.

Non esistono controlli sui risultati delle query come quelli per la regola di analisi di aggregazione.

Le query di elenco possono utilizzare solo operatori matematici. Non possono utilizzare altre funzioni (come l'aggregazione o lo scalare).

Argomenti

- Elenca la struttura e la sintassi delle interrogazioni
- Regola di analisi delle liste: controlli di interrogazione
- Struttura predefinita della regola di analisi delle liste
- Regola di analisi delle liste: esempio

Elenca la struttura e la sintassi delle interrogazioni

Le interrogazioni su tabelle che dispongono di una regola di analisi degli elenchi devono rispettare la sintassi seguente.

```
--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]
```

Nella tabella seguente vengono illustrate tutte le espressioni elencate nella sintassi precedente.

Expression	Definizione	Esempi
select_list_expression	Un elenco separato da virgole contenente almeno il nome di una colonna della tabella. È richiesto un `DISTINCT` parametro. **Note** Le colonne `select_list_expression` possono essere utilizzate come alias con o senza il `AS` parametro. Supporta anche il `TOP` parametro. Per ulteriori informazioni, vedere AWS Clean RoomsSQL Reference .	`SELECT DISTINCT segment`
table_expression	Una tabella, o unione di tabelle, `join_condition` a cui connetterla`join_condition` . `join_condition` restituisce un valore booleano. I `table_expression` supporti:	`FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2`

Expression	Definizione	Esempi
	• Un tipo di JOIN specifico (INNERJOIN) • Le condizioni di confronto dell'uguaglianza all'interno di a `join_condition` (=) • Operatori logici (AND,OR).	

where_expression	Un'espressione condizionale che restituisce un valore booleano. Può essere composta dai seguenti elementi:
	• Nomi di colonna delle tabelle
	• Operatori matematici
	• Stringhe letterali
	• Letterali numerici
	
	Le condizioni di confronto supportate sono ()=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL.
	
	Gli operatori logici supportati sono (AND, OR).
	
	`where_expression` È facoltativo.
		`WHERE state + '_' + city = 'NY_NYC'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

Expression	Definizione	Esempi
limit_expression	Questa espressione deve assumere un numero intero positivo. Può anche essere scambiato con un parametro TOP. Il limit_expression è facoltativo.	LIMIT 100

Per quanto riguarda la struttura e la sintassi delle query di elenco, tenete presente quanto segue:

- I comandi SQL diversi da SELECT non sono supportati.
- Le sottoquery e le espressioni di tabella comuni (ad esempio,WITH) non sono supportate
- Le BY clausole GROUP BY HAVING e ORDER non sono supportate
- Il parametro OFFSET non è supportato

Regola di analisi delle liste: controlli di interrogazione

Con i controlli di interrogazione degli elenchi, puoi controllare come le colonne della tabella vengono utilizzate per interrogare la tabella. Ad esempio, è possibile controllare quale colonna viene utilizzata per l'unione o quale colonna può essere utilizzata nell'istruzione e nella WHERE clausola SELECT.

Le seguenti sezioni spiegano ogni controllo.

Argomenti

- Unisci i controlli
- Elenca i controlli

Unisci i controlli

Con i controlli Join, puoi controllare come la tua tabella può essere unita ad altre tabelle in table_expression. AWS Clean Roomssupporta solo JOIN. INNER Nella regola di analisi dell'elenco, è richiesto almeno un INNER JOIN e il membro che può eseguire la query deve includere una tabella

di sua proprietà nel INNER JOIN. Ciò significa che devono unire il tuo tavolo al loro, direttamente o transitivamente.

Di seguito è riportato un esempio di transitività.

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

INNERLe istruzioni JOIN possono utilizzare solo colonne che sono state esplicitamente classificate come una delle regole di `joinColumn` analisi.

Il INNER JOIN deve funzionare su una `joinColumn` tabella configurata e su un'altra tabella configurata nella collaborazione. `joinColumn` Sei tu a decidere quali colonne della tua tabella possono essere utilizzate come`joinColumn`.

Ogni condizione di corrispondenza all'interno della ON clausola è richiesta per utilizzare la condizione di confronto di uguaglianza (=) tra due colonne.

Le condizioni di corrispondenza multiple all'interno di una ON clausola possono essere:

- Combinato utilizzando l'operatore AND logico
- Separato utilizzando l'operatore OR logico

> **Note**
>
> Tutte le JOIN condizioni di partita devono corrispondere a una riga su ciascun lato delJOIN. Anche tutti i condizionali collegati da un operatore logico OR o da un operatore AND logico devono rispettare questo requisito.

Di seguito è riportato un esempio di interrogazione con un operatore logicoAND.

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

Di seguito è riportato un esempio di interrogazione con un operatore OR logico.

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

Controllo	Definizione	Utilizzo
`joinColumns`	Le colonne che si desidera consentire al membro che può eseguire la query di utilizzare nell'istruzione INNER JOIN.	La stessa colonna non può essere classificata sia come a `joinColumn` che come `listColumn` (vediElenca i controlli). `joinColumn` non può essere utilizzato in altre parti della query diverse da INNER JOIN.

Elenca i controlli

I controlli elenco controllano le colonne che possono essere elencate nell'output della query (ovvero utilizzate nell'istruzione SELECT) o utilizzate per filtrare i risultati (ovvero utilizzate nell'WHEREistruzione).

Controllo	Definizione	Utilizzo
`listColumns`	Le colonne che consentite al membro che può eseguire la query di utilizzare nell'istr uzione SELECT e WHERE	A `listColumn` può essere utilizzato in SELECT eWHERE. La stessa colonna non può essere utilizzata sia come che come `listColum n joinColumn` .

Struttura predefinita della regola di analisi delle liste

L'esempio seguente include una struttura predefinita che mostra come completare una regola di analisi degli elenchi.

Nell'esempio seguente, *MyTable*fa riferimento alla tabella di dati. È possibile sostituire ogni *segnaposto di input dell'utente* con le proprie informazioni.

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

Regola di analisi delle liste: esempio

L'esempio seguente dimostra come due aziende possono collaborare AWS Clean Rooms utilizzando l'analisi delle liste.

L'azienda A dispone di dati sulla gestione delle relazioni con i clienti (CRM). L'azienda A desidera ottenere dati di segmento aggiuntivi sui propri clienti per saperne di più sui propri clienti e potenzialmente utilizzare gli attributi come input per altre analisi. L'azienda B dispone di dati sui segmenti composti da attributi di segmento unici creati sulla base dei dati di prima parte. La società B desidera fornire gli attributi univoci del segmento alla società A solo ai clienti che si sovrappongono tra i loro dati e i dati dell'azienda A.

Le aziende decidono di collaborare in modo che l'azienda A possa arricchire i dati sovrapposti. La società A è il socio che può effettuare le domande e la società B è il collaboratore.

Per creare una collaborazione ed eseguire l'analisi degli elenchi in collaborazione, le aziende eseguono le seguenti operazioni:

1. L'azienda A crea una collaborazione e crea un'iscrizione. La collaborazione ha l'azienda B come altro membro della collaborazione. La società A consente la registrazione delle interrogazioni nella collaborazione e la registrazione delle interrogazioni nel proprio account.
2. L'azienda B crea un'appartenenza alla collaborazione. Consente la registrazione delle interrogazioni nel proprio account.
3. L'azienda A crea una tabella configurata con CRM
4. La società A aggiunge la regola di analisi alla tabella configurata dal cliente, come mostrato nell'esempio seguente.

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

`joinColumns`— La società A desidera utilizzare `hashedemail` e/o `thirdpartyid` (ottenuto da un fornitore di identità) abbinare i clienti dei dati CRM ai clienti dei dati del segmento. Ciò contribuirà a garantire che l'azienda A abbini dati arricchiti per i clienti giusti. Dispongono di due JoinColumns per migliorare potenzialmente il tasso di corrispondenza dell'analisi.

`listColumns`— La società A le utilizza `listColumns` accanto per ottenere colonne arricchite e `internalid` le utilizza all'interno dei propri sistemi. `segment1`Aggiungono `segment2` e `customercategory` potenzialmente limitano l'arricchimento a segmenti specifici utilizzandoli nei filtri.

5. La società B crea una tabella configurata per segmenti.
6. La società B aggiunge la regola di analisi alla tabella configurata del segmento.

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

`joinColumns`— La società B consente all'azienda A di partecipare `identifier2` per abbinare i clienti dai dati del segmento ai dati CRM. La società A e la società B hanno collaborato con il fornitore di identità per ottenere `identifier2` una soluzione adatta a questa collaborazione. Non

ne hanno aggiunti altri `joinColumns` perché ritenevano che `identifier2` fornisse il tasso di corrispondenza più elevato e preciso e non fossero necessari altri identificatori per le query.

`listColumns`— L'azienda B consente all'azienda A di arricchire i propri dati con `segment3` `segment4` attributi unici che ha creato, raccolto e utilizzato (con il cliente A) per contribuire all'arricchimento dei dati. Vogliono che l'azienda A ottenga questi segmenti per la sovrapposizione a livello di riga perché si tratta di una collaborazione per l'arricchimento dei dati.

7. L'azienda A crea un'associazione di tabelle CRM alla collaborazione.
8. La società B crea un'associazione di tabelle di segmenti alla collaborazione.
9. L'azienda A esegue interrogazioni, come la seguente, per arricchire i dati sovrapposti dei clienti.

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

10. L'azienda A e la società B esaminano i registri delle interrogazioni. La società B verifica che la richiesta sia in linea con quanto concordato nell'accordo di collaborazione.

Regola di analisi personalizzata in AWS Clean Rooms

In AWS Clean Rooms, una regola di analisi personalizzata è un nuovo tipo di regola di analisi che consente di eseguire query personalizzate sulla tabella configurata. Le query SQL personalizzate sono ancora limitate al solo SELECT comando, ma possono utilizzare più costrutti SQL rispetto alle query di aggregazione ed elenco (ad esempio, funzioni di finestra, OUTER JOIN, CTE o sottoquery; per un elenco completo, consulta il AWS Clean Rooms riferimento SQL). Le query SQL personalizzate non devono seguire una struttura di query come le query di aggregazione e le query a elenco.

La regola di analisi personalizzata supporta casi d'uso più avanzati rispetto a quelli che possono essere supportati dalla regola di aggregazione e analisi degli elenchi, come l'analisi di attribuzione personalizzata, il benchmarking, l'analisi di incrementalità e l'individuazione dell'audience. Ciò si aggiunge a un superset dei casi d'uso supportati dalle regole di aggregazione e analisi degli elenchi.

La regola di analisi personalizzata supporta anche la privacy differenziale. La privacy differenziale è un quadro matematicamente rigoroso per la protezione della privacy dei dati. Per ulteriori informazioni, consulta AWS Clean Rooms Privacy differenziale. Quando si crea un modello di analisi, AWS Clean Rooms Differential Privacy controlla il modello per determinare se è compatibile con la

struttura di interrogazione generica per Differential Privacy. AWS Clean Rooms Questa convalida garantisce che non si crei un modello di analisi non consentito con una tabella differenziale protetta dalla privacy.

Per configurare la regola di analisi personalizzata, i proprietari dei dati possono scegliere di consentire l'esecuzione di query personalizzate specifiche, archiviate in modelli di analisi, sulle tabelle configurate. I proprietari dei dati esaminano i modelli di analisi prima di aggiungerli al controllo di analisi consentito nella regola di analisi personalizzata. I modelli di analisi sono disponibili e visibili solo nella collaborazione in cui vengono creati (anche se la tabella è associata ad altre collaborazioni) e possono essere eseguiti solo dal membro che può eseguire query nell'ambito di tale collaborazione.

In alternativa, i membri possono scegliere di consentire ad altri membri (fornitori di query) di creare query senza revisione. I membri aggiungono gli account dei provider di query controllati dai provider di query consentiti nella regola di analisi personalizzata. Se il provider di query è il membro che può eseguire le query, possono eseguire qualsiasi query direttamente sulla tabella configurata. I provider di query possono anche creare interrogazioni creando modelli di analisi. Tutte le query create dai provider di query possono essere eseguite automaticamente sulla tabella in tutte le collaborazioni in cui Account AWS è presente e la tabella è associata.

I proprietari dei dati possono consentire solo ai modelli di analisi o agli account di creare query, non entrambi. Se il proprietario dei dati lo lascia vuoto, il membro che può eseguire le query non può eseguire query sulla tabella configurata.

Argomenti

- Struttura predefinita della regola di analisi personalizzata
- Esempio di regola di analisi personalizzata
- Regola di analisi personalizzata con privacy differenziale

Struttura predefinita della regola di analisi personalizzata

L'esempio seguente include una struttura predefinita che mostra come completare una regola di analisi personalizzata con la privacy differenziale attivata. Il *`userIdentifier`* valore è la colonna che identifica in modo univoco gli utenti, ad esempio user_id. Quando in una collaborazione sono attivate due o più tabelle con privacy differenziale, è AWS Clean Rooms necessario configurare la stessa colonna come colonna dell'identificatore utente in entrambe le regole di analisi per mantenere una definizione coerente degli utenti tra le tabelle.

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

Puoi eseguire una delle seguenti operazioni:

- Aggiungi gli ARN dei modelli di analisi al controllo consentito delle analisi. In questo caso, il `allowedAnalysisProviders` controllo non è incluso.

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

- Aggiungi gli Account AWS ID dei membri al `allowedAnalysisProviders` controllo. In questo caso, si aggiunge ANY_QUERY qualcosa al `allowedAnalyses` controllo.

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

Esempio di regola di analisi personalizzata

L'esempio seguente dimostra come due aziende possono collaborare AWS Clean Rooms utilizzando la regola di analisi personalizzata.

L'azienda A dispone di dati sui clienti e sulle vendite. L'azienda A è interessata a comprendere l'incrementalità delle vendite di una campagna pubblicitaria sul sito della Società B. L'azienda B dispone di dati sulle visualizzazioni e attributi dei segmenti utili all'azienda (ad esempio, il dispositivo utilizzato per visualizzare la pubblicità).

L'azienda A ha una query di incrementalità specifica che desidera eseguire nell'ambito della collaborazione.

Per creare una collaborazione ed eseguire un'analisi personalizzata in collaborazione, le aziende eseguono le seguenti operazioni:

1. L'azienda A crea una collaborazione e crea un'iscrizione. La collaborazione ha l'azienda B come altro membro della collaborazione. La società A consente la registrazione delle interrogazioni nella collaborazione e la registrazione delle interrogazioni nel proprio account.
2. L'azienda B crea un'appartenenza alla collaborazione. Consente la registrazione delle interrogazioni nel proprio account.
3. L'azienda A crea una tabella configurata con CRM
4. La società A aggiunge una regola di analisi personalizzata vuota alla tabella configurata per le vendite.
5. La società A associa la tabella configurata per le vendite alla collaborazione.
6. La società B crea una tabella configurata per la visualizzazione.
7. La società B aggiunge una regola di analisi personalizzata vuota alla tabella configurata per la visualizzazione.
8. La società B associa la tabella configurata per la visualizzazione alla collaborazione.
9. La società A visualizza la tabella delle vendite e la tabella delle visualizzazioni associate alla collaborazione e crea un modello di analisi, aggiungendo la query di incrementalità e il parametro per il mese della campagna.

```
{
    "analysisParameters": [
    {
        "defaultValue": ""
        "type": "DATE"
        "name": "campaign_month"
    }
    ],
    "description": "Monthly incrementality query using sales and viewership data"
    "format": "SQL"
    "name": "Incrementality analysis"
    "source":
        "WITH labeleddata AS
        (
        SELECT hashedemail, deviceid, purchases, unitprice, purchasedate,
```

```
        CASE
            WHEN testvalue IN ('value1', 'value2', 'value3') THEN 0
            ELSE 1
        END AS testgroup
        FROM viewershipdata
        )
        SELECT labeleddata.purchases, provider.impressions
        FROM labeleddata
        INNER JOIN salesdata
          ON labeleddata.hashedemail = provider.hashedemail
        WHERE MONTH(labeleddata.purchasedate) > :campaignmonth
        AND testgroup = :group
       "
}
```

10. La società A aggiunge il proprio account (ad esempio, 444455556666) al controllo consentito dal fornitore di analisi nella regola di analisi personalizzata. Utilizzano il controllo del provider di analisi consentito perché desiderano consentire l'esecuzione di tutte le query create sulla tabella configurata per le vendite.

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

11. L'azienda B vede il modello di analisi creato nell'ambito della collaborazione e ne esamina il contenuto, inclusi la stringa di query e il parametro.
12. La società B stabilisce che il modello di analisi soddisfa il caso d'uso dell'incrementalità e soddisfa i requisiti di privacy relativi alle modalità di interrogazione della tabella configurata per la visualizzazione.
13. La società B aggiunge il modello di analisi ARN al controllo di analisi consentito nella regola di analisi personalizzata della tabella di visualizzazione. Utilizzano il controllo di analisi consentito perché desiderano solo consentire l'esecuzione della query di incrementalità sulla tabella configurata per la visualizzazione.

```
{
  "allowedAnalyses": [
```

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

14La società A esegue il modello di analisi e utilizza il valore del parametro. `05-01-2023`

Regola di analisi personalizzata con privacy differenziale

Nel AWS Clean Rooms, la regola di analisi personalizzata supporta la privacy differenziale. La privacy differenziale è un framework matematicamente rigoroso per la protezione della privacy dei dati che consente di proteggere i dati dai tentativi di reidentificazione.

La privacy differenziale supporta analisi aggregate come la pianificazione di campagne pubblicitarie, la post-ad-campaign misurazione, il benchmarking in un consorzio di istituti finanziari e i test A/B per la ricerca sanitaria.

La struttura e la sintassi delle query supportate sono definite in. Struttura e sintassi delle query

Regola di analisi personalizzata con esempio di privacy differenziale

Considerate l'esempio di regola di analisi personalizzata presentato nella sezione precedente. Questo esempio dimostra come è possibile utilizzare la privacy differenziale per proteggere i dati dai tentativi di reidentificazione, permettendo al contempo al partner di acquisire informazioni fondamentali per l'azienda dai dati. Supponiamo che l'azienda B, che dispone dei dati sulle visualizzazioni, voglia proteggere i propri dati utilizzando una privacy differenziale. Per completare la configurazione della privacy differenziale, l'azienda B completa i seguenti passaggi:

1. La società B attiva la privacy differenziale aggiungendo una regola di analisi personalizzata alla tabella configurata per la visualizzazione. La società B seleziona `viewershipdata.hashedemail` come colonna identificativa dell'utente.
2. La società B aggiunge una politica sulla privacy differenziale alla collaborazione per rendere disponibile la tabella dei dati di visualizzazione per le interrogazioni. L'azienda B seleziona la politica predefinita per completare rapidamente la configurazione.

La società A, che desidera comprendere l'incrementalità delle vendite di una campagna pubblicitaria sul sito dell'azienda B, utilizza il modello di analisi. Poiché la query è compatibile con la struttura di interrogazione generica di AWS Clean Rooms Differential Privacy, la query viene eseguita correttamente.

Struttura e sintassi delle query

Le query contenenti almeno una tabella con la privacy differenziale attivata devono rispettare la sintassi seguente.

```
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**
>
> Per quanto riguarda la struttura e la sintassi delle query di privacy differenziali, tenete presente quanto segue:
>
> - Le sottoquery non sono supportate.
> - Le Common Table Expressions (CTE) dovrebbero emettere la colonna dell'identificatore utente se una tabella o un CTE coinvolgono dati protetti dalla privacy differenziale. I filtri, i raggruppamenti e le aggregazioni devono essere eseguiti a livello di utente.
> - Final_select consente le funzioni di aggregazione COUNT DISTINCT, COUNT, SUM, AVG e STDDEV.

Per ulteriori dettagli su quali parole chiave SQL sono supportate per la privacy differenziale, vedere. Funzionalità SQL di AWS Clean Rooms Differential Privacy

AWS Clean Rooms Privacy differenziale

AWS Clean Rooms Differential Privacy ti aiuta a proteggere la privacy dei tuoi utenti con una tecnica basata su basi matematiche implementata con controlli intuitivi in pochi clic. Essendo una funzionalità completamente gestita, non è necessaria alcuna esperienza precedente in materia di privacy differenziale per aiutarti a prevenire la reidentificazione degli utenti. AWS Clean Rooms aggiunge automaticamente una quantità di rumore accuratamente calibrata ai risultati delle query in fase di esecuzione per proteggere i dati a livello individuale.

AWS Clean Rooms Differential Privacy supporta un'ampia gamma di query analitiche ed è ideale per un'ampia varietà di casi d'uso, in cui una piccola quantità di errore nei risultati delle query non compromette l'utilità dell'analisi. Grazie a questa soluzione, i vostri partner possono generare informazioni fondamentali per l'azienda su campagne pubblicitarie, decisioni di investimento, ricerca clinica e altro ancora, il tutto senza richiedere alcuna configurazione aggiuntiva da parte dei partner.

AWS Clean Rooms Differential Privacy protegge dall'overflow o dagli errori di cast non validi che utilizzano funzioni scalari o simboli di operatori matematici in modo malevolo.

Per ulteriori informazioni sulla privacy AWS Clean Rooms differenziale, consulta i seguenti argomenti.

Argomenti

Privacy differenziale

La privacy differenziale consente solo approfondimenti aggregati e offusca il contributo dei dati di ogni individuo a tali approfondimenti. La privacy differenziale protegge i dati di collaborazione dal membro che può ricevere risultati imparando a conoscere una persona specifica. Senza privacy differenziale, il membro che può ricevere risultati può tentare di dedurre i dati dei singoli utenti aggiungendo o rimuovendo record relativi a un individuo e osservando la differenza nei risultati delle query.

Quando la privacy differenziale è attivata, viene aggiunta una determinata quantità di rumore ai risultati della query per offuscare il contributo dei singoli utenti. Se il membro che può ricevere i risultati cerca di osservare la differenza tra i risultati della query dopo aver rimosso i record relativi a un individuo dal relativo set di dati, la variabilità dei risultati della query aiuta a impedire l'identificazione dei dati dell'individuo. AWS Clean Rooms Differential Privacy utilizza il SampCertsampler, un'implementazione di campionamento collaudata e corretta sviluppata da. AWS

Come funziona Differential Privacy in AWS Clean Rooms

Il flusso di lavoro per attivare la privacy differenziale AWS Clean Rooms richiede i seguenti passaggi aggiuntivi per completare il flusso di lavoro per: AWS Clean Rooms

1. La privacy differenziale viene attivata quando si aggiunge una regola di analisi personalizzata.
2. La politica sulla privacy differenziale per la collaborazione è configurata per rendere le tabelle di dati protette con privacy differenziale disponibili per le interrogazioni.

Dopo aver completato questi passaggi, il membro che può eseguire le query può iniziare a eseguire query su dati differenziali protetti dalla privacy. AWS Clean Rooms restituisce risultati conformi alla politica sulla privacy differenziale. AWS Clean Rooms Differential Privacy registra il numero stimato di domande rimanenti che è possibile eseguire, in modo analogo all'indicatore del livello di benzina di un'auto che mostra il livello attuale del carburante dell'auto. Il numero di query che il membro che può eseguire la query è limitato dai parametri Privacy budget e Noise aggiunti per query che sono impostati in. Informativa sulla privacy differenziale

Considerazioni

Quando utilizzi la privacy differenziale in AWS Clean Rooms, considera quanto segue:

- Il membro che può ricevere risultati non può utilizzare la privacy differenziale. Configureranno una regola di analisi personalizzata con la privacy differenziale disattivata per le tabelle configurate.
- Il membro che può eseguire le query non può unire le tabelle di due o più fornitori di dati quando entrambi hanno attivato la privacy differenziale.

Informativa sulla privacy differenziale

L'informativa sulla privacy differenziale controlla quante funzioni di aggregazione il membro che può interrogare può eseguire in una collaborazione. Il budget per la privacy definisce una risorsa comune

e limitata che viene applicata a tutte le tabelle in una collaborazione. Il rumore aggiunto per query determina la velocità di esaurimento del budget dedicato alla privacy.

È necessaria una politica sulla privacy differenziale per rendere disponibili per le interrogazioni le tabelle differenziali protette dalla privacy. Si tratta di un passaggio che si effettua una sola volta in una collaborazione e include due input:

- Budget per la privacy: quantificato in termini di epsilon, il budget per la privacy controlla il livello di protezione della privacy. È una risorsa comune e limitata che viene applicata a tutte le tabelle protette con privacy differenziale nella collaborazione, perché l'obiettivo è preservare la privacy degli utenti le cui informazioni possono essere presenti in più tabelle.

  Il budget per la privacy viene utilizzato ogni volta che viene eseguita una query sulle tabelle. Quando il budget per la privacy è completamente esaurito, il membro della collaborazione che può eseguire query non può eseguire query aggiuntive finché non viene aumentato o aggiornato. Impostando un budget più elevato per la privacy, il membro che può ricevere risultati può ridurre l'incertezza sugli individui all'interno dei dati. Scegliete un budget per la privacy che bilanci i requisiti di collaborazione con le vostre esigenze di privacy e dopo aver consultato i responsabili delle decisioni aziendali.

  Puoi selezionare Aggiorna mensilmente il budget per la privacy per creare automaticamente un nuovo budget per la privacy ogni mese di calendario, se prevedi di inserire regolarmente nuovi dati nella collaborazione. La scelta di questa opzione consente di rivelare quantità arbitrarie di informazioni sulle righe di dati quando vengono ripetutamente interrogate durante gli aggiornamenti. Evita di scegliere questa opzione se le stesse righe verranno ripetutamente interrogate tra un aggiornamento del budget relativo alla privacy e l'altro.
- Il rumore aggiunto per ogni query viene misurato in termini di numero di utenti i cui contributi si desidera oscurare. Questo valore determina la velocità di esaurimento del budget destinato alla privacy. Un valore di rumore più elevato riduce la velocità con cui viene esaurito il budget per la privacy e quindi consente di eseguire più query sui dati. Tuttavia, ciò dovrebbe essere bilanciato dal rilascio di informazioni meno accurate sui dati. Quando imposti questo valore, considera la precisione desiderata per le informazioni sulla collaborazione.

Puoi utilizzare l'informativa sulla privacy differenziale predefinita per completare rapidamente la configurazione o personalizzare la tua politica sulla privacy differenziale in base al tuo caso d'uso. AWS Clean Rooms Differential Privacy fornisce controlli intuitivi per configurare la politica. AWS Clean Rooms Differential Privacy consente di visualizzare in anteprima l'utilità in termini di numero di

aggregazioni possibili tra tutte le query sui dati e di stimare quante query possono essere eseguite in una collaborazione sui dati.

Puoi utilizzare gli esempi interattivi per capire in che modo i diversi valori di Privacy, budget e Noise aggiunti per query influirebbero sui risultati di diversi tipi di query SQL. In generale, è necessario bilanciare le esigenze di privacy con il numero di query che si desidera consentire e l'accuratezza di tali query. Un budget inferiore per la privacy o un aumento del rumore aggiunto per query possono proteggere meglio la privacy degli utenti, ma forniscono informazioni meno significative ai partner di collaborazione.

Se aumenti il budget per la privacy mantenendo invariato il parametro Noise added per query, il membro che può eseguire le query può eseguire più aggregazioni sulle tue tabelle nell'ambito della collaborazione. Puoi aumentare il budget per la privacy in qualsiasi momento durante la collaborazione. Se riduci il budget per la privacy mantenendo invariato il parametro Noise added per query, il membro che può eseguire la query può eseguire meno aggregazioni. Non puoi ridurre il budget per la privacy dopo che il membro che può eseguire la query ha iniziato ad analizzare i tuoi dati.

Se aumenti il Noise aggiunto per query mantenendo invariato il budget per la privacy, il membro che può eseguire le query può eseguire più aggregazioni sulle tue tabelle nell'ambito della collaborazione. Se riduci il Noise aggiunto per query mantenendo invariato l'input del budget per la privacy, il membro che può eseguire la query può eseguire meno aggregazioni. Puoi aumentare o diminuire il rumore aggiunto per query in qualsiasi momento durante la collaborazione.

L'informativa sulla privacy differenziale è gestita dalle azioni API del modello di privacy budget.

Funzionalità SQL di AWS Clean Rooms Differential Privacy

AWS Clean Rooms Differential Privacy utilizza una struttura di query generica per supportare query SQL complesse. I modelli di analisi personalizzati vengono convalidati in base a questa struttura per garantire che possano essere eseguiti su tabelle protette dalla privacy differenziale. La tabella seguente indica quali funzioni sono supportate. Per ulteriori informazioni, consulta Struttura e sintassi delle query.

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Funzioni di aggregazione	• Funzione ANY_VALUE	Supportato a condizione che i CTE	Aggregazioni supportate: AVG,

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
	• Funzione APPROXIMATE PERCENTILE_DISC • Funzione AVG • Funzioni COUNT e COUNT DISTINCT • Funzione LISTAGG • Funzione MAX • Funzione MEDIAN • Funzione MIN • Funzione PERCENTILE_CONT • Funzioni STDDEV_SAMP e STDDEV_POP • Funzioni SUM e SUM DISTINCT • Funzioni VAR_SAMP e VAR_POP	che utilizzano tabelle differenziali protette dalla privacy debbano generare dati con record a livello utente. È necessario scrivere l'espressione SELECT in quei CTE utilizzando format. `SELECT userIdentifierColumn...'	COUNT, COUNT DISTINCT, STDDEV e SUM.

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
CTE	clausola WITH, sottoquery clausola WITH	Supportata a condizione che i CTE che utilizzano tabelle differenziali protette dalla privacy debbano generare dati con record a livello utente. È necessario scrivere l'espressione SELECT in quei CTE utilizzan do format. `SELECT userIdent ifierColu mn...'	N/D
Sottoquery	Sottoquery dell'elenco SELECT, sottoquery della clausola FROM, sottoquery della clausola WHERE	Non supportato. Le sottoquery nella query che fa riferimento a una tabella con la privacy differenziale attivata non sono supportate. Riscrivi le tue sottoquery come Common Table Expressions (CTE).	

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Clausole Join	• INNER JOIN • LEFT JOIN • RIGHT JOIN • ADESIONE COMPLETA • [JOIN] operatore OR • CROSS JOIN	Supportato a condizione che solo le funzioni JOIN che sono equi-join nelle colonne degli identificatori utente siano supportate e siano obbligatorie quando si eseguono query su due o più tabelle con la privacy differenziale attivata. Assicurati che le condizioni equi-join obbligato rie siano corrette. Verifica che il proprieta rio della tabella abbia configurato la stessa colonna identificativa utente in tutte le tabelle in modo che la definizione di un utente rimanga coerente tra le tabelle. Le funzioni CROSS JOIN non sono supportate quando si combinano due o più relazioni con la privacy differenziale attivata.	
Operatori su set	UNION, UNION ALL, INTERSECT , EXCEPT | MINUS (questi sono sinonimi)	Tutti sono supportati	Non supportato

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Funzioni finestra	Funzioni di aggregazione • Funzione finestra AVG • Funzione finestra COUNT • Funzione finestra CUME_DIST • Funzione finestra DENSE_RANK • Funzione finestra FIRST_VALUE • Funzione finestra LAG • Funzione finestra LAST_VALUE • Funzione finestra LEAD • Funzioni MAX Window • Funzioni della finestra MEDIAN • Funzioni della finestra MIN • Funzione finestra NTH_VALUE • Funzione finestra RATIO_TO_REPORT	Tutte sono supportate a condizione che la colonna dell'identificatore utente nella clausola di partizione della funzione finestra sia richiesta quando si esegue una query su una relazione con la privacy differenziale attivata.	Non supportato

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
	• funzione di finestra STDDEV_SAMP e STDDEV_POP (STDDEV_SAMP e STDDEV sono sinonimi) • Funzioni della finestra SUM • Funzioni di finestra VAR_SAMP e VAR_POP (VAR_SAMP e VARIANCE sono sinonimi)		
	Funzioni di classific azione • Funzione finestra DENSE_RANK • Funzione finestra NTILE • Funzione finestra PERCENT_RANK • Funzione finestra RANK • Funzione finestra ROW_NUMBER		

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Espressioni condizionali	• espressione della condizione CASE • espressione COALESCE • Funzioni GREATEST e LEAST • Funzioni NVL e COALESCE • Funzione NVL2 • Funzione NULLIF	Tutti sono supportati	Sono tutte supportate
Condizioni	• Condizione di confronto • Condizioni logiche • Condizioni di corrispondenza di modelli • Condizioni di intervallo BETWEEN • Condizione Null	`EXISTS`e `IN` non possono essere utilizzati perché richiedono sottoquery. Tutti gli altri sono supportati.	Tutti sono supportati

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Funzioni data-ora	• Funzioni di data e ora nelle transazioni • Operatore di concatenazione • Funzioni ADD_MONTHS • Funzione CONVERT_TIMEZONE • Funzione CURRENT_DATE • Funzione DATEADD • Funzione DATEDIFF • Funzioni DATE_PART • Funzione DATE_TRUNC • Funzione EXTRACT • Funzione GETDATE • Funzioni TIMEOFDAY • Funzione TO_TIMESTAMP • Parti di data per funzioni di data e timestamp	Sono tutte supportate	Sono tutte supportate

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Funzioni stringa	• || operatore (concatenazione) • Funzione BTRIM • Funzione CHAR_LENGTH • Funzione CHARACTER _LENGTH • Funzione CHARINDEX • Funzione CONCAT • Funzioni LEFT e RIGHT • Funzione LEN • Funzione LENGTH • Funzione LOWER • Funzioni LPAD e RPAD • Funzione LTRIM • Funzioni POSITION • Funzione REGEXP_COUNT • Funzione REGEXP_INSTR • Funzione REGEXP_RE PLACE • Funzione REGEXP_SUBSTR • Funzione REPEAT	Sono tutte supportate	Sono tutte supportate

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
	• Funzione REPLACE • Funzione REPLICATE • Funzione REVERSE • Funzione RTRIM • Funzione SOUNDEX • Funzione SPLIT_PART • Funzione STRPOS • Funzione SUBSTRING • Funzione TEXTLEN • Funzione TRANSLATE • Funzioni TRIM • Funzione UPPER		
Funzioni di formattazione del tipo di dati	• Funzione CAST • TO_CHAR • Funzione TO_DATE • TO_NUMBER • Stringhe di formato datetime • Stringhe di formato numerico	Sono tutte supportate	Sono tutte supportate

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Funzioni hash	• Funzione MD5 • Funzione SHA • Funzione SHA1 • Funzione SHA2 • MURMUR3_32_HASH	Sono tutte supportate	Sono tutte supportate
Simboli degli operatori matematici	+, -, *,/,% e @	Tutti sono supportati	Sono tutte supportate

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Funzioni matematiche	• Funzione ABS • Funzione ACOS • Funzione ASIN • Funzione ATAN • Funzione ATAN2 • Funzione CBRT • Funzione CEILING (oppure CEIL) • Funzione COS • Funzione COT • Funzione DEGREES • Funzione DEXP • Funzione LTRIM • Funzione DLOG1 • Funzione DLOG10 • Funzione EXP • Funzione FLOOR • Funzione LN • Funzione LOG • Funzione MOD • Funzione PI • Funzione POWER • Funzioni RADIANS • Funzione RANDOM • Funzione ROUND • Funzione SIGN • Funzione SIN	Sono tutte supportate	Sono tutte supportate

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
	• Funzioni SQRT • Funzione TRUNC		
Funzioni di informazioni sul tipo SUPER	• Funzione DECIMAL_PRECISION • Funzione DECIMAL_SCALE • Funzione IS_ARRAY • Funzione IS_BIGINT • Funzione IS_CHAR • Funzione IS_DECIMAL • Funzione IS_FLOAT • Funzione IS_INTEGER • Funzione IS_OBJECT • Funzione IS_SCALAR • Funzione IS_SMALLINT • Funzione IS_VARCHAR • Funzione JSON_TYPEOF	Sono tutte supportate	Sono tutte supportate

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Funzioni VARBYTE	• funzione FROM_HEX • funzione FROM_VARBYTE • Funzione TO_HEX • Funzione TO_VARBYTE	Sono tutte supportate	Sono tutte supportate
JSON	• Funzione CAN_JSON_ PARSE • Funzione JSON_EXTR ACT_ARRAY _ELEMENT_TEXT • Funzione JSON_EXTR ACT_PATH_TEXT • Funzione JSON_PARSE • Funzione JSON_SERIALIZE • Funzione JSON_SERA LIZE_TO_V ARBYTE	Sono tutte supportate	Sono tutte supportate

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Funzioni di array	• Funzione array • funzione array_concat • Funzione array_flatten • Funzione get_array_length • Funzione split_to_array • Funzione subarray	Non supportato	Non supportato
GROUP BY esteso	SET DI RAGGRUPPAMENTO, ROLLUP, CUBO	Non supportato	Non supportato
Operazione di ordinamento	ORDER BY	Supportata a condizione che una clausola ORDER BY sia supportata solo nella clausola di partizione di una funzione finestra quando si eseguono interrogazioni su tabelle con privacy differenziale attivata.	Supportato
Limiti di riga	LIMIT, OFFSET	Non supportato nei CTE che utilizzano tabelle differenziali protette dalla privacy	Sono tutte supportate

Nome breve	Costrutti SQL	Espressioni di tabella comuni (CTE)	Clausola SELECT finale
Alias di tabelle e colonne		Supportato	Supportato
Funzioni matematiche su funzioni aggregate		Supportato	Supportato
Funzioni scalari all'interno di funzioni aggregate		Supportato	Supportato

Alternative comuni per costrutti SQL non supportati

Categoria	costrutto SQL	In alternativa
Funzioni finestra	• LISTAGG • PERCENTILE_CONT • PERCENTILE_DISC	È possibile utilizzare la funzione di aggregazione equivalente con GROUP BY.
Simboli degli operatori matematici	• $colonna ||/ 2 • $colonna |/ 2 • $colonna ^ 2	• CBRT • SQRT • POTENZA ($colonna, 2)
Funzioni scalari	• SYSDATE • $colonna: :intero • converti (tipo, $colonna)	• CURRENT_DATE • CAST $column COME numero intero • Tipo AS CAST $column
Valori letterali	INTERVALLO '1 SECONDO'	INTERVALLO '1' SECONDO
limitazione delle righe	TOP n	LIMITE n

Categoria	costrutto SQL	In alternativa
Join	• USING • NATURAL	La clausola ON deve contenere esplicitamente un criterio di unione.

Suggerimenti ed esempi di interrogazioni differenziali sulla privacy

AWS Clean Rooms Differential Privacy utilizza una struttura di query generica per supportare un'ampia varietà di costrutti SQL come Common Table Expressions (CTE) per la preparazione dei dati e funzioni aggregate di uso comune come, o. `COUNT` `SUM` Per offuscare il contributo di ogni possibile utente ai dati aggiungendo disturbi ai risultati delle query aggregate in fase di esecuzione, AWS Clean Rooms Differential Privacy richiede che le funzioni aggregate nel finale vengano eseguite su dati a livello di utente. `SELECT statement`

L'esempio seguente utilizza due tabelle denominate `socialco_impressions` e `socialco_users` provenienti da un editore di contenuti multimediali che desidera proteggere i dati utilizzando una privacy differenziale mentre collabora con un marchio sportivo con i dati. `athletic_brand_sales` L'editore multimediale ha configurato la `user_id` colonna come colonna dell'identificativo utente abilitando al contempo la privacy differenziale in. AWS Clean Rooms L'inserzionista non necessita di una protezione differenziale della privacy e desidera eseguire una query utilizzando i CTE su dati combinati. Poiché il CTE utilizza tabelle differenziali protette dalla privacy, l'inserzionista include la colonna dell'identificatore utente di tali tabelle protette nell'elenco delle colonne CTE e unisce le tabelle protette nella colonna dell'identificatore utente.

```
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
```

Allo stesso modo, se desideri eseguire funzioni di finestra su tabelle di dati differenziali protette dalla privacy, devi includere la colonna dell'identificatore utente nella clausola. `PARTITION BY`

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

Limitazioni della privacy differenziale AWS Clean Rooms

AWS Clean Rooms Differential Privacy non affronta le seguenti situazioni:

1. AWS Clean Rooms Differential Privacy non affronta gli attacchi temporali. Ad esempio, questi attacchi sono possibili in scenari in cui un singolo utente inserisce un numero elevato di righe e l'aggiunta o la rimozione di tale utente modifica in modo significativo il tempo di calcolo della query.
2. AWS Clean Rooms Differential Privacy non garantisce la privacy differenziale quando una query SQL può causare overflow o errori di cast non validi in fase di esecuzione a causa dell'uso di determinati costrutti SQL. La tabella seguente è un elenco di alcuni, ma non di tutti, i costrutti SQL che possono produrre errori di runtime e devono essere verificati nei modelli di analisi. Si consiglia di approvare modelli di analisi che riducano al minimo le possibilità di tali errori di run-time e di esaminare periodicamente i log delle query per determinare se le query sono conformi all'accordo di collaborazione.

   I seguenti costrutti SQL sono vulnerabili agli errori di overflow:

   - Funzioni aggregate: AVG, LISTAVG, PERCENTILE_COUNT, PERCENTILE_DISC, SUM/ SUM_DISTINCT
   - Funzioni di formattazione dei tipi di dati: TO_TIMESTAMP, TO_DATE
   - Funzioni di data e ora: ADD_MONTHS, DATEADD, DATEDIFF

- Funzioni matematiche - +, -, *,/, POWER
- Funzioni di stringa - ||, CONCAT, REPEAT, REPLICATE
- Funzioni della finestra: AVG, LISTAGG, PERCENTILE_COUNT, PERCENTILE_DISC, RATIO_TO_REPORT, SUM

La funzione di formattazione del tipo di dati CAST è vulnerabile agli errori di cast non validi.

AWS Clean Rooms ML

AWS Clean Rooms ML

AWS Clean Rooms ML fornisce un metodo di tutela della privacy che consente a due parti di identificare utenti simili nei propri dati senza la necessità di condividerli tra loro. La prima parte fornisce i dati di formazione AWS Clean Rooms in modo che possano creare e configurare un modello simile e associarlo a una collaborazione. La seconda parte trasferisce quindi i propri dati iniziali AWS Clean Rooms e genera un segmento simile ai dati di addestramento.

Per una spiegazione più dettagliata di come funziona, vedi. Lavori su più account

- Fornitore di dati di formazione: la parte che fornisce i dati di formazione, crea e configura un modello simile e quindi associa tale modello a una collaborazione.
- Fornitore di dati iniziali: la parte che fornisce i dati iniziali, genera un segmento simile ed esporta il segmento simile.
- Dati di formazione: i dati del fornitore dei dati di formazione, utilizzati per generare un modello simile. I dati di addestramento vengono utilizzati per misurare la somiglianza nei comportamenti degli utenti.

  I dati di addestramento devono contenere un ID utente, un ID articolo e una colonna con timestamp. Facoltativamente, i dati di allenamento possono contenere altre interazioni come caratteristiche numeriche o categoriali. Esempi di interazioni sono un elenco di video guardati, articoli acquistati o articoli letti.
- Dati di avviamento: i dati del fornitore di dati iniziali, utilizzati per creare un segmento simile. L'output del segmento Lookalike è un insieme di utenti tratto dai dati di addestramento che assomiglia di più agli utenti seed.
- Modello Lookalike: un modello di apprendimento automatico dei dati di addestramento utilizzato per trovare utenti simili in altri set di dati.

  Quando si utilizza l'API, il termine modello di audience viene utilizzato in modo equivalente al modello lookalike. Ad esempio, si utilizza l'API CreateAudienceModel per creare un modello simile.
- Segmento simile: un sottoinsieme dei dati di addestramento che più assomiglia ai dati iniziali.

  Quando si utilizza l'API, si crea un segmento simile con l'API. StartAudienceGenerationJob

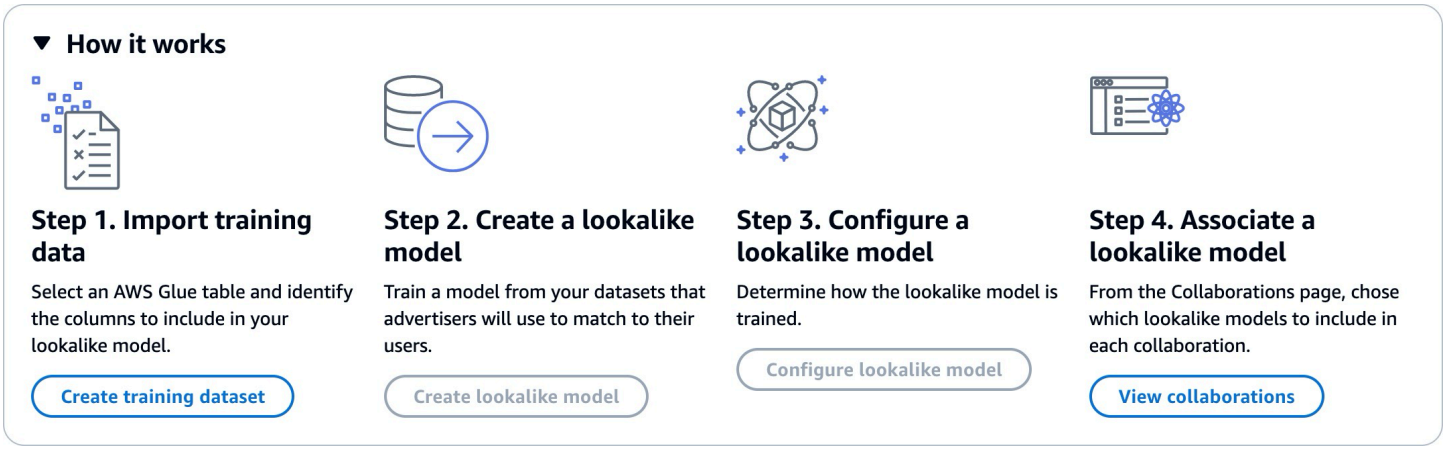
I dati del fornitore di dati di addestramento non vengono mai condivisi con il fornitore di dati di avviamento e i dati del fornitore di dati di avviamento non vengono mai condivisi con il fornitore di dati di formazione. L'output del segmento simile viene condiviso con il fornitore dei dati di addestramento, ma mai con il fornitore di dati iniziali.

Per ulteriori informazioni sui modelli simili, consultate i seguenti argomenti.

Argomenti

- Come funziona il machine learning AWS Clean Rooms

Come funziona il machine learning AWS Clean Rooms



Clean Rooms ML richiede che due parti, un fornitore di dati di formazione e un fornitore di dati iniziali, collaborino in sequenza AWS Clean Rooms per portare i propri dati in una collaborazione. Questo è il flusso di lavoro che il fornitore di dati di formazione deve completare per primo:

1. I dati del fornitore di dati di formazione devono essere archiviati in una tabella del catalogo AWS Glue dati contenente le interazioni tra utenti e elementi. Come minimo, i dati di addestramento devono contenere una colonna ID utente, una colonna ID di interazione e una colonna timestamp.
2. Il fornitore di dati di formazione registra i dati di allenamento con. AWS Clean Rooms
3. Il fornitore di dati di addestramento crea un modello simile che può essere condiviso con più fornitori di dati iniziali. Il modello Lookalike è una rete neurale profonda che può impiegare fino a 24 ore per addestrarsi. Non viene riaddestrato automaticamente e ti consigliamo di riaddestrare il modello settimanalmente.
4. Il fornitore di dati di formazione configura il modello lookalike, incluso se condividere i parametri di pertinenza e la posizione in Amazon S3 dei segmenti di output. Il fornitore di dati di formazione può creare più modelli simili configurati a partire da un unico modello simile.

5. Il fornitore di dati di formazione associa il modello di audience configurato a una collaborazione condivisa con un fornitore di dati iniziali.

Questo è il flusso di lavoro che il fornitore di dati iniziali deve completare successivamente:

1. I dati del fornitore di dati iniziali devono essere archiviati in un bucket Amazon S3.
2. Il fornitore di dati di avviamento avvia la collaborazione che condivide con il fornitore di dati di formazione.
3. Il fornitore di dati iniziali crea un segmento simile dalla scheda Clean Rooms ML della pagina di collaborazione.
4. Il fornitore di dati iniziali può valutare le metriche di pertinenza, se sono state condivise, ed esportare il segmento simile per utilizzarlo all'esterno. AWS Clean Rooms

Protezioni della privacy del machine learning AWS Clean Rooms

Clean Rooms ML è progettato per ridurre il rischio di attacchi di inferenza dei membri, in cui il fornitore di dati di formazione può scoprire chi è presente nei dati iniziali e il fornitore di dati iniziali può scoprire chi c'è nei dati di formazione. Sono state adottate diverse misure per prevenire questo attacco.

Innanzitutto, i fornitori di dati di avviamento non osservano direttamente l'output di Clean Rooms ML e i fornitori di dati di formazione non possono mai osservare i dati iniziali. I fornitori di dati di semina possono scegliere di includere i dati di semina nel segmento di output.

Successivamente, il modello simile viene creato da un campione casuale dei dati di addestramento. Questo esempio include un numero significativo di utenti che non corrispondono al pubblico iniziale. Questo processo rende più difficile determinare se un utente non fosse presente nei dati, il che rappresenta un altro modo per inferire l'appartenenza.

Inoltre, è possibile utilizzare più clienti di seed per ogni parametro di addestramento basato su modelli simili specifici per ciascun seme. Ciò limita quanto il modello può sovra-adattarsi e quindi quanto si può dedurre su un utente. Di conseguenza, consigliamo che la dimensione minima dei dati iniziali sia di 500 utenti.

Infine, le metriche a livello di utente non vengono mai fornite ai fornitori di dati di formazione, il che elimina un'altra possibilità per un attacco di inferenza dell'appartenenza.

AWS Clean Rooms Metriche di valutazione del modello ML

Clean Rooms ML calcola il punteggio di richiamo e pertinenza per determinare le prestazioni del modello. Recall confronta la somiglianza tra i dati simili e i dati di addestramento. Il punteggio di pertinenza viene utilizzato per decidere quanto deve essere numeroso il pubblico, non se il modello ha buone prestazioni.

Il richiamo è una misura imparziale della somiglianza tra il segmento simile e i dati di addestramento. Il richiamo è la percentuale di utenti più simili (per impostazione predefinita, il 20%) tratta da un campione di dati di formazione inclusi nel gruppo di utenti iniziali in base alla funzione di generazione di audience. I valori vanno da 0 a 1, valori più alti indicano un pubblico migliore. Un valore di richiamo approssimativamente uguale alla percentuale massima di contenitori indica che il modello di audience è equivalente alla selezione casuale.

Riteniamo che questa sia una metrica di valutazione migliore rispetto all'accuratezza, alla precisione e ai punteggi F1, perché Clean Rooms ML non ha etichettato accuratamente gli utenti «veri negativi» durante la creazione del suo modello.

Il punteggio di pertinenza a livello di segmento è una misura della somiglianza con valori che vanno da -1 (meno simile) a 1 (più simile). Clean Rooms ML calcola una serie di punteggi di pertinenza per segmenti di varie dimensioni per aiutarti a determinare la dimensione del segmento migliore per i tuoi dati. I punteggi di pertinenza diminuiscono in modo monotono all'aumentare della dimensione del segmento, quindi all'aumentare della dimensione del segmento può essere meno simile ai dati iniziali. Quando il punteggio di pertinenza a livello di segmento raggiunge 0, il modello prevede che tutti gli utenti del segmento «lookalike» abbiano la stessa distribuzione dei dati iniziali. È probabile che l'aumento delle dimensioni dell'output includa utenti del segmento dei lookalike che non hanno la stessa distribuzione dei dati iniziali.

I punteggi di pertinenza sono normalizzati all'interno di una singola campagna e non devono essere utilizzati per effettuare confronti tra campagne diverse. I punteggi di pertinenza non devono essere utilizzati come elemento di prova univoco per determinare i risultati aziendali, in quanto oltre alla pertinenza, sono influenzati da molteplici fattori complessi, come la qualità dell'inventario, il tipo di inventario, la tempistica della pubblicità e così via.

I punteggi di pertinenza non dovrebbero essere utilizzati per giudicare la qualità del seme, ma piuttosto per stabilire se è possibile aumentarla o diminuirla. Considerare i seguenti esempi:

- Tutti i punteggi positivi: ciò indica che ci sono più utenti di output che si prevede siano simili rispetto a quelli inclusi nel segmento dei lookalike. Questo è comune per i dati sulle sementi che fanno

parte di un grande mercato, come tutti coloro che hanno acquistato dentifricio nel mese scorso. Consigliamo di esaminare i dati relativi ai semi più piccoli, ad esempio a tutti coloro che hanno acquistato il dentifricio più di una volta nell'ultimo mese.

- Tutti i punteggi negativi o negativi per la dimensione desiderata del segmento simile: ciò indica che Clean Rooms ML prevede che non ci siano abbastanza utenti simili nella dimensione desiderata del segmento di riferimento. Ciò può essere dovuto al fatto che i dati iniziali sono troppo specifici o che il mercato è troppo piccolo. Consigliamo di applicare un minor numero di filtri ai dati relativi alle sementi o di ampliare il mercato. Ad esempio, se i dati iniziali erano relativi a clienti che avevano acquistato un passeggino e un seggiolino per auto, potresti espandere il mercato ai clienti che hanno acquistato più prodotti per bambini.

I fornitori di dati di formazione determinano se vengono esposti i punteggi di pertinenza e i contenitori in cui vengono calcolati i punteggi di pertinenza.

Lavorare con ML AWS Clean Rooms

Un modello simile è un modello di dati di un fornitore di dati di addestramento che consente a un fornitore di dati iniziali di creare un segmento simile dei dati del fornitore di dati di addestramento che più assomiglia ai propri dati iniziali. Per creare un modello simile da utilizzare in una collaborazione, è necessario importare i dati di addestramento, creare un modello simile, configurare quel modello simile e quindi associarlo a una collaborazione.

Dopo che il fornitore di dati di addestramento ha terminato di creare il modello ML, il fornitore di dati iniziali può creare ed esportare il segmento seed.

Argomenti

Lavorare con modelli simili (fornitore di dati di formazione)

Importa i dati di allenamento

Prima di creare un modello simile, è necessario specificare la AWS Glue tabella che contiene i dati di addestramento. Clean Rooms ML non memorizza una copia di questi dati, ma solo i metadati che gli consentono di accedere ai dati.

Per importare i dati di allenamento in AWS Clean Rooms

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli ML Modeling.
3. Nella scheda Set di dati di allenamento, scegli Crea set di dati di allenamento.
4. Inserisci un nome e una descrizione opzionale.
5. Per Origine dati, scegli la tua AWS Glue tabella:

    a. Scegli il database che desideri configurare dall'elenco a discesa.

    b. Scegli l'origine dei dati di formazione selezionando il database e la tabella che desideri configurare dagli elenchi a discesa.

    > **Note**
    >
    > Per verificare che questa sia la tabella corretta, esegui una delle seguenti operazioni:
    >
    > - Scegliete Visualizza in AWS Glue.
    > - Attiva Visualizza schema per visualizzare lo schema.

6. Per i dettagli sulla formazione, scegli la colonna Identificatore utente, la colonna Identificatore articolo e la colonna Timestamp dai tuoi dati. I dati di allenamento devono contenere queste tre colonne. Puoi anche selezionare qualsiasi altra colonna che desideri includere nei dati di allenamento.

    I dati nella colonna Timestamp devono essere nel formato Unix epoch time in secondi.
7. In Service access, è necessario specificare un ruolo di servizio che può accedere ai dati e fornire una chiave KMS se i dati sono crittografati. Scegli Crea e usa un nuovo ruolo di servizio e Clean Rooms ML creerà automaticamente un ruolo di servizio e aggiungerà la politica di autorizzazioni

necessaria. Scegli Usa un ruolo di servizio esistente e inseriscilo nel campo Nome del ruolo di servizio se hai un ruolo di servizio specifico che desideri utilizzare.

Se i tuoi dati sono crittografati, inserisci la tua chiave KMS nel AWS KMS keycampo o fai clic su Crea una AWS KMS key per generare una nuova chiave KMS.

8. Se desideri abilitare i tag per il set di dati di addestramento, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.
9. Scegli Crea set di dati di allenamento.

Per l'azione API corrispondente, consulta CreateTrainingDataset.

Crea un modello simile

Dopo aver creato un set di dati di addestramento, sei pronto per creare un modello simile. È possibile creare molti modelli simili a partire da un singolo set di dati di addestramento.

È necessario creare un database predefinito nel proprio account AWS Glue Data Catalog o includere l'`glue:createDatabase`autorizzazione nel ruolo fornito.

Per creare un modello simile in AWS Clean Rooms

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli ML Modeling.
3. Nella scheda Modelli simili, scegli Crea un modello simile.
4. Per Crea un modello simile, per i dettagli del modello Lookalike:
   a. Inserisci un nome e una descrizione opzionale.
   b. Scegli il set di dati di addestramento che desideri modellare dall'elenco a discesa.
   c. Inserisci una finestra di formazione opzionale.
5. Se desideri abilitare le impostazioni di crittografia personalizzate per il modello simile, scegli Personalizza le impostazioni di crittografia e quindi inserisci la chiave KMS.
6. Se desideri abilitare i tag per il modello simile, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.
7. Scegli Crea un modello simile.

Per l'azione API corrispondente, consulta CreateAudience Model.

Configura un modello simile

Dopo aver creato un modello simile, sei pronto a configurarlo per l'utilizzo in collaborazione. È possibile creare più modelli simili configurati a partire da un unico modello simile.

Per configurare un modello simile in AWS Clean Rooms

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli ML Modeling.
3. Nella scheda Modelli simili configurati, scegli Configura modello simile.
4. Per Configura il modello simile, per i dettagli del modello simile configurato:
    a. Inserisci un nome e una descrizione opzionale.
    b. Scegli il modello Lookalike che desideri configurare dall'elenco a discesa.
    c. Scegli la dimensione minima del seme corrispondente che desideri. Questo è il numero minimo di utenti nei dati del fornitore di dati iniziali che si sovrappongono agli utenti nei dati di addestramento. Questo valore deve essere maggiore di 0.
5. Per condividere Metrics con altri membri, scegli se desideri che il fornitore di dati iniziali che collabora riceva le metriche del modello, compresi i punteggi di pertinenza.
6. Per la posizione di destinazione del segmento Lookalike, inserisci il bucket Amazon S3 in cui viene esportato il segmento Lookalike. Questo bucket deve trovarsi nella stessa regione delle altre risorse.
7. Per Accesso al servizio, scegli il nome del ruolo di servizio esistente che verrà utilizzato per accedere a questa tabella.
8. Scegli Configura modello Lookalike.
9. Se desideri abilitare i tag per la risorsa della tabella configurata, scegli Aggiungi nuovo tag, quindi inserisci la coppia Chiave e Valore.

Per l'azione API corrispondente, consulta CreateConfiguredAudienceModel.

Associa un modello simile configurato

Dopo aver configurato un modello simile, puoi associarlo a una collaborazione.

Per associare un modello simile configurato in AWS Clean Rooms

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Nella scheda Con iscrizione attiva, scegli una collaborazione.
4. Nella scheda ML Modeling, scegli Associa modello simile.
5. Per il modello sosia configurato da Associate, per i dettagli del modello sosia associato:
    a. Immettete un nome per il modello di audience configurato associato.
    b. Inserire una descrizione della tabella.

        La descrizione aiuta a distinguere tra altri modelli di audience configurati associati con nomi simili.
6. Per Modello simile configurato, scegli un modello simile configurato dall'elenco a discesa.
7. Selezionare Associate (Associa).

Per l'azione API corrispondente, consulta Association. CreateConfigured AudienceModel

Aggiorna un modello simile configurato

Dopo aver associato un modello simile configurato, puoi aggiornarlo per modificare informazioni come il nome, i parametri da condividere o la posizione di output di Amazon S3.

Per aggiornare un modello simile configurato associato in AWS Clean Rooms

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Modellazione ML.
3. Nella scheda Modelli simili configurati, scegli un modello simile configurato e seleziona Modifica.
4. Per Configura il modello simile, per i dettagli del modello simile configurato:
    a. Scegli il modello Lookalike che desideri configurare dall'elenco a discesa.
    b. Scegli la dimensione minima del seme corrispondente che desideri. Questo è il numero minimo di utenti nei dati del fornitore di dati iniziali che si sovrappongono agli utenti nei dati di addestramento. Questo valore deve essere maggiore di 0.

5. Per condividere Metrics con altri membri, scegli se desideri che il fornitore di dati iniziali che collabora riceva le metriche del modello, compresi i punteggi di pertinenza.
6. Per la posizione di destinazione del segmento Lookalike, inserisci il bucket Amazon S3 in cui viene esportato il segmento Lookalike. Questo bucket deve trovarsi nella stessa regione delle altre risorse.
7. Per Accesso al servizio, scegli il nome del ruolo di servizio esistente che verrà utilizzato per accedere a questa tabella.
8. Per la configurazione avanzata delle dimensioni dei contenitori, scegli come desideri configurare le dimensioni dei contenitori per destinatari.
9. Seleziona Salvataggio delle modifiche.

Per l'azione API corrispondente, consulta UpdateConfiguredAudienceModel.

Utilizzo di segmenti simili (fornitore di dati iniziali)

Crea un segmento simile

Un segmento simile è un sottoinsieme dei dati di addestramento che più assomiglia ai dati iniziali.

Per creare un segmento simile in AWS Clean Rooms

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Nella scheda Con iscrizione attiva, scegli una collaborazione.
4. Nella scheda ML Modeling, scegli Crea segmento simile.
5. Per Crea un segmento simile, per i dettagli del segmento simile inserisci un nome e una descrizione facoltativa.
6. Per i profili Seed, scegli la fonte di input Amazon S3 in cui sono archiviati i dati dei seed.
7. Per l'accesso al servizio, scegli il nome del ruolo di servizio esistente che verrà utilizzato per accedere a questa tabella.
8. Se desideri abilitare i tag per il set di dati di addestramento, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.
9. Scegli Crea un segmento simile.

Per l'azione API corrispondente, consulta. StartAudienceGenerationJob

Esporta un segmento simile

Dopo aver creato un segmento simile, puoi esportare i dati in un bucket Amazon S3.

Per esportare un segmento simile in AWS Clean Rooms

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Nella scheda Con iscrizione attiva, scegli una collaborazione.
4. Nella scheda ML Modeling, seleziona un segmento simile e scegli Esporta.
5. Per Esporta modello simile, per Esporta dettagli del modello simile, inserisci un nome e una descrizione opzionale.
6. Per Dimensioni del segmento, scegli la dimensione desiderata per il segmento esportato.
7. Scegli Export (Esporta).

Per l'azione API corrispondente, consulta StartAudienceExportJob.

Passaggi successivi

Ora che avete creato un modello simile ed esportato un segmento iniziale, siete pronti per:

- Manage (Gestione) AWS Clean Rooms

Elaborazione crittografica per Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) è una funzionalità AWS Clean Rooms che può essere utilizzata in aggiunta alle regole di analisi. Con C3R, le organizzazioni possono riunire dati sensibili per ricavare nuove informazioni dall'analisi dei dati, limitando al contempo crittograficamente ciò che può essere appreso da qualsiasi parte del processo. C3R può essere utilizzato da due o più parti che desiderano collaborare con i propri dati sensibili ma sono tenute a utilizzare solo dati crittografati nel cloud.

Il client di crittografia C3R è uno strumento di crittografia lato client che è possibile utilizzare per crittografare i dati per utilizzarli. AWS Clean Rooms Quando si utilizza il client di crittografia C3R, i dati rimangono protetti crittograficamente durante l'uso in una collaborazione. AWS Clean Rooms Come in una normale AWS Clean Rooms collaborazione, i dati di input sono tabelle di database relazionali e il calcolo viene espresso come una query SQL. Tuttavia, C3R supporta solo un sottoinsieme limitato di query SQL su dati crittografati.

In particolare, C3R supporta SQL JOIN e SELECT istruzioni su dati protetti crittograficamente. Ogni colonna della tabella di input può essere utilizzata esattamente in uno dei seguenti tipi di istruzioni SQL:

- Le colonne protette crittograficamente per l'uso nelle JOIN istruzioni sono chiamate fingerprint colonne.
- Le colonne protette crittograficamente per l'uso nelle SELECT istruzioni vengono chiamate colonne. sealed
- Le colonne che non sono protette crittograficamente per l'uso nelle SELECT istruzioni JOIN o nelle istruzioni vengono chiamate colonne. cleartext

In alcuni casi, GROUP BY le istruzioni sono supportate su fingerprint colonne. Per ulteriori informazioni, consulta Fingerprintcolonne. Attualmente, C3R non supporta l'uso di altri costrutti SQL su dati crittografati, come WHERE clausole o funzioni aggregate come SUM eAVERAGE, anche se sarebbero altrimenti consentiti dalle regole di analisi pertinenti.

C3R è progettato per proteggere i dati nelle singole celle di una tabella. Utilizzando la configurazione predefinita per C3R, i dati sottostanti che un cliente mette a disposizione di terzi tramite una collaborazione rimangono crittografati mentre il contenuto è in uso all'interno. AWS Clean Rooms C3R utilizza la crittografia AES-GCM standard del settore per tutte le sealed colonne e una funzione

pseudocasuale standard del settore, nota come codice di autenticazione dei messaggi basato su hash (HMAC), per proteggere le colonne. fingerprint

Sebbene C3R crittografi i dati nelle tabelle, è ancora possibile dedurre le seguenti informazioni:

- Informazioni sulle tabelle stesse, incluso il numero di colonne, i nomi delle colonne e il numero di righe della tabella.
- Come con la maggior parte delle forme di crittografia standard, C3R non cerca di nascondere la lunghezza dei valori crittografati. C3R offre la possibilità di aggiungere valori crittografati per nascondere la lunghezza esatta dei testi in chiaro. Tuttavia, un limite superiore alla lunghezza dei testi in chiaro in ogni colonna potrebbe comunque essere rivelato a un'altra parte.
- Informazioni a livello di registrazione, ad esempio quando una determinata riga è stata aggiunta a una tabella C3R crittografata.

Per ulteriori informazioni su C3R, consultate i seguenti argomenti.

Argomenti

Considerazioni sull'utilizzo del calcolo crittografico per Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) mira a massimizzare la protezione dei dati. Tuttavia, alcuni casi d'uso potrebbero trarre vantaggio da livelli inferiori di protezione dei dati in cambio di funzionalità aggiuntive. È possibile apportare questi compromessi specifici modificando C3R dalla sua configurazione più sicura. In qualità di cliente, dovreste essere consapevoli di

questi compromessi e determinare se sono appropriati per il vostro caso d'uso. I compromessi da considerare includono quanto segue:

Argomenti

- Consentire l'inserimento di dati misti cleartext e crittografati nelle tabelle
- Consentire valori ripetuti nelle fingerprint colonne
- Allentamento delle restrizioni sul modo in cui fingerprint vengono denominate le colonne
- Determinazione della modalità di rappresentazione NULL dei valori

Per ulteriori informazioni su come impostare i parametri per questi scenari, vedere. Parametri di calcolo crittografico

Consentire l'inserimento di dati misti cleartext e crittografati nelle tabelle

La crittografia di tutti i dati lato client offre la massima protezione dei dati. Tuttavia, ciò limita determinati tipi di interrogazioni (ad esempio, la funzione di SUM aggregazione). Il rischio di consentire cleartext i dati è che è possibile che chiunque abbia accesso alle tabelle crittografate possa dedurre alcune informazioni sui valori crittografati. Ciò potrebbe essere fatto eseguendo un'analisi statistica sui cleartext dati associati.

Ad esempio, immagina di avere le colonne di `City` e`State`. La `City` colonna è cleartext e la `State` colonna è crittografata. Quando vedi il valore `Chicago` nella `City` colonna, ciò ti aiuta a determinare con alta probabilità che `State` è`Illinois`. Al contrario, se una colonna è `City` e l'altra lo è`EmailAddress`, cleartext `City` è improbabile che a riveli qualcosa su una colonna crittografata`EmailAddress`.

Per ulteriori informazioni sul parametro per questo scenario, vedereParametro Allow columns cleartext.

Consentire valori ripetuti nelle fingerprint colonne

Per un approccio più sicuro, assumiamo che ogni fingerprint colonna contenga esattamente un'istanza di una variabile. Nessun elemento può essere ripetuto in una fingerprint colonna. Il client di crittografia C3R mappa questi cleartext valori in valori unici che sono indistinguibili dai valori casuali. Pertanto, è impossibile dedurre informazioni su di da questi valori casuali. cleartext

Il rischio di valori ripetuti in una fingerprint colonna è che valori ripetuti si traducano in valori ripetuti dall'aspetto casuale. Pertanto, chiunque abbia accesso alle tabelle crittografate potrebbe, in teoria,

eseguire un'analisi statistica delle fingerprint colonne che potrebbe rivelare informazioni sui valori. cleartext

Ancora una volta, supponiamo che la fingerprint colonna sia `State` e che ogni riga della tabella corrisponda a una famiglia statunitense. Effettuando un'analisi della frequenza, si potrebbe dedurre quale stato è `California` e quale è `Wyoming` con alta probabilità. Questa inferenza è possibile perché `California` ha molti più residenti di. `Wyoming` Al contrario, supponiamo che la fingerprint colonna si trovi su un identificativo della famiglia e che ogni famiglia sia apparsa nel database da 1 a 4 volte in un database di milioni di voci. È improbabile che un'analisi della frequenza possa rivelare informazioni utili.

Per ulteriori informazioni sul parametro per questo scenario, consultaParametro Consenti duplicati.

Allentamento delle restrizioni sul modo in cui fingerprint vengono denominate le colonne

Per impostazione predefinita, si presume che quando due tabelle vengono unite utilizzando fingerprint colonne crittografate, tali colonne abbiano lo stesso nome in ogni tabella. Il motivo tecnico di questo risultato è che, per impostazione predefinita, deriviamo una chiave crittografica diversa per crittografare ogni colonna. fingerprint Tale chiave deriva da una combinazione della chiave segreta condivisa per la collaborazione e del nome della colonna. Se proviamo a unire due colonne con nomi di colonna diversi, deriviamo chiavi diverse e non possiamo calcolare un join valido.

Per risolvere questo problema, puoi disattivare la funzionalità che ricava le chiavi dal nome di ogni colonna. Quindi, il client di crittografia C3R utilizza un'unica chiave derivata per tutte le colonne. fingerprint Il rischio è che si possa eseguire un altro tipo di analisi della frequenza che potrebbe rivelare informazioni.

Usiamo nuovamente l'`State`esempio `City` and. Se ricaviamo gli stessi valori casuali per ogni fingerprint colonna (non incorporando il nome della colonna). `New York`ha lo stesso valore casuale nelle colonne `City` and`State`. New York è una delle poche città degli Stati Uniti in cui il `City` nome è uguale al `State` nome. Al contrario, se il set di dati ha valori completamente diversi in ogni colonna, non viene divulgata alcuna informazione.

Per ulteriori informazioni sul parametro per questo scenario, vedere. Consenti colonne con JOIN nomi diversi (parametro)

Determinazione della modalità di rappresentazione NULL dei valori

L'opzione disponibile è se elaborare i valori crittograficamente (cifrare e HMAC) come qualsiasi altro NULL valore. Se non elaborate NULL i valori come qualsiasi altro valore, è possibile che vengano rivelate delle informazioni.

Ad esempio, supponiamo che NULL nella `Middle Name` colonna in si cleartext indichino persone senza secondi nomi. Se non si crittografano questi valori, si rivelano quali righe della tabella crittografata vengono utilizzate per le persone senza secondi nomi. Queste informazioni potrebbero essere un segnale identificativo per alcune persone in alcune popolazioni. Ma se si elaborano NULL valori crittograficamente, alcune query SQL agiscono in modo diverso. Ad esempio, le GROUP BY clausole non fingerprint NULL raggrupperanno i valori in colonne. fingerprint

Per ulteriori informazioni sul parametro per questo scenario, vedere. Parametro NULL Mantiene i valori

Tipi di file e dati supportati in Cryptographic Computing per Clean Rooms

Il client di crittografia C3R riconosce i seguenti tipi di file:

- File CSV
- Parquetfile

È possibile utilizzare il `--fileFormat` flag nel client di crittografia C3R per specificare un formato di file in modo esplicito. Se specificato in modo esplicito, il formato del file non è determinato dall'estensione del file.

Argomenti

- File CSV
- Parquetfile
- Crittografia di valori non stringhe

File CSV

Si presume che un file con estensione.csv sia in formato CSV e contenga testo con codifica UTF-8. Il client di crittografia C3R tratta tutti i valori come stringhe.

Proprietà supportate nei file.csv

Il client di crittografia C3R richiede che i file.csv abbiano le seguenti proprietà:

- Potrebbe contenere o meno una riga di intestazione iniziale che nomina in modo univoco ogni colonna.
- Delimitato da virgole. (Attualmente, i delimitatori personalizzati non sono supportati.)
- Testo con codifica UTF-8.

Riduzione degli spazi bianchi dalle voci in formato.csv

Sia gli spazi bianchi iniziali che quelli finali vengono eliminati dalle voci in formato.csv.

Codifica personalizzata per un file.csv NULL

Un file.csv può utilizzare una codifica personalizzata. NULL

Con il client di crittografia C3R, è possibile specificare codifiche personalizzate per le NULL voci nei dati di input utilizzando il flag. `--csvInputNULLValue=<csv-input-null>` Il client di crittografia C3R può utilizzare codifiche personalizzate nel file di output generato per le voci NULL utilizzando il flag. `--csvOutputNULLValue=<csv-output-null>`

> **Note**
>
> Una NULL voce è considerata priva di contenuto, in particolare nel contesto di un formato tabulare più ricco come una tabella SQL. Sebbene .csv non supporti esplicitamente questa caratterizzazione per ragioni storiche, è una convenzione comune considerare come tale una voce vuota che contiene solo spazi bianchi. NULL Pertanto, questo è il comportamento predefinito del client di crittografia C3R e può essere personalizzato in base alle esigenze.

Come vengono interpretate le voci in formato.csv da C3R

La tabella seguente fornisce esempi di come le voci in formato.csv vengono organizzate (cleartextper maggiore chiarezza) in base cleartext ai valori (se presenti) forniti per i flag and. `--csvInputNULLValue=<csv-input-null>` `--csvOutputNULLValue=<csv-output-null>` Gli spazi bianchi iniziali e finali al di fuori delle virgolette vengono tagliati prima che C3R interpreti il significato di qualsiasi valore.

<csv-input-null>	**<csv-output-null>**	Inserimento di input	Entrata in uscita
Nessuno	Nessuna	,AnyProduct,	,AnyProduct,
Nessuna	Nessuna	, AnyProduct ,	,AnyProduct,
Nessuna	Nessuna	,"AnyProduct",	,AnyProduct,
Nessuna	Nessuna	, "AnyProduct" ,	,AnyProduct,
Nessuna	Nessuna	,,	,,
Nessuna	Nessuna	, ,	,,
Nessuna	Nessuna	,"",	,,
Nessuna	Nessuna	," ",	," ",
Nessuna	Nessuna	, " " ,	," ",
"AnyProduct"	"NULL"	,AnyProduct,	,NULL,
"AnyProduct"	"NULL"	, AnyProduct ,	,NULL,
"AnyProduct"	"NULL"	,"AnyProduct",	,NULL,
"AnyProduct"	"NULL"	, "AnyProduct" ,	,NULL,
Nessuna	"NULL"	,,	,NULL,
Nessuna	"NULL"	, ,	,NULL,
Nessuna	"NULL"	,"",	,NULL,
Nessuna	"NULL"	," ",	," ",
Nessuno	"NULL"	, " " ,	," ",
""	"NULL"	,,	,NULL,

<csv-input-null>	**<csv-output-null>**	Inserimento di input	Entrata in uscita
""	"NULL"	, ,	,NULL,
""	"NULL"	,"",	,"",
""	"NULL"	," ",	," ",
""	"NULL"	, " " ,	," ",
"\"\""	"NULL"	,,	,,
"\"\""	"NULL"	, ,	,,
"\"\""	"NULL"	,"",	,NULL,
"\"\""	"NULL"	," ",	," ",
"\"\""	"NULL"	, " " ,	," ",

File CSV senza intestazioni

Non è necessario che il file.csv di origine contenga intestazioni nella prima riga che denominano in modo univoco ogni colonna. Tuttavia, un file.csv senza una riga di intestazione richiede uno schema di crittografia posizionale. Lo schema di crittografia posizionale è richiesto al posto del tipico schema mappato utilizzato sia per i file.csv con una riga di intestazione che per i file. Parquet

Uno schema di crittografia posizionale specifica le colonne di output per posizione anziché per nome. Uno schema di crittografia mappato associa i nomi delle colonne di origine ai nomi delle colonne di destinazione. Per ulteriori informazioni, inclusa una discussione dettagliata ed esempi di entrambi i formati di schema, vedereSchemi di tabelle mappati e posizionali.

Parquetfile

Si presume che un file con .parquet estensione sia nel Apache Parquet formato.

Tipi di Parquet dati supportati

Il client di crittografia C3R può elaborare qualsiasi dato non complesso (ovvero di tipo primitivo) in un Parquet file che rappresenta un tipo di dati supportato da. AWS Clean Rooms

Tuttavia, solo le colonne di stringhe possono essere utilizzate per le colonne. sealed

Sono supportati i seguenti tipi di dati Parquet:

- `Binary`tipo primitivo con le seguenti annotazioni logiche:
  - Nessuno se `--parquetBinaryAsString` è impostato (tipo di `STRING` dati)
  - `Decimal(scale, precision)`(tipo di `DECIMAL` dati)
  - `String`(tipo di `STRING` dati)
- `Boolean`tipo di dati primitivo senza annotazioni logiche (tipo di `BOOLEAN` dati)
- `Double`tipo di dati primitivo senza annotazioni logiche (tipo di dati) `DOUBLE`
- `Fixed_Len_Binary_Array`tipo primitivo con annotazione `Decimal(scale, precision)` logica (tipo di dati) `DECIMAL`
- `Float`tipo di dati primitivo senza annotazioni logiche (tipo di dati) `FLOAT`
- `Int32`tipo primitivo con le seguenti annotazioni logiche:
  - Nessuno (tipo di `INT` dati)
  - `Date`(tipo di `DATE` dati)
  - `Decimal(scale, precision)`(tipo di `DECIMAL` dati)
  - `Int(16, true)`(tipo di `SMALLINT` dati)
  - `Int(32, true)`(tipo di `INT` dati)
- `Int64`tipo di dati primitivo con le seguenti annotazioni logiche:
  - Nessuno (tipo di `BIGINT` dati)
  - `Decimal(scale, precision)`(tipo di `DECIMAL` dati)
  - `Int(64, true)`(tipo di `BIGINT` dati)
  - `Timestamp(isUTCAdjusted, TimeUnit.MILLIS)`(tipo di `TIMESTAMP` dati)
  - `Timestamp(isUTCAdjusted, TimeUnit.MICROS)`(tipo di `TIMESTAMP` dati)
  - `Timestamp(isUTCAdjusted, TimeUnit.NANOS)`(tipo di `TIMESTAMP` dati)

Crittografia di valori non stringhe

Attualmente, per le colonne sono supportati solo i valori di sealed stringa.

Per i file.csv, il client di crittografia C3R tratta tutti i valori come testo con codifica UTF-8 e non tenta di interpretarli in modo diverso prima della crittografia.

Per le colonne di impronte digitali, i tipi sono raggruppati in classi di equivalenza. Una classe di equivalenza è un insieme di tipi di dati che possono essere confrontati in modo inequivocabile per quanto riguarda l'uguaglianza tramite un tipo di dati rappresentativo.

Le classi di equivalenza consentono di assegnare impronte digitali identiche allo stesso valore semantico indipendentemente dalla rappresentazione originale. Tuttavia, lo stesso valore in due classi di equivalenza non darà come risultato la stessa colonna di impronte digitali.

Ad esempio, al `INTEGRAL` valore `42` verrà assegnata la stessa impronta digitale indipendentemente dal fatto che originariamente fosse un`SMALLINT`, `INT` o. `BIGINT` Inoltre, il `INTEGRAL` valore non `0` corrisponderà mai al `BOOLEAN` valore `FALSE` (che è rappresentato dal valore`0`).

Le seguenti classi di equivalenza e AWS Clean Rooms i tipi di dati corrispondenti sono supportati dalle colonne di impronte digitali:

Classe di equivalenza	Tipo di AWS Clean Rooms dat i supportato
`BOOLEAN`	`BOOLEAN`
`DATE`	`DATE`
`INTEGRAL`	`BIGINT`, `INT`, `SMALLINT`
`STRING`	`CHAR`, `STRING`, `VARCHAR`

Nomi delle colonne in Cryptographic Computing for Clean Rooms

Per impostazione predefinita, i nomi delle colonne sono importanti in Cryptographic Computing for. Clean Rooms

Se il valore del parametro Consenti JOIN colonne con nomi diversi è falso, i nomi delle colonne vengono utilizzati durante la crittografia delle fingerprint colonne. Per questo motivo, per impostazione

predefinita, i collaboratori devono coordinarsi in anticipo e utilizzare gli stessi nomi delle colonne di destinazione per i dati che utilizzeranno JOIN le istruzioni nelle query. Per impostazione predefinita, le colonne crittografate per JOIN con nomi diversi non funzionano correttamente JOIN su nessun valore.

Se il valore del parametro Allow JOIN of columns with different names è vero, JOIN le istruzioni tra le colonne crittografate come fingerprint colonne hanno esito positivo. La crittografia dei dati con questo parametro potrebbe consentire una certa inferenza dei cleartext valori. Ad esempio, se una riga ha lo stesso valore HMAC (Hash based Message Authentication Code) sia nella colonna che nella `City` `State` colonna, il valore potrebbe essere. `New York`

Normalizzazione dei nomi delle intestazioni delle colonne

I nomi delle intestazioni delle colonne vengono normalizzati dal client di crittografia C3R. Qualsiasi spazio bianco iniziale e finale viene rimosso e il nome della colonna viene reso minuscolo per l'output trasformato.

La normalizzazione viene applicata prima di tutti gli altri calcoli, calcoli o altre operazioni che potrebbero essere influenzate dai nomi delle colonne. Il file di output emesso contiene solo i nomi normalizzati.

Tipi di colonne nel calcolo crittografico per Clean Rooms

Questo argomento fornisce informazioni sui tipi di colonna in Cryptographic Computing for. Clean Rooms

Argomenti

- Fingerprintcolonne
- Colonne sigillate
- Cleartextcolonne

Fingerprintcolonne

Fingerprintle colonne sono colonne protette crittograficamente per l'uso nelle JOIN istruzioni.

I dati fingerprint delle colonne non possono essere decrittografati. Solo i dati delle colonne sigillate possono essere decrittografati.

Fingerprintle colonne devono essere utilizzate solo nelle seguenti clausole e funzioni SQL:

- JOIN (INNER, OUTER, LEFT, RIGHT, or FULL)rispetto ad altre colonnefingerprint:
  - Se il valore del `allowJoinsOnColumnsWithDifferentNames` parametro è impostato su`false`, entrambe fingerprint le colonne JOIN devono avere lo stesso nome.
- `SELECT COUNT()`
- `SELECT COUNT(DISTINCT )`
- `GROUP BY`(Utilizzare solo se la collaborazione ha impostato il valore del `preserveNulls` parametro su`true`.)

Le query che violano questi vincoli potrebbero produrre risultati errati.

Colonne sigillate

Le colonne sigillate sono colonne protette crittograficamente per essere utilizzate nelle SELECT istruzioni.

Le colonne sigillate devono essere utilizzate solo nelle seguenti clausole e funzioni SQL:

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

> **Note**
>
> `SELECT COUNT(DISTINCT )` non è supportato.

Le interrogazioni che violano questi vincoli potrebbero produrre risultati errati.

Inserimento dei dati di una colonna prima della crittografia sealed

Quando specificate che una colonna deve essere una sealed colonna, C3R vi chiede che tipo di riempimento scegliere. L'imbottitura dei dati prima della crittografia è facoltativa. Senza imbottitura (un tipo di padnone), la lunghezza dei dati crittografati indica la dimensione di. cleartext In alcune circostanze, la dimensione di cleartext potrebbe esporre il testo in chiaro. Con il padding (un tipo di pad di `fixed` or`max`), tutti i valori vengono prima aggiunti a una dimensione comune e poi

crittografati. Con il padding, la lunghezza dei dati crittografati non fornisce informazioni sulla cleartext lunghezza originale, a parte fornire un limite superiore alla loro dimensione.

Se desideri il padding per una colonna e conosci la lunghezza massima in byte dei dati in quella colonna, usa il padding. `fixed` Utilizzate un `length` valore che sia almeno pari alla lunghezza in byte del valore più lungo in quella colonna.

> **Note**
>
> Si verifica un errore e la crittografia fallisce se un valore è più lungo di quello fornito. `length`

Se desideri il riempimento per una colonna e la lunghezza massima in byte dei dati in quella colonna non è nota, usa il padding. `max` Questa modalità di riempimento inserisce tutti i dati in base alla lunghezza del valore più lungo più byte aggiuntivi. `length`

> **Note**
>
> Potresti voler crittografare i dati in batch o aggiornare periodicamente le tabelle con nuovi dati. Tieni presente che il `max` riempimento riempirà le voci in base alla lunghezza (più `length` byte) della voce di testo in chiaro più lunga di un determinato batch. Ciò significa che la lunghezza del testo cifrato può variare da batch a batch. Pertanto, se conosci la lunghezza massima in byte per una colonna, dovresti usare invece di. `fixed` `max`

Cleartextcolonne

Cleartextle colonne sono colonne che non sono protette crittograficamente per essere utilizzate nelle istruzioni JOIN oSELECT.

Cleartextle colonne possono essere utilizzate in qualsiasi parte della query SQL.

Parametri di calcolo crittografico

I parametri di calcolo crittografico sono disponibili per le collaborazioni che utilizzano Cryptographic Computing for Clean Rooms (C3R) durante la creazione di una collaborazione. È possibile creare una collaborazione utilizzando la AWS Clean Rooms console o l'operazione API. `CreateCollaboration` Nella console, è possibile impostare i valori per i parametri in Parametri

di calcolo crittografico dopo aver attivato l'opzione Support cryptographic computing. Per ulteriori informazioni, consulta i seguenti argomenti.

Argomenti

Parametro Allow columns cleartext

Nella console, puoi impostare il parametro Allow cleartextcolumns durante la creazione di una collaborazione per specificare se cleartext i dati sono consentiti in una tabella con dati crittografati.

La tabella seguente descrive i valori per il parametro Allow cleartext columns.

Valore del parametro	Descrizione
No	Cleartextle colonne non sono consentite nella tabella crittogra fata. Tutti i dati sono protetti crittograficamente.
Sì	Cleartextle colonne sono consentite nella tabella crittografata. Cleartextle colonne non sono protette crittograficamente e sono incluse come. cleartext È necessario prendere nota di ciò che i cleartext dati delle righe potrebbero rivelare sugli altri dati della tabella. Per essere eseguite SUM o AVG su colonne specifiche, le colonne devono essere inserite. cleartext

Utilizzando l'operazione `CreateCollaboration` API, per il `dataEncryptionMetadata` parametro è possibile impostare il valore di `allowCleartext` to `true` o`false`. Per ulteriori informazioni sulle operazioni API, consulta l'AWS Clean Rooms API Reference.

Cleartextle colonne corrispondono alle colonne classificate secondo lo cleartext schema specifico della tabella. I dati in queste colonne non sono crittografati e possono essere utilizzati in qualsiasi

modo. Cleartextle colonne possono essere utili se i dati non sono sensibili e/o se è necessaria una maggiore flessibilità rispetto a quella consentita da una sealed colonna o una fingerprint colonna crittografate.

Parametro Consenti duplicati

Nella console, è possibile impostare il parametro Allow duplicates durante la creazione di una collaborazione per specificare se le colonne crittografate per le JOIN query possono contenere valori non duplicati. NULL

> **Important**
>
> I parametri Allow duplicates, Allow JOIN of columns with different names e Preserve NULL values hanno effetti separati ma correlati.

La tabella seguente descrive i valori per il parametro Allow duplicates.

Valore del parametro	Descrizione
No	I valori ripetuti non sono consentiti in una fingerprint colonna. Tutti i valori in una singola fingerprint colonna devono essere univoci.
Sì	I valori ripetuti sono consentiti in una fingerprint colonna. Se devi unire colonne con valori ripetuti, imposta questo valore su Sì. Se impostato su Sì, i modelli di frequenza che appaiono nelle fingerprint colonne della tabella o dei risultati C3R potrebbero implicare alcune informazioni aggiuntive sulla struttura dei dati. cleartext

Utilizzando l'operazione `CreateCollaboration` API, per il `dataEncryptionMetadata` parametro è possibile impostare il valore di o. `allowDuplicates` `true` `false` Per ulteriori informazioni sulle operazioni API, consulta l'AWS Clean Rooms API Reference.

Per impostazione predefinita, se è necessario utilizzare dati crittografati nelle JOIN query, il client di crittografia C3R richiede che tali colonne non contengano valori duplicati. Questo requisito è uno

sforzo per aumentare la protezione dei dati. Questo comportamento può aiutare a garantire che i modelli ripetuti nei dati non siano osservabili. Tuttavia, se desideri utilizzare dati crittografati nelle JOIN query e non ti preoccupi dei valori duplicati, il parametro Allow duplicates può disabilitare questo controllo conservativo.

Consenti colonne con JOIN nomi diversi (parametro)

Nella console, puoi impostare il parametro Consenti colonne con nomi diversi durante la creazione JOIN di una collaborazione per specificare se sono supportate JOIN istruzioni tra colonne con nomi diversi.

Per ulteriori informazioni, consulta Normalizzazione dei nomi delle intestazioni delle colonne

La tabella seguente descrive i valori per il parametro Allow JOIN of columns with different names.

Valore del parametro	Descrizione
No	Le unioni di fingerprint colonne con nomi diversi non sono supportate. JOINIe istruzioni forniscono risultati accurati solo su colonne con lo stesso nome. **Important** Il valore No offre una maggiore sicurezza delle informazioni, ma richiede che i partecipanti alla collaborazione concordino in precedenza sui nomi delle colonne. Se due colonne hanno nomi diversi quando sono crittografate come fingerprint colonne e l'opzione Consenti JOIN colonne con nomi diversi è impostata su No, JOIN le istruzioni su tali colonne non producono risultati. Questo perché nessun valore dopo la crittogra fia viene condiviso tra di loro.
Sì	Sono supportate le unioni di fingerprint colonne con nomi diversi. Per una maggiore flessibilità, gli utenti possono impostare questo valore su Sì, che consente JOIN le istruzioni sulle colonne indipendentemente dal nome della colonna.

Valore del parametro	Descrizione
	Se impostato su Sì, il client di crittografia C3R non considera il nome della colonna durante la protezione fingerprint delle colonne. Di conseguenza, i valori comuni tra diverse fingerprint colonne sono osservabili nella tabella C3R. Ad esempio, se una riga ha lo stesso JOIN valore crittografato sia in una `City` colonna che in una `State` colonna, potrebbe essere ragionevole dedurre che il valore sia. `New York`

Utilizzando l'operazione `CreateCollaboration` API, per il `dataEncryptionMetadata` parametro è possibile impostare il valore `allowJoinsOnColumnsWithDifferentNames` di `true` o`false`. Per ulteriori informazioni sulle operazioni API, consulta l'AWS Clean Rooms API Reference.

Per impostazione predefinita, la crittografia delle fingerprint colonne è influenzata dall'impostazione `targetHeader` for that column, impostata inFase 4: Generazione di uno schema di crittografia per un file tabulare . Pertanto, lo stesso cleartext valore ha diverse rappresentazioni crittografate in ogni fingerprint colonna diversa per cui è crittografato.

Questo parametro può essere utile per impedire l'inferenza di cleartext valori in alcuni casi. Ad esempio, viene visualizzato lo stesso valore crittografato in fingerprint colonne `City` e `State` potrebbe essere utilizzato per dedurre ragionevolmente che il valore è. `New York` Tuttavia, l'uso di questo parametro richiede un coordinamento aggiuntivo in anticipo, in modo che tutte le colonne da unire nelle query abbiano nomi condivisi.

È possibile utilizzare il parametro Consenti JOIN colonne con nomi diversi per allentare questa restrizione. Quando il valore del parametro è impostato su`Yes`, consente di utilizzare insieme tutte le colonne crittografate indipendentemente dal nome. JOIN

Parametro NULL Mantiene i valori

Nella console, puoi impostare il parametro Preserve NULL values quando crei una collaborazione per indicare che non è presente alcun valore per quella colonna.

La tabella seguente descrive i valori per il parametro Preserve NULL values.

Valore del parametro	Descrizione
No	NULLi valori non vengono conservati. NULLi valori non vengono visualizzati come NULL in una tabella crittografata. NULLi valori vengono visualizzati come valori casuali unici in una tabella C3R.
Sì	NULLi valori vengono preservati. NULLi valori vengono visualizzati come NULL in una tabella crittografata. Se è necessaria la semantica SQL dei NULL valori, è possibile impostare questo valore su Sì. Di conseguenza, NULL le voci vengono visualizzate come NULL nella tabella C3R, indipendentemente dal fatto che la colonna sia crittografata e indipendentemente dall'impostazione del parametro Consenti duplicati.

Utilizzando l'operazione `CreateCollaboration` API, per il `dataEncryptionMetadata` parametro, è possibile impostare il valore di `preserveNulls` o. `true` `false` Per ulteriori informazioni sulle operazioni API, consulta l'AWS Clean Rooms API Reference.

Quando il parametro Preserve NULL values è impostato su No per la collaborazione:

1. NULLLe voci nelle `cleartext` colonne rimangono invariate.
2. NULLLe voci nelle `fingerprint` colonne crittografate vengono crittografate come valori casuali per nasconderne il contenuto. L'unione su una colonna crittografata con le NULL voci presenti nella cleartext colonna non produce alcuna corrispondenza per nessuna delle NULL voci. Non vengono effettuate corrispondenze perché ognuna di esse riceve il proprio contenuto casuale unico.
3. NULLLe voci nelle `sealed` colonne crittografate sono crittografate.

Quando il valore del parametro Preserve NULL values è impostato su Sì per la collaborazione, le NULL voci di tutte le colonne rimangono invariate NULL indipendentemente dal fatto che la colonna sia crittografata.

Il parametro Preserve NULL values è utile in scenari come l'arricchimento dei dati, in cui si desidera condividere una mancanza di informazioni espressa comeNULL. Il parametro Preserve NULL values

è utile anche nel formato HMAC se nella colonna desiderata sono presenti NULL valori fingerprint o. JOIN GROUP BY

Se il valore dei parametri Allow duplicates e Preserve NULL values è impostato su No, la presenza di più NULL voci in una fingerprint colonna genera un errore e interrompe la crittografia. Se il valore di uno dei parametri è impostato su Sì, non si verifica alcun errore di questo tipo.

Flag opzionali in Cryptographic Computing per Clean Rooms

Le sezioni seguenti descrivono i flag opzionali che è possibile impostare quando si crittografano i dati utilizzando il client di crittografia C3R per la personalizzazione e il test dei file tabulari.

Argomenti

`--csvInputNULLValue`contrassegnare

È possibile utilizzare il `--csvInputNULLValue` flag per specificare codifiche personalizzate per le NULL voci nei dati di input quando si crittografano i dati utilizzando il client di crittografia C3R.

La tabella seguente riassume l'utilizzo e i parametri di questo flag.

Utilizzo	Parametri
Facoltativo. Gli utenti possono specificare codifiche personalizzate per le NULL voci nei dati di input.	Codifica dei NULL valori specificata dall'utente nel file CSV di input

Una NULL voce è una voce considerata priva di contenuto, in particolare nel contesto di un formato tabulare più ricco come una tabella SQL. Sebbene .csv non supporti esplicitamente questa caratterizzazione per ragioni storiche, è una convenzione comune considerare come tale una voce

vuota contenente solo spazi bianchi. NULL Pertanto, questo è il comportamento predefinito del client di crittografia C3R e può essere personalizzato in base alle esigenze.

`--csvOutputNULLValue`contrassegnare

È possibile utilizzare il `--csvOutputNULLValue` flag per specificare codifiche personalizzate per le NULL voci nei dati di output quando si crittografano i dati utilizzando il client di crittografia C3R.

La tabella seguente riassume l'utilizzo e i parametri di questo flag.

Utilizzo	Parametri
Facoltativo. Gli utenti possono specificare codifiche personalizzate nel file di output generato per le NULL voci.	Codifica specificata dall'utente dei NULL valori nel file CSV di output

Una NULL voce è una voce considerata priva di contenuto, in particolare nel contesto di un formato tabulare più ricco come una tabella SQL. Sebbene .csv non supporti esplicitamente questa caratterizzazione per ragioni storiche, è una convenzione comune considerare come tale una voce vuota contenente solo spazi bianchi. NULL Pertanto, questo è il comportamento predefinito del client di crittografia C3R e può essere personalizzato in base alle esigenze.

`--enableStackTraces`contrassegnare

Quando crittografate i dati utilizzando il client di crittografia C3R, utilizzate il `--enableStackTraces` flag per fornire informazioni contestuali aggiuntive per la segnalazione degli errori quando C3R rileva un errore.

AWS non raccoglie errori. Se riscontri un errore, usa lo stack trace per risolvere tu stesso l'errore o invia lo stack trace a per ricevere assistenza. AWS Support

La tabella seguente riassume l'utilizzo e i parametri di questo flag.

Utilizzo	Parametri
Facoltativo. Utilizzato per fornire informazioni contestuali aggiuntive per la segnalazione degli	Nessuno

Utilizzo	Parametri
errori quando il client di crittografia C3R rileva un errore.	

`--dryRun`contrassegnare

I comandi del client di crittografia C3R per crittografare e decrittografare includono un flag opzionale. `--dryRun` Il flag accetta tutti gli argomenti forniti dall'utente e ne verifica la validità e la coerenza.

È possibile utilizzare il `--dryRun` flag per verificare se il file di schema è valido e coerente con il file di input corrispondente.

La tabella seguente riassume l'utilizzo e i parametri di questo flag.

Utilizzo	Parametri
Facoltativo. Fa sì che il client di crittografia C3R analizzi i parametri e controlli i file, ma non esegue alcuna crittografia o decrittografia.	Nessuno

`--tempDir`contrassegnare

Potresti voler usare una directory temporanea perché i file crittografati a volte possono avere dimensioni maggiori dei file non crittografati, a seconda delle relative impostazioni. Inoltre, i set di dati devono essere crittografati per ogni collaborazione per funzionare correttamente.

Quando crittografate i dati utilizzando C3R, utilizzate il `--tempDir` flag per specificare la posizione in cui è possibile creare i file temporanei durante l'elaborazione dell'input.

La tabella seguente riassume l'utilizzo e i parametri di questo flag.

Utilizzo	Parametri
Gli utenti possono specificare la posizione in cui possono essere creati i file temporanei durante l'elaborazione dell'input.	L'impostazione predefinita è la directory temporanea del sistema.

Interrogazioni con calcolo crittografico per Clean Rooms

Questo argomento fornisce informazioni sulla scrittura di query che utilizzano tabelle di dati che sono state crittografate utilizzando Cryptographic Computing for. Clean Rooms

Argomenti

Interrogazioni che si estendono su NULL

Avere un ramo di query su un'NULListruzione significa usare una sintassi come. `IF x IS NULL THEN 0 ELSE 1`

Le interrogazioni possono sempre basarsi su NULL istruzioni disposte in cleartext colonne.

Le query possono diramarsi su NULL istruzioni in sealed colonne e fingerprint colonne solo quando il valore del parametro Preserve NULL values (`preserveNulls`) è impostato su. `true`

Le query che violano questi vincoli potrebbero produrre risultati errati.

Mappatura di una colonna di origine su più colonne di destinazione

Una colonna di origine può essere mappata su più colonne di destinazione. Ad esempio, potresti voler eseguire entrambe le operazioni JOIN e SELECT su una colonna.

Per ulteriori informazioni, consulta Utilizzo degli stessi dati per entrambe JOIN le SELECT query.

Utilizzo degli stessi dati per entrambe JOIN le SELECT query

Se i dati di una colonna non sono sensibili, possono essere visualizzati in una colonna di cleartext destinazione, il che consente di utilizzarli per qualsiasi scopo.

Se i dati in una colonna sono riservati e devono essere utilizzati per entrambe le JOIN SELECT query, mappate la colonna di origine su due colonne di destinazione nel file di output. Una colonna viene crittografata con la colonna `type` come fingerprint colonna e una colonna viene crittografata con la `type` colonna sigillata. La generazione dello schema interattivo del client di crittografia C3R

suggerisce i suffissi di intestazione di and. `_fingerprint` `_sealed` Questi suffissi di intestazione possono essere una convenzione utile per differenziare rapidamente tali colonne.

Linee guida per il client di crittografia C3R

Il client di crittografia C3R è uno strumento che consente alle organizzazioni di riunire dati sensibili per ricavare nuove informazioni dall'analisi dei dati. Lo strumento limita crittograficamente ciò che può essere appreso da qualsiasi parte e durante il processo. AWS Sebbene ciò sia di vitale importanza, il processo di protezione crittografica dei dati può comportare un notevole sovraccarico sia in termini di risorse di elaborazione che di archiviazione. Pertanto, è importante comprendere i compromessi derivanti dall'utilizzo di ciascuna impostazione e come ottimizzare le impostazioni pur mantenendo le garanzie crittografiche desiderate. Questo argomento si concentra sulle implicazioni prestazionali delle diverse impostazioni nel client e negli schemi di crittografia C3R.

Tutte le impostazioni di crittografia del client di crittografia C3R offrono diverse garanzie crittografiche. Le impostazioni a livello di collaborazione sono le più sicure per impostazione predefinita. L'attivazione di funzionalità aggiuntive durante la creazione di una collaborazione indebolisce le garanzie di privacy, consentendo di condurre attività come l'analisi della frequenza sul testo cifrato. Per ulteriori informazioni su come vengono utilizzate queste impostazioni e quali sono le loro implicazioni, consulta. Calcolo crittografico

Argomenti

- Implicazioni sulle prestazioni per i tipi di colonna
- Risoluzione dei problemi relativi agli aumenti imprevisti delle dimensioni del testo cifrato

Implicazioni sulle prestazioni per i tipi di colonna

C3R utilizza tre tipi di colonne: cleartextfingerprint, e. sealed Ciascuno di questi tipi di colonna offre garanzie crittografiche diverse e ha diverse destinazioni d'uso. Nelle sezioni seguenti, vengono discusse le implicazioni prestazionali del tipo di colonna e l'impatto sulle prestazioni di ciascuna impostazione.

Argomenti

- Cleartextcolonne
- Fingerprintcolonne
- Sealedcolonne

Cleartextcolonne

Cleartextle colonne non vengono modificate rispetto al loro formato originale e non vengono elaborate crittograficamente in alcun modo. Questo tipo di colonna non può essere configurato e non influisce sulle prestazioni di archiviazione o di calcolo.

Fingerprintcolonne

Fingerprintle colonne sono pensate per essere utilizzate per unire dati su più tabelle. A tal fine, la dimensione del testo cifrato risultante deve essere sempre la stessa. Tuttavia, queste colonne sono influenzate dalle impostazioni a livello di collaborazione. Fingerprintle colonne possono avere diversi gradi di impatto sulla dimensione del file di output a seconda del contenuto nell'cleartextinput.

Argomenti

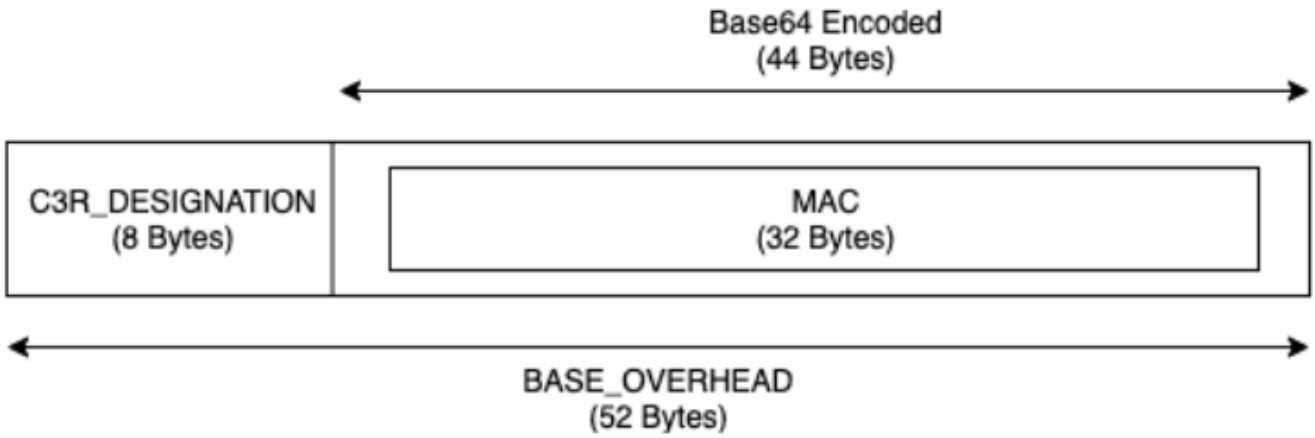
- Sovraccarico di base per le colonne fingerprint
- Impostazioni di collaborazione per le colonne fingerprint
- Dati di esempio per una fingerprint colonna
- colonne di risoluzione dei problemi fingerprint

Sovraccarico di base per le colonne fingerprint

C'è un sovraccarico di base per le fingerprint colonne. Questo sovraccarico è costante e sostituisce la dimensione dei cleartext byte.

I dati nelle fingerprint colonne vengono elaborati crittograficamente tramite una funzione HMAC (Message Authentication Code) basata su Hash, che trasforma i dati in un codice di autenticazione dei messaggi (MAC) a 32 byte. Questi dati vengono quindi elaborati tramite un codificatore base64, aggiungendo circa il 33 percento alla dimensione in byte. È preceduto da una designazione C3R a 8 byte per designare il tipo di colonna a cui appartengono i dati e la versione client che li ha prodotti. Il risultato finale è di 52 byte. Questo risultato viene quindi moltiplicato per il conteggio delle righe per ottenere il sovraccarico totale di base (usa il numero di `null` valori diversi totali se `preserveNulls` è impostato su true).

L'immagine seguente mostra come $BASE\_OVERHEAD = C3R\_DESIGNATION + (MAC * 1.33)$



Il testo cifrato in uscita nelle fingerprint colonne sarà sempre di 52 byte. Questa può essere una riduzione significativa dello spazio di archiviazione se la media cleartext dei dati di input supera i 52 byte (ad esempio, indirizzi completi). Questo può essere un aumento significativo dello spazio di archiviazione se la media cleartext dei dati di input è inferiore a 52 byte (ad esempio, l'età dei clienti).

Impostazioni di collaborazione per le colonne fingerprint

`preserveNulls`Impostazione

Quando l'impostazione a livello di collaborazione `preserveNulls` è `false` (impostazione predefinita), ogni `null` valore viene sostituito con 32 byte casuali univoci ed elaborato come se non lo fosse. `null` Il risultato è che ogni `null` valore è ora di 52 byte. Ciò può aggiungere requisiti di archiviazione significativi per le tabelle che contengono dati molto scarsi rispetto a quando questa impostazione è `true` e `null` i valori vengono passati come. `null`

Se non hai bisogno delle garanzie sulla privacy di questa impostazione e preferisci mantenere `null` i valori all'interno dei tuoi set di dati, abilita l'`preserveNulls`impostazione al momento della creazione della collaborazione. L'`preserveNulls`impostazione non può essere modificata dopo la creazione della collaborazione.

Dati di esempio per una fingerprint colonna

Di seguito è riportato un set di esempio di dati di input e output per una fingerprint colonna con impostazioni da riprodurre. Altre impostazioni a livello di collaborazione come `allowCleartext` e `allowDuplicates` non influiscono sui risultati e possono essere impostate come `true` o `false` se si tenta di riprodurre localmente.

Esempio di segreto condiviso: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Esempio di ID di collaborazione: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

allowJoinsOnColumnsWithDifferentNames: `True` questa impostazione non influisce sui requisiti di prestazioni o di archiviazione. Tuttavia, questa impostazione rende irrilevante la scelta del nome della colonna quando si riproducono i valori mostrati nelle tabelle seguenti.

Esempio 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministico	`Yes`
Byte di input	0
Byte di uscita	0

Esempio 2

Input	`null`
`preserveNulls`	`FALSE`
Output	`01:hmac:3lkFjthvV3IUu6mMvFc1a +XAHwgw/ElmOq4p3Yg25kk=`
Deterministico	No
Byte di input	0
Byte di uscita	52

Esempio 3

Input	`empty string`
`preserveNulls`	-

Output	`01:hmac:oKTgi3Gba+eUb3JteSz 2EMgXUkF1WgM77UP0Ydw5kPQ=`
Deterministico	`Yes`
Byte di input	0
Byte di uscita	52

Esempio 4

Input	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:hmac:kU/IqwG7FMmzzshr0B9 scomE0UJUEE7j9keTctplGww=`
Deterministico	`Yes`
Byte di input	26
Byte di uscita	52

Esempio 5

Input	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Output	`01:hmac:ks3htnQbw2vdhCRFF6J NzW5LMndJaHG57uvE26mBtSs=`
Deterministico	`Yes`
Byte di input	62

Byte di uscita	52

colonne di risoluzione dei problemi fingerprint

Perché il testo cifrato nelle mie fingerprint colonne è parecchie volte più grande della dimensione del testo in cleartext esse contenuto?

La lunghezza del testo cifrato in una fingerprint colonna è sempre di 52 byte. Se i dati di input erano piccoli (ad esempio, l'età dei clienti), mostreranno un aumento significativo delle dimensioni. Ciò può verificarsi anche se l'`preserveNulls`impostazione è impostata su`false`.

Perché il testo cifrato nelle mie fingerprint colonne è parecchie volte più piccolo della dimensione del testo in cleartext esse contenuto?

La lunghezza del testo cifrato in una fingerprint colonna è sempre di 52 byte. Se i dati di input erano di grandi dimensioni (ad esempio, gli indirizzi completi dei clienti), mostrerà una riduzione significativa delle dimensioni.

Come faccio a sapere se ho bisogno delle garanzie crittografiche fornite da? **`preserveNulls`**

Sfortunatamente, la risposta è che dipende. Come minimo, è the section called “Parametri” necessario verificare in che modo l'`preserveNulls`impostazione protegge i dati. Tuttavia, ti consigliamo di fare riferimento ai requisiti di gestione dei dati della tua organizzazione e agli eventuali contratti applicabili alla rispettiva collaborazione.

Perché devo sostenere il sovraccarico di base64?

Per consentire la compatibilità con i formati di file tabulari come CSV, è necessaria la codifica base64. Sebbene alcuni formati di file come quelli Parquet supportino le rappresentazioni binarie dei dati, è importante che tutti i partecipanti a una collaborazione rappresentino i dati nello stesso modo per garantire risultati di interrogazione corretti.

Sealedcolonne

Sealedle colonne sono pensate per il trasferimento di dati tra i membri di una collaborazione. Il testo cifrato in queste colonne non è deterministico e ha un impatto significativo sulle prestazioni e sullo storage in base alla configurazione delle colonne. Queste colonne possono essere configurate singolarmente e spesso hanno il maggiore impatto sulle prestazioni del client di crittografia C3R e sulla dimensione del file di output risultante.

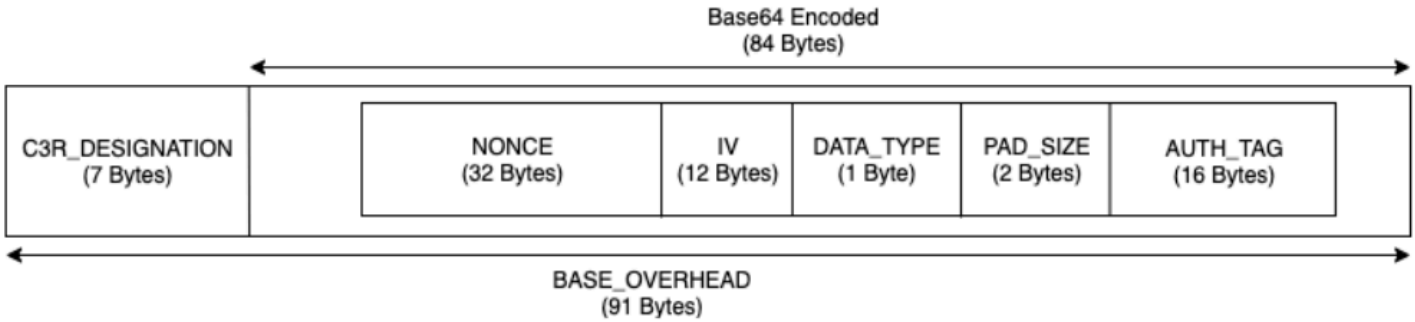
Argomenti

Sovraccarico di base per le colonne sealed

C'è un sovraccarico di base per le sealed colonne. Questo sovraccarico è costante e si aggiunge alla dimensione dei byte cleartext e al riempimento (se presente).

Prima di qualsiasi crittografia, ai dati nelle sealed colonne viene aggiunto un carattere da 1 byte che indica il tipo di dati contenuti. Se è selezionato il padding, i dati vengono quindi riempiti e aggiunti con 2 byte che indicano la dimensione del pad. Dopo l'aggiunta di questi byte, i dati vengono elaborati crittograficamente utilizzando AES-GCM e archiviati con IV (12 byte), (32 byte) e (16 byte). nonce Auth Tag Questi dati vengono quindi elaborati tramite un codificatore base64, aggiungendo circa il 33 percento alla dimensione dei byte. I dati sono preceduti da una designazione C3R a 7 byte per indicare il tipo di colonna a cui appartengono i dati e la versione client utilizzata per produrli. Il risultato è un sovraccarico finale di base di 91 byte. Questo risultato può quindi essere moltiplicato per il numero di righe per ottenere il sovraccarico di base totale (usa il numero di valori totali non nulli se `preserveNulls` impostato su true).

L'immagine seguente mostra come *`BASE_OVERHEAD = C3R_DESIGNATION + ((NONCE + IV + DATA_TYPE + PAD_SIZE + AUTH_TAG) * 1.33)`*



Impostazioni di collaborazione per le colonne sealed

`preserveNulls`Impostazione

Quando l'impostazione del livello di collaborazione `preserveNulls` è `false` (impostazione predefinita), ogni `null` valore è unico, casuale di 32 byte ed è elaborato come se non lo fosse. `null` Il risultato è che ogni `null` valore ora è di 91 byte (di più se inserito). Ciò può aggiungere requisiti di archiviazione significativi per le tabelle che contengono dati molto scarsi rispetto a quando questa impostazione è impostata `true` e `null` i valori vengono passati come. `null`

Se non hai bisogno delle garanzie sulla privacy di questa impostazione e preferisci mantenere `null` i valori all'interno dei tuoi set di dati, abilita l'`preserveNulls`impostazione al momento della creazione della collaborazione. L'`preserveNulls`impostazione non può essere modificata dopo la creazione della collaborazione.

sealedColonne delle impostazioni dello schema: tipi di riempimento

Argomenti

- Tipo di pad: none
- Tipo di pad di fixed
- Tipo di pad di max

Tipo di pad: **`none`**

La selezione di un tipo di pad `none` non aggiunge alcuna imbottitura cleartext e non aggiunge alcun sovraccarico aggiuntivo al sovraccarico di base descritto in precedenza. L'assenza di imbottitura garantisce la dimensione di output più efficiente in termini di spazio. Tuttavia, non offre le stesse garanzie di privacy dei tipi di imbottitura. `fixed` `max` Questo perché la dimensione del sottostante cleartext è distinguibile dalla dimensione del testo cifrato.

Tipo di pad di **`fixed`**

La selezione di un tipo di pad `fixed` è una misura di tutela della privacy per nascondere la lunghezza dei dati contenuti all'interno di una colonna. Questo viene fatto inserendo tutti i dati nel riquadro fornito prima che cleartext venga crittografato. `pad_length` Qualsiasi dato che superi tale dimensione causa il fallimento del client di crittografia C3R.

Dato che il padding viene aggiunto cleartext prima della crittografia, AES-GCM dispone di una mappatura 1 a 1 di due byte di testo cifrato. cleartext La codifica base64 aggiungerà il 33 percento.

Il sovraccarico di archiviazione aggiuntivo del padding può essere calcolato sottraendo la lunghezza media di cleartext dal valore di e moltiplicandola per 1,33. `pad_length` Il risultato è il sovraccarico medio del padding per record. Questo risultato può quindi essere moltiplicato per il numero di righe per ottenere il sovraccarico totale del padding (usa il numero di `null` valori diversi dal totale se `preserveNulls` è impostato su). `true`

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

Ti consigliamo di selezionare il valore minimo `pad_length` che racchiude il valore più grande in una colonna. Ad esempio, se il valore più grande è 50 byte, è sufficiente un valore `pad_length` di 50. Un valore superiore a tale valore aggiungerà solo un sovraccarico di archiviazione aggiuntivo.

Il padding fisso non aggiunge alcun sovraccarico di calcolo significativo.

Tipo di pad di **`max`**

La selezione di un tipo di pad `max` è una misura di tutela della privacy per nascondere la lunghezza dei dati contenuti all'interno di una colonna. Questa operazione viene eseguita inserendo tutti i dati cleartext fino al valore più grande della colonna e a quello aggiuntivo prima che venga crittografata. `pad_length` In genere, il `max` padding offre le stesse garanzie del `fixed` padding per un singolo set di dati, pur consentendo di non conoscere il valore più grande nella colonna. cleartext Tuttavia, il `max` padding potrebbe non fornire le stesse garanzie di privacy del `fixed` padding tra gli aggiornamenti perché il valore massimo nei singoli set di dati potrebbe essere diverso.

Ti consigliamo di selezionare un valore aggiuntivo `pad_length` di 0 quando usi il padding. `max` Questa lunghezza riempie tutti i valori in modo che abbiano le stesse dimensioni del valore più grande nella colonna. Un valore maggiore di quello aggiungerà solo un sovraccarico di archiviazione aggiuntivo.

Se è noto il cleartext valore massimo per una determinata colonna, ti consigliamo di utilizzare invece il tipo di `fixed` pad. L'uso del `fixed` padding crea coerenza tra i set di dati aggiornati. L'utilizzo del `max` padding fa sì che ogni sottoinsieme di dati venga aggiunto al valore più grande presente nel sottoinsieme.

Dati di esempio per una colonna sealed

Di seguito è riportato un set di esempio di dati di input e output per una sealed colonna con impostazioni da riprodurre. Altre impostazioni a livello di collaborazione, ad esempio `allowCleartext`allowJoinsOnColumnsWithDifferentNames, `allowDuplicates` non

influiscono sui risultati e possono essere impostate come `true` o `false` se si tenta di riprodurre localmente. Sebbene queste siano le impostazioni di base da riprodurre, la sealed colonna non è deterministica e i valori cambieranno ogni volta. L'obiettivo è mostrare i byte in ingresso rispetto ai byte in uscita. I `pad_length` valori di esempio sono stati scelti intenzionalmente. Mostrano che il `fixed` padding produce gli stessi valori del `max` padding con le `pad_length` impostazioni minime consigliate o quando si desidera un riempimento aggiuntivo.

Esempio di segreto condiviso: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Esempio di ID di collaborazione: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

Argomenti

- Tipo di pad: none
- Tipo di pad di fixed (esempio 1)
- Tipo di pad di fixed (esempio 2)
- Tipo di pad di max (esempio 1)
- Tipo di pad di max (esempio 2)

Tipo di pad: **none**

Esempio 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministico	`Yes`
Byte di input	0
Byte di uscita	0

Esempio 2

Input	`null`

preserveNulls	FALSE
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSPbNIJfG3iXmu6cbCUrizuV
Deterministico	No
Byte di input	0
Byte di uscita	91

Esempio 3

Input	empty string
preserveNulls	-
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSPEM6qR8DWC2PB2GMlX41YK
Deterministico	No
Byte di input	0
Byte di uscita	91

Esempio 4

Input	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0

	`h7t6OmWMLTWCvO2ckr6pkx9sGL5VLDQeHzh6DmPpyWNuI=`
Deterministico	No
Byte di input	26
Byte di uscita	127

Esempio 5

Input	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Deterministico	No
Byte di input	62
Byte di uscita	175

Tipo di pad di **`fixed`** (esempio 1)

In questo esempio, `pad_length` è 62 e l'input più grande è 62 byte.

Esempio 1

Input	`null`

preserveNulls	TRUE
Output	null
Deterministico	Yes
Byte di input	0
Byte di uscita	0

Esempio 2

Input	null
preserveNulls	FALSE
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=
Deterministico	No
Byte di input	0
Byte di uscita	175

Esempio 3

Input	empty string
preserveNulls	-
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7S

	`MX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=`
Deterministico	No
Byte di input	0
Byte di uscita	175

Esempio 4

Input	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=`
Deterministico	No
Byte di input	26
Byte di uscita	175

Esempio 5

Input	`abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`
`preserveNulls`	-

Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=`
Deterministico	No
Byte di input	62
Byte di uscita	175

Tipo di pad di **`fixed`** (esempio 2)

In questo esempio, `pad_length` è 162 e l'input più grande è 62 byte.

Esempio 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministico	`Yes`
Byte di input	0
Byte di uscita	0

Esempio 2

Input	`null`
`preserveNulls`	`FALSE`

Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcnkB0xbLWD7zNdAqQGR0rXoSESdW0I0vpNoGcBfv4cJbG0A3h1DvtkSSVc2B80OOGppzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn+8o4WtG/ClipNcjDXvXVtK4vfCohcCA6uwrmwv/xAySX+xcntotL703aBTBb`
Deterministico	No
Byte di input	0
Byte di uscita	307

Esempio 3

Input	`empty string`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcnkB0xbLWD7zNdAqQGR0rXoSESdW0I0vpNoGcBfv4cJbG0A3h1DvtkSSVc2B80OOGppzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn+8o4WtG/ClipNcjDXvXVtK4vfCohcCA6uwrmwv84lVaT9Yd+6oQx65/+gdVT`
Deterministico	No

Byte di input	0
Byte di uscita	307

Esempio 4

Input	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf`
Deterministico	No
Byte di input	26
Byte di uscita	307

Esempio 5

Input	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY`

	`Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/QOQ3cXb/pbvPcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i``
Deterministico	No
Byte di input	62
Byte di uscita	307

Tipo di pad di **`max`** (esempio 1)

In questo esempio, `pad_length` è 0 e l'input più grande è 62 byte.

Esempio 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministico	`Yes`
Byte di input	0
Byte di uscita	0

Esempio 2

Input	`null`
`preserveNulls`	`FALSE`

Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=`
Deterministico	No
Byte di input	0
Byte di uscita	175

Esempio 3

Input	`empty string`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=`
Deterministico	No
Byte di input	0
Byte di uscita	175

Esempio 4

Input	`abcdefghijklmnopqrstuvwxyz`

preserveNulls	-
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=
Deterministico	No
Byte di input	26
Byte di uscita	175

Esempio 5

Input	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
preserveNulls	-
Output	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=
Deterministico	No
Byte di input	62
Byte di uscita	175

Tipo di pad di **`max`** (esempio 2)

In questo esempio, `pad_length` è 100 e l'input più grande è 62 byte.

Esempio 1

Input	`null`
`preserveNulls`	`TRUE`
Output	`null`
Deterministico	`Yes`
Byte di input	0
Byte di uscita	0

Esempio 2

Input	`null`
`preserveNulls`	`FALSE`
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb`
Deterministico	No
Byte di input	0

Byte di uscita	307

Esempio 3

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

Esempio 4

Input	`abcdefghijklmnopqrstuvwxyz`
`preserveNulls`	-
Output	`01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE`

	`Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf`
Deterministico	No
Byte di input	26
Byte di uscita	307

Esempio 5

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

sealedcolonne di risoluzione dei problemi

Perché il testo cifrato nelle mie sealed colonne è parecchie volte più grande della dimensione del testo in cleartext esse contenuto?

Ciò dipende da diversi fattori. Innanzitutto, il testo cifrato in una Cleartext colonna ha sempre una lunghezza di almeno 91 byte. Se i dati di input erano piccoli (ad esempio, l'età dei clienti), mostreranno un aumento significativo delle dimensioni. In secondo luogo, se `preserveNulls` fossimo impostati su `false` e i dati di input contenessero molti `null` valori, ognuno di questi `null` valori sarebbe stato trasformato in 91 byte di testo cifrato. Infine, se si utilizza il padding, per definizione i byte vengono aggiunti ai cleartext dati prima che vengano crittografati.

La maggior parte dei miei dati in una sealed colonna è davvero piccola e ho bisogno di usare il padding. Posso semplicemente rimuovere i valori più grandi ed elaborarli separatamente per risparmiare spazio?

Non è consigliabile rimuovere valori di grandi dimensioni ed elaborarli separatamente. In questo modo vengono modificate le garanzie sulla privacy fornite dal client di crittografia C3R. Come modello di minaccia, supponiamo che un osservatore possa vedere entrambi i set di dati crittografati. Se l'osservatore rileva che un sottoinsieme di dati ha una colonna riempita in modo significativo in più o in meno rispetto a un altro sottoinsieme, può fare inferenze sulla dimensione dei dati in ciascun sottoinsieme. Ad esempio, supponiamo che una `fullName` colonna venga aggiunta a un totale di 40 byte in un file e venga aggiunta a 800 byte in un altro file. Un osservatore potrebbe supporre che un set di dati contenga il nome più lungo del mondo (747 byte).

Devo fornire un'imbottitura aggiuntiva quando utilizzo il tipo di imbottitura? **`max`**

No. Quando si utilizza il `max` padding, si consiglia di impostare il padding`pad_length`, noto anche come padding aggiuntivo oltre il valore più grande nella colonna, su 0.

Posso semplicemente scegliere un valore grande **`pad_length`** quando uso il **`fixed`** padding per evitare di preoccuparmi se il valore più grande si adatta?

Sì, ma l'ampia lunghezza del pad è inefficiente e utilizza più spazio di archiviazione del necessario. Ti consigliamo di controllare quanto è grande il valore più grande e di `pad_length` impostarlo su quel valore.

Come faccio a sapere se ho bisogno delle garanzie crittografiche fornite da? **`preserveNulls`**

Sfortunatamente, la risposta è che dipende. Come minimo, è Elaborazione crittografica per Clean Rooms necessario verificare in che modo l'`preserveNulls`impostazione protegge i dati. Tuttavia, ti

consigliamo di fare riferimento ai requisiti di gestione dei dati della tua organizzazione e agli eventuali contratti applicabili alla rispettiva collaborazione.

Perché devo sostenere il sovraccarico di base64?

Per consentire la compatibilità con i formati di file tabulari come CSV, è necessaria la codifica base64. Sebbene alcuni formati di file come quelli Parquet supportino le rappresentazioni binarie dei dati, è importante che tutti i partecipanti a una collaborazione rappresentino i dati nello stesso modo per garantire risultati di interrogazione corretti.

Risoluzione dei problemi relativi agli aumenti imprevisti delle dimensioni del testo cifrato

Supponiamo che tu abbia crittografato i tuoi dati e che la dimensione dei dati risultanti sia sorprendentemente grande. I passaggi seguenti possono aiutarti a identificare dove si è verificato l'aumento delle dimensioni e quali azioni, se del caso, puoi intraprendere.

Identificare dove si è verificato l'aumento delle dimensioni

Prima di poter risolvere il motivo per cui i dati crittografati sono significativamente più grandi cleartext dei dati, è necessario innanzitutto identificare dove si trova l'aumento delle dimensioni. Cleartextle colonne possono essere tranquillamente ignorate perché rimangono invariate. Guarda le sealed colonne rimanenti fingerprint e scegline una che appaia significativa.

Identificare il motivo per cui si è verificato l'aumento delle dimensioni

Una fingerprint colonna o una sealed colonna potrebbero contribuire all'aumento delle dimensioni.

Argomenti

- L'aumento delle dimensioni proviene da una fingerprint colonna?
- L'aumento delle dimensioni proviene da una sealed colonna?

L'aumento delle dimensioni proviene da una fingerprint colonna?

Se la colonna che contribuisce maggiormente all'aumento dello spazio di archiviazione è una fingerprint colonna, è probabile che i cleartext dati siano piccoli (ad esempio, l'età del cliente). Ogni fingerprint testo cifrato risultante ha una lunghezza di 52 byte. Sfortunatamente, non si può fare nulla per risolvere questo problema su una base. column-by-column Per ulteriori informazioni, consulta

Sovraccarico di base per le colonne fingerprint i dettagli su questa colonna, incluso il modo in cui influisce sui requisiti di archiviazione.

L'altra possibile causa dell'aumento delle dimensioni di una fingerprint colonna è l'impostazione di collaborazione,`preserveNulls`. Se l'impostazione di collaborazione per `preserveNulls` è disabilitata (impostazione predefinita), tutti i `null` valori nelle fingerprint colonne saranno diventati 52 byte di testo cifrato. Non c'è nulla che si possa fare per questo nell'attuale collaborazione. L'`preserveNulls`impostazione viene impostata al momento della creazione di una collaborazione e tutti i collaboratori devono utilizzare la stessa impostazione per garantire risultati di interrogazione corretti. Per ulteriori informazioni sull'`preserveNulls`impostazione e su come la sua attivazione influisce sulle garanzie di privacy dei dati, consulta. Calcolo crittografico

L'aumento delle dimensioni proviene da una sealed colonna?

Se la colonna che contribuisce maggiormente all'aumento dello spazio di archiviazione è una sealed colonna, ci sono alcuni dettagli che potrebbero contribuire all'aumento delle dimensioni.

Se i cleartext dati sono piccoli (ad esempio, l'età del cliente), ogni sealed testo cifrato risultante ha una lunghezza di almeno 91 byte. Purtroppo non si può fare nulla per risolvere questo problema. Per ulteriori informazioni, consulta Sovraccarico di base per le colonne sealed i dettagli su questa colonna, incluso il modo in cui influisce sui requisiti di archiviazione.

La seconda causa principale dell'aumento dello spazio di archiviazione nelle sealed colonne è il padding. Il padding aggiunge byte aggiuntivi cleartext prima che venga crittografato per nascondere le dimensioni dei singoli valori in un set di dati. Ti consigliamo di impostare il padding sul valore minimo possibile per il tuo set di dati. Come minimo, `pad_length` il `fixed` padding deve essere impostato in modo da includere il valore più grande possibile nella colonna. Qualsiasi impostazione superiore a quella non aggiunge ulteriori garanzie di privacy. Ad esempio, se sai che il valore più grande possibile in una colonna può essere di 50 byte, ti consigliamo di `pad_length` impostarlo su 50 byte. Tuttavia, se la sealed colonna utilizza il `max` padding, ti consigliamo di `pad_length` impostarlo su 0 byte. Questo perché il `max` padding si riferisce al padding aggiuntivo oltre il valore più grande nella colonna.

L'ultima possibile causa dell'aumento delle dimensioni di una sealed colonna è l'impostazione di collaborazione,. `preserveNulls` Se l'impostazione di collaborazione per `preserveNulls` è disabilitata (impostazione predefinita), tutti i `null` valori nelle sealed colonne saranno diventati 91 byte di testo cifrato. Non c'è nulla che si possa fare per questo nell'attuale collaborazione. L'`preserveNulls`impostazione viene impostata al momento della creazione di una collaborazione e tutti i collaboratori devono utilizzare la stessa impostazione per garantire risultati di interrogazione

corretti. Per ulteriori informazioni sulle funzionalità di questa impostazione e su come la sua attivazione influisce sulle garanzie di privacy dei dati, consulta. Calcolo crittografico

Registrazione delle query AWS Clean Rooms

La registrazione delle query è una funzionalità di. AWS Clean Rooms Quando crei una collaborazione e attivi la registrazione delle query, i membri possono archiviare i log delle query pertinenti in Amazon CloudWatch Logs.

Con i log delle query, i membri possono determinare se le query sono conformi alle regole di analisi e sono in linea con l'accordo di collaborazione. Inoltre, i log delle interrogazioni aiutano a supportare gli audit.

Quando l'opzione di registrazione delle query è attivata nella AWS Clean Rooms console, i log delle query includono quanto segue:

- `analysisRule`— La regola di analisi per la tabella configurata.
- `analysisTemplateArn`— Il modello di analisi che è stato eseguito (viene visualizzato in base alla regola di analisi).
- `collaborationId`— L'identificatore univoco per la collaborazione in cui è stata eseguita la query.
- `configuredTableID`— L'identificatore univoco per la tabella configurata a cui si fa riferimento nella query.
- `directQueryAnalysisRulePolicy.custom.allowedAnalysis`— Il modello di analisi consentito per l'esecuzione sulla tabella configurata (viene visualizzato in base alla regola di analisi).
- `directQueryAnalysisRulePolicy.v1.custom.allowedAnalysisProviders`— I provider di query autorizzati a creare query (viene visualizzato in base alla regola di analisi).
- `eventID`— L'identificatore univoco per l'esecuzione della query. Dopo il 31 agosto 2023, l'identificatore univoco è lo stesso del. `protectedQueryID`
- `eventTimestamp`— Il tempo di esecuzione della query.
- `parameters.parametervalue`— I valori dei parametri (visualizzati in base al testo dell'interrogazione).
- `queryText`— La definizione SQL dell'esecuzione della query. Se sono presenti parametri, vengono etichettati come`:parametervalue`.
- `queryValidationErrors`— Gli errori di interrogazione durante la convalida dell'interrogazione.
- `schemaName`— Il nome dell'associazione di tabelle configurata a cui si fa riferimento nella query.

Ricezione dei registri delle interrogazioni

Non è necessario eseguire alcuna azione al di fuori di AWS Clean Rooms per configurare i registri delle query. AWS Clean Rooms crea gruppi di log per le collaborazioni dopo che ogni membro della collaborazione ha creato un'iscrizione.

I membri che possono eseguire query, i membri che possono ricevere risultati e i membri le cui tabelle di configurazione sono referenziate nella query riceveranno un registro delle query.

Il membro che può eseguire query e il membro che può ricevere risultati riceveranno i log delle query per ogni tabella configurata a cui viene fatto riferimento nella query. Se non possiedono la tabella configurata, non saranno in grado di visualizzare l'ID della tabella configurata ()`configuredTableID`.

Se un membro ha più associazioni di tabelle configurate a cui fa riferimento la query, riceverà un registro delle query per ogni tabella configurata.

I log vengono creati per le query che contengono istruzioni SQL non supportate e supportate in. AWS Clean RoomsPer ulteriori dettagli, vedere SQL Reference.AWS Clean Rooms

I log vengono creati anche quando le query fanno riferimento a tabelle configurate che non sono associate alla collaborazione.

I log non vengono creati per un accesso SQL errato. AWS Clean Rooms

I log delle query non indicano che una query ha avuto esito positivo e che l'output della query è stato fornito. Confermano che una richiesta è stata inviata dal membro che può eseguire la query. I registri delle query confermano inoltre che la query contiene SQL supportato AWS Clean Rooms e fa riferimento alle tabelle configurate associate alla collaborazione.

Example

Ad esempio, non viene prodotto un log se la query è stata annullata dopo averne AWS Clean Rooms convalidata la conformità alle regole di analisi e durante l'elaborazione della query.

Se si elimina il gruppo di log, è necessario ricrearlo manualmente con lo stesso nome del gruppo di log (ID di collaborazione della collaborazione). In alternativa, puoi disattivare e riattivare la registrazione nella tua iscrizione.

Per ulteriori informazioni su come attivare la registrazione delle query, consulta. Creazione di una collaborazione in AWS Clean Rooms

Per ulteriori informazioni su Amazon CloudWatch Logs, consulta la Amazon CloudWatch Logs User Guide.

Utilizzo dei log di interrogazione

Consigliamo ai membri di intraprendere periodicamente le seguenti azioni:

- Per verificare che le query corrispondano ai casi d'uso o alle query concordate per la collaborazione, esamina le query eseguite nella collaborazione.

  Per ulteriori informazioni su come visualizzare le interrogazioni recenti, vedere Visualizzazione delle interrogazioni recenti.
- Per verificare che le colonne della tabella configurate corrispondano a quanto concordato per la collaborazione, esamina le colonne della tabella configurate utilizzate nelle regole di analisi dei membri della collaborazione e nelle query.

  Per ulteriori informazioni su come visualizzare le colonne configurate, vedere Visualizzazione delle tabelle e delle regole di analisi.

Configurazione AWS Clean Rooms

I seguenti argomenti spiegano come eseguire la configurazione AWS Clean Rooms.

Argomenti

Registrati per AWS

Prima di poterne utilizzare qualsiasi Servizio AWS AWS Clean Rooms, incluso, devi registrarti a AWS.

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.
3. Quando ti iscrivi a Account AWS, viene creato un utente Account AWS root. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

Imposta i ruoli di servizio per AWS Clean Rooms

Argomenti

- Crea un ruolo di servizio per ricevere risultati

Crea un utente amministratore

Per utilizzarlo AWS Clean Rooms, è necessario creare un utente amministratore e aggiungere l'utente amministratore a un gruppo di amministratori.

Per creare un utente amministratore, scegli una delle seguenti opzioni.

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
In IAM Identity Center (Consigliato)	Usa credenziali a breve termine per accedere a AWS. Ciò è in linea con le best practice per la sicurezza. Per informazioni sulle best practice, consulta Best practice per la sicurezza in IAM nella Guida per l'utente di IAM.	Segui le istruzioni riportate in Nozioni di base nella Guida per l'utente di AWS IAM Identity Center .	Configura l'accesso programmatico configurando l'uso AWS IAM Identity Center nella AWS CLI Guida per l'utente.AWS Command Line Interface
In IAM (Non consigliato)	Usa credenziali a lungo termine per accedere a AWS.	Segui le istruzioni in Creazione del primo utente e gruppo di utenti IAM di amministrazione nella Guida per l'utente di IAM.	Configura l'accesso programmatico seguendo quanto riportato in Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM.

Crea un ruolo IAM per un membro della collaborazione

Un membro è un AWS cliente che partecipa a una collaborazione.

Creare un ruolo IAM per un membro della collaborazione

1. Segui la procedura Creazione di un ruolo per delegare le autorizzazioni a una procedura utente IAM nella Guida per l'AWS Identity and Access Management utente.
2. Per la fase di creazione della policy, seleziona la scheda JSON nell'editor delle politiche, quindi aggiungi le politiche in base alle capacità concesse al membro della collaborazione.

   AWS Clean Rooms offre le seguenti politiche gestite basate su casi d'uso comuni:

Se vuoi ...	Quindi usa...
Visualizza le risorse e i metadati	AWS politica gestita: `AWSCleanRoomsReadOnlyAccess`
Query	AWS politica gestita: `AWSCleanRoomsFullAccess`
Interroga e ricevi risultati	AWS politica gestita: `AWSCleanRoomsFullAccess`
Gestisci le risorse di collaborazione ma non interrogare	AWS politica gestita: `AWSCleanRoomsFullAccessNoQuerying`

   Per informazioni sulle diverse politiche gestite offerte da AWS Clean Rooms, vedere AWS politiche gestite per AWS Clean Rooms

Creare un ruolo di servizio per leggere i dati

AWS Clean Rooms utilizza un ruolo di servizio per leggere i dati.

Esistono due modi per creare questo ruolo di servizio:

Se...	Allora
Disponi delle autorizzazioni IAM necessarie per creare un ruolo di servizio	Usa la AWS Clean Rooms console per creare un ruolo di servizio.
Non disponi di `iam:CreateRole` `iam:AttachRolePolicy` autorizzazioni `iam:CreatePolicy` e oppure Vuoi creare i ruoli IAM manualmente	Esegui una di queste operazioni: • Utilizza la seguente procedura per creare un ruolo di servizio. • Chiedere all'amministratore di creare il ruolo di servizio utilizzando la procedura seguente.

Per creare un ruolo di servizio per leggere i dati

> **Note**
>
> Tu o il tuo amministratore IAM dovreste seguire questa procedura solo se non disponete delle autorizzazioni necessarie per creare un ruolo di servizio utilizzando la AWS Clean Rooms console.

1. Segui la procedura Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console) nella Guida per l'AWS Identity and Access Management utente.
2. Utilizza la seguente politica di fiducia personalizzata in base alla procedura Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console).

   > **Note**
   >
   > Se desideri assicurarti che il ruolo possa essere utilizzato solo nel contesto di una determinata appartenenza alla collaborazione, puoi definire ulteriormente la politica di fiducia. Per ulteriori informazioni, consulta Prevenzione del problema "confused deputy" tra servizi.

   ```
   {
   ```

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

3. Utilizza la seguente politica di autorizzazioni in base alla procedura Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console).

> **Note**
>
> La seguente policy di esempio supporta le autorizzazioni necessarie per leggere AWS Glue i metadati e i dati Amazon S3 corrispondenti. Tuttavia, potrebbe essere necessario modificare questa politica a seconda di come hai configurato i dati S3. Ad esempio, se hai impostato una chiave KMS personalizzata per i tuoi dati S3, potresti dover modificare questa politica con autorizzazioni aggiuntive. AWS KMS
> AWS Glue Le tue risorse e le risorse Amazon S3 sottostanti devono essere le Regione AWS stesse della AWS Clean Rooms collaborazione.

```
{
    "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. Sostituisci ogni *segnaposto* con le tue informazioni.
5. Continua a seguire la procedura Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console) per creare il ruolo.

Crea un ruolo di servizio per ricevere risultati

> **Note**
>
> Se sei il membro che può solo ricevere risultati (nella console, le tue abilità da membro sono solo Ricevi risultati), segui questa procedura.
> Se sei un membro che può sia interrogare che ricevere risultati (nella console, le tue abilità di membro sono sia Query che Ricevi risultati), puoi saltare questa procedura.

Per i membri della collaborazione che possono solo ricevere risultati, AWS Clean Rooms utilizza un ruolo di servizio per scrivere i risultati dei dati interrogati nella collaborazione nel bucket Amazon S3 specificato.

Esistono due modi per creare questo ruolo di servizio:

Se...	Allora
Disponi delle autorizzazioni IAM necessarie per creare un ruolo di servizio	Usa la AWS Clean Rooms console per creare un ruolo di servizio.

Se...	Allora
Non disponi di `iam:CreateRole` `iam:AttachRolePolicy` autorizzazioni `iam:CreatePolicy` e oppure Vuoi creare i ruoli IAM manualmente	Esegui una di queste operazioni: • Utilizza la seguente procedura per creare un ruolo di servizio. • Chiedere all'amministratore di creare il ruolo di servizio utilizzando la procedura seguente.

Creare un ruolo di servizio per ricevere risultati

> **Note**
>
> Tu o il tuo amministratore IAM dovreste seguire questa procedura solo se non disponete delle autorizzazioni necessarie per creare un ruolo di servizio utilizzando la AWS Clean Rooms console.

1. Segui la procedura Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console) nella Guida per l'AWS Identity and Access Management utente.
2. Utilizza la seguente politica di fiducia personalizzata in base alla procedura Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowIfExternalIdMatches",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "sts:ExternalId":
 "arn:aws:*:region:*:dbuser:*/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa*"
                }
```

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

                }
            }
        }
    ]
}
```

3. Utilizza la seguente politica di autorizzazioni in base alla procedura Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console).

> **Note**
>
> La seguente policy di esempio supporta le autorizzazioni necessarie per leggere AWS Glue i metadati e i dati Amazon S3 corrispondenti. Tuttavia, potrebbe essere necessario modificare questa politica a seconda di come hai configurato i dati S3.
> AWS Glue Le tue risorse e le risorse Amazon S3 sottostanti devono essere le Regione AWS stesse della AWS Clean Rooms collaborazione.

```
{
    "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. Sostituisci ogni *segnaposto* con le tue informazioni:

   - *regione*: il nome di. Regione AWS Ad esempio, **us-east-1**.
   - *A1B2C3D4-5678-90AB-CDEF-ExampleAAAAA*: l'ID di iscrizione del membro che può effettuare la richiesta. L'ID di iscrizione è disponibile nella scheda Dettagli della collaborazione. Ciò garantisce che AWS Clean Rooms assuma il ruolo solo quando questo membro esegue l'analisi nell'ambito di questa collaborazione.
   - *arn:aws:cleanrooms:us-east- 1:5555:membership/a1b2c3d4-5678-90ab-cdef-exampleAAAAA — L'ARN di appartenenza singolo del membro* che può eseguire la query. L'ARN di iscrizione è disponibile nella scheda Dettagli della collaborazione. Ciò garantisce AWS Clean Rooms che assuma il ruolo solo quando questo membro esegue l'analisi nell'ambito di questa collaborazione.
   - *bucket_name* — L'Amazon Resource Name (ARN) del bucket S3. L'Amazon Resource Name (ARN) è disponibile nella scheda Proprietà del bucket in Amazon S3.

- *AccountID*: l' Account AWS ID in cui si trova il bucket S3.

  bucket_name/optional_key_prefix — L'Amazon Resource Name (ARN) della destinazione dei risultati in S3. L'Amazon Resource Name (ARN) è disponibile nella scheda Proprietà del bucket in Amazon S3.

5. Continua a seguire la procedura Creazione di un ruolo utilizzando politiche di fiducia personalizzate (console) per creare il ruolo.

Configura i ruoli di servizio per il machine AWS Clean Rooms learning

Argomenti

- Crea un ruolo di servizio per leggere i dati di formazione
- Crea un ruolo di servizio per scrivere un segmento simile
- Crea un ruolo di servizio per leggere i dati iniziali

Crea un ruolo di servizio per leggere i dati di formazione

AWS Clean Rooms utilizza un ruolo di servizio per leggere i dati di addestramento. Puoi creare questo ruolo utilizzando la console se disponi delle autorizzazioni IAM necessarie. Se non disponi `CreateRole` delle autorizzazioni, chiedi all'amministratore di creare il ruolo di servizio.

Per creare un ruolo di servizio per addestrare un set di dati

1. Accedi alla console IAM (https://console.aws.amazon.com/iam/) con il tuo account amministratore.
2. In Gestione accessi scegli Policy.
3. Seleziona Create Policy (Crea policy).
4. Nell'editor delle politiche, seleziona la scheda JSON, quindi copia e incolla la seguente policy.

> **Note**
>
> La seguente policy di esempio supporta le autorizzazioni necessarie per leggere AWS Glue i metadati e i dati Amazon S3 corrispondenti. Tuttavia, potrebbe essere necessario

modificare questa politica a seconda di come hai configurato i dati S3. Questa politica non include una chiave KMS per decrittografare i dati.
AWS Glue Le tue risorse e le risorse Amazon S3 sottostanti devono essere le Regione AWS stesse della AWS Clean Rooms collaborazione.

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

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

Se devi usare una chiave KMS per decrittografare i dati, aggiungi questa AWS KMS dichiarazione al modello precedente:

```
{
            "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. Seleziona Successivo.
6. Per Revisione e creazione, inserisci il nome e la descrizione della politica e consulta il riepilogo.
7. Scegli Crea policy.

   Hai creato una politica per AWS Clean Rooms.
8. In Access management (Gestione accessi), scegli Roles (Ruoli).

   Con Roles, puoi creare credenziali a breve termine, operazione consigliata per una maggiore sicurezza. Puoi anche scegliere Utenti per creare credenziali a lungo termine.
9. Scegli Crea ruolo.
10. Nella procedura guidata di creazione del ruolo, per il tipo di entità attendibile, scegli Criteri di attendibilità personalizzati.
11. Copia e incolla la seguente politica di fiducia personalizzata nell'editor JSON.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms-ml.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEqualsIfExists": {
                    "aws:SourceAccount": ["accountId"]
                },
                "StringLikeIfExists": {
                    "aws:SourceArn": "arn:aws:cleanrooms-
ml:region:account:training-dataset/*"
```

```
                }
            }
        }
    ]
}
```

`SourceAccount`È sempre il tuo AWS account. `SourceArn`Può essere limitato a un set di dati di addestramento specifico, ma solo dopo la creazione di tale set di dati. Poiché non è possibile conoscere in anticipo l'ARN del set di dati di addestramento, qui viene specificata la jolly.

12. Scegli Avanti e in Aggiungi autorizzazioni, inserisci il nome della politica che hai appena creato. (Potrebbe essere necessario ricaricare la pagina.)
13. Seleziona la casella di controllo accanto al nome della politica che hai creato, quindi scegli Avanti.
14. Per Nome, revisione e creazione, inserisci il nome e la descrizione del ruolo.

> **Note**
>
> Il nome del ruolo deve corrispondere allo schema delle `passRole` autorizzazioni concesse al membro che può interrogare e ricevere risultati e ruoli dei membri.

    a. Rivedi Seleziona entità attendibili e, se necessario, apporta le modifiche.
    b. Controlla le autorizzazioni in Aggiungi autorizzazioni e modificale se necessario.
    c. Controlla i tag e aggiungi i tag se necessario.
    d. Scegli Crea ruolo.
15. Il ruolo di servizio per AWS Clean Rooms è stato creato.

Crea un ruolo di servizio per scrivere un segmento simile

AWS Clean Rooms utilizza un ruolo di servizio per scrivere segmenti simili in un bucket. Puoi creare questo ruolo utilizzando la console se disponi delle autorizzazioni IAM necessarie. Se non disponi `CreateRole` delle autorizzazioni, chiedi all'amministratore di creare il ruolo di servizio.

Per creare un ruolo di servizio, scrivere un segmento simile

1. Accedi alla console IAM (https://console.aws.amazon.com/iam/) con il tuo account amministratore.

2. In Gestione accessi scegli Policy.
3. Seleziona Create Policy (Crea policy).
4. Nell'editor delle politiche, seleziona la scheda JSON, quindi copia e incolla la seguente policy.

> **Note**
>
> La seguente policy di esempio supporta le autorizzazioni necessarie per leggere AWS Glue i metadati e i dati Amazon S3 corrispondenti. Tuttavia, potrebbe essere necessario modificare questa politica a seconda di come hai configurato i dati S3. Questa politica non include una chiave KMS per decrittografare i dati.
> AWS Glue Le tue risorse e le risorse Amazon S3 sottostanti devono essere le Regione AWS stesse della AWS Clean Rooms collaborazione.

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

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

Se devi utilizzare una chiave KMS per crittografare i dati, aggiungi questa AWS KMS dichiarazione al modello:

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

Se devi usare una chiave KMS per decrittografare i dati, aggiungi questa AWS KMS dichiarazione al modello:

```
{
            "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. Seleziona Successivo.
6. Per Revisione e creazione, inserisci il nome e la descrizione della politica e consulta il riepilogo.
7. Scegli Crea policy.

   Hai creato una politica per AWS Clean Rooms.
8. In Access management (Gestione accessi), scegli Roles (Ruoli).

   Con Roles, puoi creare credenziali a breve termine, operazione consigliata per una maggiore sicurezza. Puoi anche scegliere Utenti per creare credenziali a lungo termine.
9. Scegli Crea ruolo.
10. Nella procedura guidata di creazione del ruolo, per il tipo di entità attendibile, scegli Criteri di attendibilità personalizzati.
11. Copia e incolla la seguente politica di fiducia personalizzata nell'editor JSON.

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

```
                "StringEqualsIfExists": {
                    "aws:SourceAccount": ["accountId"]

                },
                "StringLikeIfExists": {
                    "aws:SourceArn": "arn:aws:cleanrooms-
ml:region:account:configured-audience-model/*"
                }
            }
        }
    ]
}
```

`SourceAccount`È sempre il tuo AWS account. `SourceArn`Può essere limitato a un set di dati di addestramento specifico, ma solo dopo la creazione di tale set di dati. Poiché non è possibile conoscere in anticipo l'ARN del set di dati di addestramento, qui viene specificata la jolly.

12. Seleziona Successivo.
13. Seleziona la casella di controllo accanto al nome della policy che hai creato, quindi scegli Avanti.
14. Per Nome, revisione e creazione, inserisci il nome e la descrizione del ruolo.

> **Note**
>
> Il nome del ruolo deve corrispondere allo schema delle `passRole` autorizzazioni concesse al membro che può interrogare e ricevere risultati e ruoli dei membri.

    a. Rivedi Seleziona entità attendibili e, se necessario, apporta le modifiche.
    b. Controlla le autorizzazioni in Aggiungi autorizzazioni e modificale se necessario.
    c. Controlla i tag e aggiungi i tag se necessario.
    d. Scegli Crea ruolo.
15. Il ruolo di servizio per AWS Clean Rooms è stato creato.

Crea un ruolo di servizio per leggere i dati iniziali

AWS Clean Rooms utilizza un ruolo di servizio per leggere i dati iniziali. Puoi creare questo ruolo utilizzando la console se disponi delle autorizzazioni IAM necessarie. Se non disponi `CreateRole` delle autorizzazioni, chiedi all'amministratore di creare il ruolo di servizio.

Per creare un ruolo di servizio per leggere i dati iniziali

1. Accedi alla console IAM (https://console.aws.amazon.com/iam/) con il tuo account amministratore.
2. In Gestione accessi scegli Policy.
3. Seleziona Create Policy (Crea policy).
4. Nell'editor delle politiche, seleziona la scheda JSON, quindi copia e incolla la seguente policy.

> **Note**
>
> La seguente policy di esempio supporta le autorizzazioni necessarie per leggere AWS Glue i metadati e i dati Amazon S3 corrispondenti. Tuttavia, potrebbe essere necessario modificare questa politica a seconda di come hai configurato i dati S3. Questa politica non include una chiave KMS per decrittografare i dati.
> AWS Glue Le tue risorse e le risorse Amazon S3 sottostanti devono essere le Regione AWS stesse della AWS Clean Rooms collaborazione.

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

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

Se devi utilizzare una chiave KMS per decrittografare i dati, aggiungi questa AWS KMS dichiarazione al modello:

```
{
            "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. Seleziona Successivo.
6. Per Revisione e creazione, inserisci il nome e la descrizione della politica e consulta il riepilogo.
7. Scegli Crea policy.

Hai creato una politica per AWS Clean Rooms.

8. In Access management (Gestione accessi), scegli Roles (Ruoli).

   Con Roles, puoi creare credenziali a breve termine, operazione consigliata per una maggiore sicurezza. Puoi anche scegliere Utenti per creare credenziali a lungo termine.

9. Scegli Crea ruolo.
10. Nella procedura guidata di creazione del ruolo, per il tipo di entità attendibile, scegli Criteri di attendibilità personalizzati.
11. Copia e incolla la seguente politica di fiducia personalizzata nell'editor JSON.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": "cleanrooms-ml.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEqualsIfExists": {
                    "aws:SourceAccount": ["accountId"]

                },
                "StringLikeIfExists": {
                    "aws:SourceArn": "arn:aws:cleanrooms-
ml:region:account:audience-generation-job/*"
                }
            }
        }
    ]
}
```

   `SourceAccount`È sempre il tuo AWS account. `SourceArn`Può essere limitato a un set di dati di addestramento specifico, ma solo dopo la creazione di tale set di dati. Poiché non è possibile conoscere in anticipo l'ARN del set di dati di addestramento, qui viene specificata la jolly.

12. Seleziona Successivo.
13. Seleziona la casella di controllo accanto al nome della policy che hai creato, quindi scegli Avanti.

14. Per Nome, revisione e creazione, inserisci il nome e la descrizione del ruolo.

> **Note**
>
> Il nome del ruolo deve corrispondere allo schema delle `passRole` autorizzazioni concesse al membro che può interrogare e ricevere risultati e ruoli dei membri.

    a. Rivedi Seleziona entità attendibili e, se necessario, apporta le modifiche.
    b. Controlla le autorizzazioni in Aggiungi autorizzazioni e modificale se necessario.
    c. Controlla i tag e aggiungi i tag se necessario.
    d. Scegli Crea ruolo.

15. Il ruolo di servizio per AWS Clean Rooms è stato creato.

Creazione di una collaborazione in AWS Clean Rooms

Una collaborazione è un limite logico sicuro AWS Clean Rooms in cui i membri possono eseguire query SQL su tabelle configurate.

Qualsiasi membro AWS Clean Rooms può creare una collaborazione.

Il creatore della collaborazione può designare un singolo membro per interrogare e ricevere risultati. Tuttavia, l'autore della collaborazione potrebbe voler impedire al membro che può eseguire la query di accedere ai risultati della query. In tal caso, l'autore della collaborazione può designare un membro che può eseguire le interrogazioni e un altro membro che può ricevere i risultati.

Nella maggior parte dei casi, il membro che può eseguire le query è anche il membro che paga i costi di elaborazione delle query. Tuttavia, il creatore della collaborazione può configurare un altro membro affinché sia responsabile del pagamento dei costi di elaborazione delle query.

Per informazioni su come creare una collaborazione utilizzando gli AWS SDK, consulta l'AWS Clean RoomsAPI Reference.

Argomenti

Crea una collaborazione

Prima di iniziare, assicurati di aver completato i seguenti prerequisiti:

- Hai il nome e l'Account AWSID di ogni membro che desideri invitare alla collaborazione.
- Hai il permesso di condividere il nome e l'Account AWSID di ogni membro con tutti i membri della collaborazione.

> **Note**
>
> Non puoi aggiungere altri membri dopo la creazione della collaborazione.

Per creare una collaborazione utilizzando la AWS Clean Rooms console

1. Accedi AWS Management Console e apri la AWS Clean Roomsconsole con il programma Account AWS che fungerà da creatore della collaborazione.
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Nell'angolo in alto a destra, scegli Crea collaborazione.
4. Per la Fase 1: Definizione della collaborazione, procedi come segue:

   a. Per i dettagli, inserisci il nome e la descrizione della collaborazione.

      Queste informazioni saranno visibili ai membri della collaborazione che sono invitati a partecipare alla collaborazione. Il nome e la descrizione li aiutano a capire a cosa si riferisce la collaborazione.

   b. Per i membri:

      i. Per Membro 1: Inserisci il nome visualizzato del Membro come desideri che appaia per la collaborazione.

      > **Note**
      >
      > Il tuo Account AWS ID viene incluso automaticamente come Account AWSID membro.

      ii. Per Membro 2, inserisci il nome visualizzato del membro e l'Account AWSID membro per il membro che desideri invitare alla collaborazione.

      Il nome visualizzato del membro e l'Account AWSID membro saranno visibili a tutti gli invitati alla collaborazione. Dopo aver inserito e salvato i valori per questi campi, questi non sono modificabili.

      > **Note**
      >
      > È necessario informare il membro della collaborazione che l'Account AWSID membro e il nome visualizzato del membro saranno visibili a tutti i collaboratori invitati e attivi nella collaborazione.

iii. Se desideri aggiungere un altro membro, scegli Aggiungi un altro membro. Quindi inserisci il nome visualizzato del membro e l'Account AWSID membro per ogni membro che può contribuire con i dati che desideri invitare alla collaborazione.

c. Per quanto riguarda le abilità dei soci, scegli una delle seguenti opzioni,

Se vuoi ...	Quindi...
Interroga i dati della collaborazione e ricevi i risultati	1. Scegli te stesso come membro che può eseguire le interrogazioni. 2. Lascia che l'impostazione predefinita del membro che può ricevere risultati sia Uguale a chi esegue le interrogazioni.
Interroga i dati della collaborazione e assegna un altro membro per ricevere i risultati	1. Scegli te stesso come membro che può eseguire le interrogazioni. 2. Seleziona il membro che può ricevere risultati dall'elenco a discesa.
Ricevi i risultati della query nella collaborazione e assegna un altro membro per interrogare i dati	1. Seleziona il membro che può eseguire interrogazioni dall'elenco a discesa. 2. Scegli te stesso come membro che può ricevere risultati dall'elenco a discesa.
Crea e gestisci la collaborazione, assegna un altro membro per interrogare i dati e assegna un altro membro per ricevere i risultati	1. Seleziona il membro che può eseguire interrogazioni dall'elenco a discesa. 2. Seleziona il membro che può ricevere risultati dall'elenco a discesa.

d. Per la configurazione del pagamento, scegli una delle seguenti opzioni:

Se vuoi ...	Quindi...
Assegna al membro che può eseguire le interrogazioni il ruolo di membro che paga i costi di calcolo delle query	Lascia che l'impostazione predefinita del membro che pagherà per le query sia la stessa di chi esegue le query.
Assegna a un membro diverso il pagamento dei costi di elaborazi one delle query	Seleziona il membro che pagherà per le domande dall'elenco a discesa.

e. Se si desidera abilitare la registrazione delle query, selezionare la casella di controllo Supporta la registrazione delle query per questa collaborazione.

f. Se desideri abilitare la funzionalità di calcolo crittografico, seleziona la casella di controllo Supporta il calcolo crittografico in questa collaborazione e scegli i seguenti parametri di calcolo crittografico:

- Consenti colonne cleartext

  Scegli No se non desideri che cleartext le colonne siano consentite nella tabella crittografata.

  Scegli Sì se desideri che cleartext le colonne siano consentite nella tabella crittografata.

  Per essere eseguite SUM o AVG su determinate colonne, le colonne devono essere inseritecleartext.

- Consenti duplicati

  Scegli No se non desideri che le voci duplicate siano consentite in una fingerprint colonna.

  Scegli Sì se desideri che le voci duplicate siano consentite in una fingerprint colonna.

- Consenti JOIN colonne con nomi diversi

  Scegli No se non desideri unire fingerprint colonne con nomi diversi.

  Scegli Sì se desideri unire fingerprint colonne con nomi diversi.

- Conserva NULL i valori

Scegliete No se non desiderate conservare NULL i valori. NULLi valori non verranno visualizzati come NULL in una tabella crittografata.

Scegli Sì se desideri conservare NULL i valori. NULLi valori verranno visualizzati come NULL in una tabella crittografata.

Per ulteriori informazioni sui parametri di calcolo crittografico, vedereParametri di calcolo crittografico.

Per ulteriori informazioni su come crittografare i dati per utilizzarli inAWS Clean Rooms, vedere. Preparazione di tabelle di dati crittografate con Cryptographic Computing per Clean Rooms

> **Note**
>
> Verifica attentamente queste configurazioni prima di completare il passaggio successivo. Dopo aver creato la collaborazione, puoi solo modificare il nome, la descrizione e se i log delle query sono archiviati in Amazon CloudWatch Logs.

g. Se desideri abilitare i tag per la risorsa di collaborazione, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.

h. Seleziona Avanti.

5. Per la Fase 2: Configurazione dell'iscrizione, procedi come segue:

   a. Scegli un'opzione:

Se scegli...	Quindi...
Sì, iscriviti creando subito l'iscrizione	Vengono create sia la collaborazione che la tua iscrizione. Il tuo status nella collaborazione è attivo.
No, creerò un abbonamento in un secondo momento	Viene creata solo la collaborazione. Il tuo status nella collaborazione è inattivo.

b. Se sei il membro che può ricevere risultati, in Impostazioni predefinite dei risultati delle query, scegli un'opzione:

Se tu...	Allora...
Mantieni selezionata la casella di controllo Imposta impostazioni predefinite ora. (È selezionata per impostazione predefinita).	1. Per la destinazione dei risultati in Amazon S3, inserisci la destinazione Amazon S3. 2. Per il formato dei risultati della query, scegli CSV o PARQUET.
Deselezionate la casella di controllo Imposta subito le impostazioni predefinite	Viene creata solo la collaborazione. Il tuo status nella collaborazione è inattivo.

c. Se hai scelto di abilitare la registrazione delle query nella fase 4.e, scegli una delle seguenti opzioni per l'archiviazione dei log in Amazon CloudWatch Logs:

Se scegli...	Quindi...
Accendi	I log delle query che ti riguardano vengono archiviati in Amazon CloudWatch Logs. Ogni membro può ricevere solo i log delle query che ha avviato o che contengono i propri dati. Il membro che può ricevere risultati riceve anche i registri di tutte le query eseguite in una collaborazione, anche se non si accede ai relativi dati tramite una query.
Disattiva	I log delle query che ti riguardano non vengono archiviati nel tuo account Amazon CloudWatch Logs.

> **Note**
>
> Dopo aver attivato la registrazione delle query, possono essere necessari alcuni minuti per configurare l'archiviazione dei log e iniziare a ricevere i log in Amazon CloudWatch Logs. Durante questo breve periodo, il membro che può eseguire query potrebbe eseguire query che in realtà non inviano log.

d. Se desideri abilitare i tag per la risorsa dedicata all'iscrizione, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.

e. Se sei il membro che paga per le query, indica la tua accettazione selezionando la casella di controllo Accetto di pagare i costi di calcolo delle query in questa collaborazione.

> **Note**
>
> È necessario selezionare questa casella di controllo per procedere.
> Per ulteriori informazioni su come vengono calcolati i prezzi, consultaPrezzi per AWS Clean Rooms.

Se sei il socio che paga i costi di elaborazione delle query ma non sei il socio che può eseguire le query, ti consigliamo di Budget AWS utilizzare l'opzione per configurare un budget AWS Clean Rooms e ricevere notifiche una volta raggiunto il budget massimo. Per ulteriori informazioni sulla configurazione di un budget, consulta Gestire i costi con Budget AWS nella Guida per l'AWS Cost Managementutente. Per ulteriori informazioni sulla configurazione delle notifiche, consulta l'argomento Creazione di un Amazon SNS per le notifiche sul budget nella Guida per l'AWS Cost Managementutente. Se è stato raggiunto il budget massimo, puoi contattare il membro che può eseguire domande o abbandonare la collaborazione. Se lasci la collaborazione, non sarà più consentita l'esecuzione di query e pertanto non ti verranno più addebitati i costi di elaborazione delle query.

f. Seleziona Avanti.

6. Per il passaggio 3: revisione e creazione, procedi come segue:

a. Rivedi le selezioni effettuate per i passaggi precedenti e modificale se necessario.

b. Seleziona una delle seguenti opzioni:

Se hai scelto di...	Allora scegli...
Crea un abbonamento con la collabora zione (Sì, iscriviti creando un abbonamento ora)	Crea collaborazione e appartenenza
Crea la collaborazione e non creare un'iscrizione in questo momento (No, creerò un'iscrizione in un secondo momento)	Crea collaborazione

Dopo che la collaborazione è stata creata con successo, puoi vedere la pagina dei dettagli della collaborazione in Collaborazioni.

Passaggi successivi

Ora sei pronto per:

- Prepara la tabella di dati in cui eseguire le interrogazioni. AWS Clean Rooms (Facoltativo se desideri interrogare i tuoi dati).
- Associa la tabella configurata alla tua collaborazione. (Facoltativo se desideri interrogare i tuoi dati).
- Configura una regola di analisi per la tabella configurata. (Facoltativo se desideri interrogare i tuoi dati).
- Crea un'iscrizione e partecipa a una collaborazione.
- Gestisci la tua collaborazione.

Creare un'iscrizione e partecipare a una collaborazione

Un'iscrizione è una risorsa che viene creata quando un membro entra a far parte di una collaborazione in AWS Clean Rooms.

È possibile partecipare a una collaborazione come membro che può interrogare i dati, membro che può ricevere i risultati di una query o entrambi. Puoi anche partecipare a una collaborazione come membro pagando i costi di elaborazione delle query. Tutti i membri possono fornire dati.

Per informazioni su come creare un'iscrizione e partecipare a una collaborazione utilizzando gli AWS SDK, consulta l'AWS Clean Rooms API Reference.

Argomenti

Crea un'iscrizione e partecipa a una collaborazione

Per creare un'iscrizione e partecipare a una collaborazione

1. Accedi AWS Management Console e apri la AWS Clean Rooms console con il tuo membro Account AWS.
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Nella scheda Disponibili per partecipare, per Collaborazioni disponibili a cui partecipare, scegli il nome della collaborazione.
4. Nella pagina dei dettagli della collaborazione, visualizza i dettagli della collaborazione, inclusi i dettagli del membro e un elenco degli altri membri.

   Verifica che gli Account AWS ID di ogni membro della collaborazione siano quelli con cui intendi entrare nella collaborazione.
5. Scegli Crea iscrizione.
6. Nella pagina Crea iscrizione, nella Panoramica, visualizza il nome della collaborazione, la descrizione della collaborazione, l' Account AWS ID del creatore della collaborazione, le abilità dei membri e l' Account AWS ID del membro che pagherà per le domande.
7. Se il creatore della collaborazione ha scelto di abilitare la registrazione delle query, scegli una delle seguenti opzioni per l'archiviazione dei log in Amazon CloudWatch Logs:

Se scegli...	Quindi...
Accendi	I log delle query che ti riguardano vengono archiviati in Amazon CloudWatch Logs. Ogni membro può ricevere solo i log delle query che ha avviato o che contengono i propri dati. Il membro che può ricevere risultati riceve anche i registri di tutte le query eseguite in collaborazione, anche se non si accede ai dati in una query.
Disattiva	I log delle query che ti riguardano non vengono memorizzati nel tuo account Amazon CloudWatch Logs.

> **Note**
>
> Dopo aver attivato la registrazione delle query, possono essere necessari alcuni minuti per configurare l'archiviazione dei log e iniziare a ricevere i log in Amazon CloudWatch Logs. Durante questo breve periodo, il membro che può eseguire query potrebbe eseguire query che in realtà non inviano log.

8. Se le abilità del tuo socio includono Ricevi risultati:

   a. Per le impostazioni dei risultati di Query,

      i. Specificate la destinazione dei risultati in Amazon S3 inserendo la destinazione S3 o scegliete Sfoglia S3 per selezionarla da un elenco di bucket S3 disponibili.

         Example

         Ad esempio: **`s3://bucket/prefix`**

      ii. Scegli il formato del risultato (CSV o PARQUET).

b. Per l'accesso al servizio, scegli tra Crea e usa un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

> **Note**
>
> È necessario selezionare un ruolo di servizio esistente o disporre delle autorizzazioni per crearne uno nuovo. Per ulteriori informazioni, consulta Crea un ruolo di servizio per ricevere risultati.

9. Se desideri abilitare i tag per la risorsa dedicata all'iscrizione, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.
10. Se il creatore della collaborazione ti ha designato come membro responsabile del pagamento delle domande, indica l'accettazione selezionando la casella di controllo Accetto di pagare i costi di calcolo delle query in questa collaborazione.

> **Note**
>
> È necessario selezionare questa casella di controllo per procedere.
> Per ulteriori informazioni su come vengono calcolati i prezzi, consultaPrezzi per AWS Clean Rooms.

Se sei il socio che paga i costi di elaborazione delle query ma non sei il socio che può eseguire le query, ti consigliamo di Budget AWS utilizzare l'opzione per configurare un budget AWS Clean Rooms e ricevere notifiche una volta raggiunto il budget massimo. Per ulteriori informazioni sulla configurazione di un budget, consulta Gestire i costi con Budget AWS nella Guida per l'AWS Cost Management utente. Per ulteriori informazioni sulla configurazione delle notifiche, consulta l'argomento Creazione di un Amazon SNS per le notifiche sul budget nella Guida per l'AWS Cost Management utente. Se è stato raggiunto il budget massimo, puoi contattare il membro che può eseguire domande o abbandonare la collaborazione. Se lasci la collaborazione, non sarà più consentita l'esecuzione di query e pertanto non ti verranno più addebitati i costi di elaborazione delle query.

11. Se sei sicuro di voler creare un'iscrizione e partecipare alla collaborazione, scegli Crea iscrizione.

Ti viene concesso l'accesso in lettura ai metadati di collaborazione. Ciò include informazioni come il nome visualizzato e la descrizione della collaborazione, oltre a tutti i nomi e gli Account AWS ID degli altri membri.

Per informazioni su come abbandonare una collaborazione, vedereLasciare una collaborazione.

Passaggi successivi

Ora sei pronto per:

- Prepara la tabella di dati in cui eseguire le interrogazioni. AWS Clean Rooms (Facoltativo se desideri interrogare i tuoi dati).
- Associa la tabella configurata alla tua collaborazione.
- Configura una regola di analisi per la tabella configurata.

Preparazione delle tabelle di dati per le interrogazioni in AWS Clean Rooms

> **Note**
>
> La preparazione delle tabelle di dati può avvenire prima o dopo l'adesione a una collaborazione. Dopo aver preparato una tabella, puoi riutilizzarla in più collaborazioni purché le tue esigenze di privacy per quella tabella siano le stesse.

In qualità di membro della collaborazione, devi preparare le tabelle di dati prima che possano essere consultate AWS Clean Rooms dal membro della collaborazione che può eseguire le query.

Se il tuo caso d'uso non richiede l'inserimento di dati personali, puoi saltare questa procedura.

Se le tabelle di dati sono già catalogate AWS Glue, passa a. Creazione di una tabella configurata in AWS Clean Rooms

La preparazione delle tabelle di dati prevede i seguenti passaggi:

- Fase 1: completamento dei prerequisiti
- Fase 2: (Facoltativo) Preparare i dati per il calcolo crittografico
- Fase 3: carica la tabella di dati su Amazon S3
- Fase 4: Creare una AWS Glue tabella
- Passaggi successivi

Per ulteriori informazioni sui formati di dati che è possibile utilizzare per le query, vedereFormati di dati per AWS Clean Rooms.

Fase 1: completamento dei prerequisiti

Per preparare le tabelle di dati da utilizzare con AWS Clean Rooms, è necessario completare i seguenti prerequisiti:

- I set di dati devono essere salvati come uno dei formati di dati supportati per. AWS Clean Rooms

- Le tabelle di dati devono essere catalogate AWS Glue e utilizzare i tipi di dati supportati per. AWS Clean Rooms
- Tutte le tabelle di dati devono essere archiviate in Amazon Simple Storage Service (Amazon S3) Regione AWS nello stesso luogo in cui è stata creata la collaborazione.
- AWS Glue Data Catalog Devono trovarsi nella stessa regione in cui è stata creata la collaborazione.
- AWS Glue Data Catalog Devono appartenere alla Account AWS stessa categoria di appartenenza.
- Il bucket Amazon S3 non può essere registrato con. AWS Lake Formation
- Il creatore della collaborazione ha creato una collaborazione in. AWS Clean Rooms Per ulteriori informazioni, consulta Creazione di una collaborazione in AWS Clean Rooms.
- Il creatore della collaborazione ti ha inviato l'ID della collaborazione come partecipante alla collaborazione.

Fase 2: (Facoltativo) Preparare i dati per il calcolo crittografico

(Facoltativo) Se utilizzi il calcolo crittografico e la tabella di dati contiene informazioni sensibili che desideri crittografare, devi crittografare la tabella di dati utilizzando il client di crittografia C3R.

Per preparare i dati per l'elaborazione crittografica, segui le procedure riportate in. Preparazione di tabelle di dati crittografate con Cryptographic Computing per Clean Rooms

Fase 3: carica la tabella di dati su Amazon S3

> **Note**
>
> Se intendi utilizzare tabelle di dati crittografate nella collaborazione, devi prima crittografare i dati per il calcolo crittografico prima di caricare la tabella di dati su Amazon S3. Per ulteriori informazioni, consulta Preparazione di tabelle di dati crittografate con Cryptographic Computing per Clean Rooms.

Per caricare la tabella di dati su Amazon S3

1. Accedi AWS Management Console e apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. Scegli Bucket, quindi scegli un bucket in cui archiviare la tabella di dati.

3. Scegli Carica, quindi segui le istruzioni.
4. Scegli la scheda Oggetti per visualizzare il prefisso in cui sono archiviati i dati. Prendi nota del nome della cartella.

   È possibile selezionare la cartella per visualizzare i dati.

Fase 4: Creare una AWS Glue tabella

Se hai già una tabella di AWS Glue dati, puoi saltare questo passaggio.

In questo passaggio, configuri un crawler AWS Glue che esegue la scansione di tutti i file nel bucket S3 e crea una tabella. AWS Glue Per ulteriori informazioni, consulta Definizione dei crawler nella Guida per l'utente. AWS GlueAWS Glue

Per ulteriori informazioni sui tipi di AWS Glue Data Catalog dati supportati, consulta. Tipi di dati supportati

> **Note**
>
> AWS Clean Rooms attualmente non supporta i bucket S3 registrati con. AWS Lake Formation

La procedura seguente descrive come creare una AWS Glue tabella. Se desideri utilizzare un AWS Glue Data Catalog oggetto crittografato con una chiave AWS Key Management Service (AWS KMS), devi configurare la politica di autorizzazione delle chiavi KMS per consentire l'accesso a quella tabella crittografata. Per ulteriori informazioni, consulta Configurare la crittografia in AWS Glue nella AWS Glue Developer Guide.

Per creare una AWS Glue tabella

1. Segui la procedura Working with crawler on the AWS Glue console nella Guida per l'AWS Glue utente.
2. Prendi nota del nome del AWS Glue database e del nome della AWS Glue tabella.

Passaggi successivi

Ora che hai preparato le tabelle di dati, sei pronto per:

- Creare una tabella configurata
- Crea un modello ML

Formati di dati per AWS Clean Rooms

I set di dati utilizzati per le query AWS Clean Rooms sono in genere gli stessi tipi di set di dati utilizzati per altre applicazioni. Ad esempio, gli stessi tipi di set di dati vengono utilizzati con Amazon Athena, Amazon EMR, Amazon Redshift Spectrum e Amazon. QuickSight Puoi interrogare i dati nel formato originale direttamente da Amazon Simple Storage Service (Amazon S3).

Per interrogare i dati, i set di dati devono essere in un formato che AWS Clean Rooms supporti. Il bucket Amazon S3 con i set di dati e il AWS Clean Rooms cluster deve trovarsi nello stesso. Regione AWS

Formati di dati supportati

AWS Clean Rooms supporta i seguenti formati strutturati:

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

> **Note**
>
> Un `timestamp` valore in un file di testo deve essere nel formato. `yyyy-MM-dd HH:mm:ss.SSSSSS` Ad esempio:`2017-05-01 11:30:59.000000`.

Ti consigliamo di utilizzare un formato di file di archiviazione a colonne, ad esempio. Apache Parquet Con un formato di questo tipo, è possibile ridurre al minimo il trasferimento di dati al di fuori di Amazon S3 selezionando solo le colonne necessarie. Per prestazioni ottimali, gli oggetti di grandi dimensioni devono essere suddivisi in oggetti da 100 MB a 1 GB.

Tipi di dati supportati

Per un'esperienza ottimale con AWS Clean Rooms, tutti i dati devono essere catalogati in. AWS Glue Per ulteriori informazioni, consulta la sezione intitolata Guida introduttiva alla Guida per AWS Glue Data Catalog gli AWS Glue sviluppatori.

AWS Clean Rooms supporta i seguenti tipi di AWS Glue Data Catalog dati:

- bigint
- boolean
- char
- date
- decimal
- double
- float
- int
- Tipi di dati annidati come:
  - array
  - map
  - struct
- smallint
- string
- timestamp
- varchar

AWS Clean Rooms non supporta:

- binary
- intervallo

tipi di compressione dei file per AWS Clean Rooms

Per ridurre lo spazio di archiviazione, migliorare le prestazioni e ridurre al minimo i costi, consigliamo vivamente di comprimere i set di dati.

AWS Clean Rooms riconosce i tipi di compressione dei file in base all'estensione del file e supporta i tipi e le estensioni di compressione mostrati nella tabella seguente.

Algoritmo di compressione	Estensione di file
GZIP	.gz
Bzip2	.bz2
Snappy	.snappy

Puoi applicare la compressione a diversi livelli. Più comunemente, comprimi un intero file o comprimi singoli blocchi all'interno di un file. La compressione dei formati colonnari a livello di file non offre vantaggi in termini di prestazioni.

Crittografia lato server per AWS Clean Rooms

> **Note**
>
> La crittografia lato server non sostituisce l'elaborazione crittografica per i casi d'uso che la richiedono.

AWS Clean Rooms decrittografa in modo trasparente i set di dati crittografati utilizzando le seguenti opzioni di crittografia:

- SSE-S3: crittografia lato server con una chiave di crittografia AES-256 gestita da Amazon S3
- SSE-KMS: crittografia lato server con chiavi gestite da AWS Key Management Service

Per utilizzare SSE-S3, il ruolo di AWS Clean Rooms servizio utilizzato per associare la tabella configurata alla collaborazione deve disporre delle autorizzazioni KMS-Decrypt. Per utilizzare SSE-KMS, la politica delle chiavi KMS deve consentire anche la decrittografia del ruolo di servizio. AWS Clean Rooms

AWS Clean Rooms non supporta la crittografia lato client di Amazon S3. Per ulteriori informazioni sulla crittografia lato server, consulta Protezione dei dati utilizzando la crittografia lato server nella Guida per l'utente di Amazon Simple Storage Service.

Utilizzo Apache Iceberg delle tabelle in AWS Clean Rooms

Apache Icebergè un formato di tabella open source per data lake. AWS Clean Rooms può utilizzare le statistiche memorizzate nei Apache Iceberg metadati per ottimizzare i piani di interrogazione e ridurre le scansioni dei file durante l'elaborazione delle query in camera bianca. Per ulteriori informazioni, consulta la documentazione di Apache Iceberg.

Considerate quanto segue quando utilizzate AWS Clean Rooms con le tabelle Iceberg:

- Tabelle all'interno di AWS Glue Data Catalog Only: Apache Iceberg le tabelle devono essere definite in AWS Glue Data Catalog base all'implementazione open source del catalogo Glue.
- Formato di file Parquet: supporta AWS Clean Rooms solo le tabelle Iceberg nel formato di file di dati Parquet.
- Compressione GZIP e Snappy: AWS Clean Rooms supporta Parquet con GZIP e compressione. Snappy
- Versioni Iceberg: AWS Clean Rooms supporta l'esecuzione di query sulle tabelle Iceberg versione 1 e versione 2.
- Partizioni: non è necessario aggiungere manualmente le partizioni per le tabelle. Apache Iceberg AWS Glue AWS Clean Rooms rileva automaticamente le nuove partizioni nelle Apache Iceberg tabelle e non è necessaria alcuna operazione manuale per aggiornare le partizioni nella definizione della tabella. Le partizioni Iceberg vengono visualizzate come colonne regolari nello schema della AWS Clean Rooms tabella e non separatamente come chiave di partizione nello schema della tabella configurato.
- Limitazioni
  - Solo nuove tabelle Iceberg

    Apache Icebergle tabelle convertite da Apache Parquet tabelle non sono supportate.
  - Query temporali

    AWS Clean Rooms non supporta le interrogazioni sui viaggi nel tempo con le Apache Iceberg tabelle.
  - Motore Athena versione 2

Icebergle tabelle create con la versione 2 del motore Athena non sono supportate.

- Formati di file

  Avroe i formati di file Orc (Optimized Row Columnar) non sono supportati.

- Compressione

  ZstandardLa compressione (Zstd) per non è supportata. Parquet

Tipi di dati supportati per le tabelle Iceberg

AWS Clean Rooms può interrogare Iceberg tabelle che contengono i seguenti tipi di dati:

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

Per ulteriori informazioni sui tipi di tabella Iceberg, consulta Schemi per Iceberg nella documentazione di Apache.

Preparazione di tabelle di dati crittografate con Cryptographic Computing per Clean Rooms

Cryptographic Computing for Clean Rooms (C3R) è una funzionalità di. AWS Clean RoomsÈ possibile utilizzare C3R per limitare crittograficamente ciò che può essere appreso da qualsiasi parte e in collaborazione. AWS AWS Clean Rooms

Puoi crittografare la tabella di dati utilizzando il client di crittografia C3R, uno strumento di crittografia lato client, prima di caricare la tabella di dati su Amazon Simple Storage Service (Amazon S3).

Per ulteriori informazioni, consulta Elaborazione crittografica per Clean Rooms.

La preparazione di tabelle di dati crittografate con C3R prevede i seguenti passaggi:

Fasi

- Fase 1: completamento dei prerequisiti
- Passaggio 2: scarica il client di crittografia C3R
- (Facoltativo) Fase 3: Visualizza i comandi disponibili nel client di crittografia C3R
- Fase 4: Generazione di uno schema di crittografia per un file tabulare
- Fase 5: Creare una chiave segreta condivisa
- Passaggio 6: memorizza la chiave segreta condivisa in una variabile di ambiente
- Fase 7: Crittografare i dati
- Fase 8: Verifica della crittografia dei dati
- (Facoltativo) Creare uno schema (utenti esperti)

Fase 1: completamento dei prerequisiti

Per preparare le tabelle di dati da utilizzare con C3R, è necessario completare i seguenti prerequisiti:

- È possibile accedere al repository Cryptographic Computing for su: Clean Rooms GitHub

  https://github.com/aws/c3r
- Sono state configurate AWS le credenziali per utilizzare il client di crittografia C3R. Queste credenziali vengono utilizzate dal client di crittografia C3R per le chiamate API di sola lettura volte a recuperare i metadati di collaborazione. AWS Clean Rooms Per ulteriori informazioni,

consulta Configurazione di nella Guida per l'utente per la versione 2 AWS CLI.AWS Command Line Interface

- Sul computer sono installate Java Runtime Environment (JRE) 11 o versioni successive.
  - Il programma consigliatoJava Runtime Environment, Amazon Corretto 11 o versione successiva, può essere scaricato da https://aws.amazon.com/corretto.
  - La Java Development Kit (JDK) include una versione corrispondente JRE della stessa. Tuttavia, le funzionalità aggiuntive di non JDK sono necessarie per eseguire il client di crittografia Cryptographic Computing for Clean Rooms (C3R).
- I tuoi file di dati tabulari (.csv) o file (. Parquet parquet) vengono salvati localmente.
- Tu o un altro membro della collaborazione avete la possibilità di creare una chiave segreta condivisa. Per ulteriori informazioni, consulta Fase 5: Creare una chiave segreta condivisa.
- Il creatore della collaborazione ha creato una collaborazione AWS Clean Rooms con il calcolo crittografico abilitato alla collaborazione. Per ulteriori informazioni, consulta Creazione di una collaborazione in AWS Clean Rooms.
- L'autore della collaborazione ti ha inviato l'ID della collaborazione come partecipante alla collaborazione. La collaborazione Amazon Resource Name (ARN) è inclusa nell'invito inviato, che contiene l'ID di collaborazione.

Passaggio 2: scarica il client di crittografia C3R

Per scaricare il client di crittografia C3R da GitHub

1. Vai al repository Cryptographic Computing for Clean RoomsAWSGitHub: https://github.com/aws/c3r
2. Seleziona e scarica i file.

   Il codice sorgente, le licenze e il materiale correlato possono essere clonati o scaricati come file. zipfile dalla pagina di destinazione del GitHub repository. (Vedi il pulsante Codice in alto a destra nell'elenco dei contenuti del repository).

   L'ultimo client di crittografia C3R firmato Java Executable File (ovvero l'applicazione di interfaccia a riga di comando) si trova nella pagina Releases del repository. GitHub

   Il pacchetto client di crittografia C3R per Apache Spark (`c3r-cli-spark`) è una versione di c3r-cli che deve essere inviata come job a un server Apache Spark in esecuzione. Per ulteriori informazioni, vedete Esecuzione di C3R su Apache Spark.

(Facoltativo) Fase 3: Visualizza i comandi disponibili nel client di crittografia C3R

Utilizzate questa procedura per acquisire familiarità con i comandi disponibili nel client di crittografia C3R.

Per visualizzare tutti i comandi disponibili nel client di crittografia C3R

1. Da un'interfaccia a riga di comando (CLI), accedi alla cartella che contiene il file scaricatoc3r-cli.jar.
2. Esegui il comando riportato qui di seguito: `java -jar c3r-cli.jar`
3. Visualizza l'elenco dei comandi e delle opzioni disponibili.

Fase 4: Generazione di uno schema di crittografia per un file tabulare

Per crittografare i dati, è necessario uno schema di crittografia che descriva come verranno utilizzati i dati. Questa sezione descrive come il client di crittografia C3R aiuta a generare uno schema di crittografia per un file CSV con una riga di intestazione o un file. Parquet

È sufficiente eseguire questa operazione una sola volta per file. Una volta che lo schema esiste, può essere riutilizzato per crittografare lo stesso file (o qualsiasi file con nomi di colonna identici). Se i nomi delle colonne o lo schema di crittografia desiderato cambiano, è necessario aggiornare il file dello schema. Per ulteriori informazioni, consulta (Facoltativo) Creare uno schema (utenti esperti).

> **Important**
>
> È fondamentale che tutte le parti che collaborano utilizzino la stessa chiave segreta condivisa. Le parti che collaborano dovrebbero inoltre coordinare i nomi delle colonne in modo che corrispondano se verranno visualizzati o JOIN confrontati in altro modo per garantire l'uguaglianza nelle query. In caso contrario, le query SQL potrebbero produrre risultati imprevisti o errati. Tuttavia, ciò non è necessario se il creatore della collaborazione ha abilitato l'impostazione di `allowJoinsOnColumnsWithDifferentNames` crittografia durante la creazione della collaborazione. Per ulteriori informazioni sulle impostazioni relative alla crittografia, vedere. Parametri di calcolo crittografico

Quando viene eseguito in modalità schema, il client di crittografia C3R analizza il file di input colonna per colonna, chiedendo se e come tale colonna debba essere trattata. Se il file contiene molte colonne non desiderate per l'output crittografato, la generazione dello schema interattivo potrebbe diventare noiosa perché è necessario saltare ogni colonna indesiderata. Per evitare ciò, è possibile scrivere manualmente uno schema o creare una versione semplificata del file di input contenente solo le colonne desiderate. Quindi, il generatore di schemi interattivo potrebbe essere eseguito su quel file ridotto. Il client di crittografia C3R fornisce informazioni sul file di schema e chiede all'utente come includere o crittografare (se del caso) le colonne di origine nell'output di destinazione.

Per ogni colonna di origine nel file di input, viene richiesto di:

1. Quante colonne di destinazione devono essere generate
2. Come deve essere crittografata ogni colonna di destinazione (se non del tutto)
3. Il nome di ogni colonna di destinazione
4. Come devono essere aggiunti i dati prima della crittografia se la colonna viene crittografata come sealed colonna

> **Note**
>
> Quando si crittografano i dati per una colonna che è stata crittografata come sealed colonna, è necessario determinare quali dati devono essere riempiti. Il client di crittografia C3R suggerisce un riempimento predefinito durante la generazione dello schema che riempie tutte le voci di una colonna con la stessa lunghezza.
> Quando si determina la lunghezza di`fixed`, si noti che il padding è in byte, non in bit.

Di seguito è riportata una tabella decisionale per la creazione dello schema.

Tabella decisionale dello schema

Decisione	Numero di colonne di destinazione dalla colonna di origine <' name-of-column '>?	Tipo di colonna di destinazione: [c]cleartext, [f] fingerprint o [s]? sealed	Nome dell'intestazione della colonna di destinazione <default 'name-of-column'>	Aggiungi il suffisso <suffix>all'intestazione per indicare come è stata crittografata, [y] sì o [n] no <default 'yes'>	<' name-of-column _sealed'> tipo di imbottitura: [n] one, [f] fissa o [m] max <default 'max'>
Lascia la colonna non crittografata.	1	c	Non applicabile	Non applicabile	Non applicabile
Crittografa la colonna come fingerprint colonna.	1	f	Scegli il valore predefinito o inserisci un nuovo nome di intestazione.	Immettete y per scegliere default (`_fingerprint`) o invio.	Non applicabile
Crittografa la colonna come sealed colonna.	1	s	Scegli il valore predefinito o inserisci un nuovo nome di intestazione.	Immettete y per scegliere default (`_sealed`) o invio.	Scegliete il tipo di imbottitura. Per ulteriori informazioni, consulta (Facoltativo) Creare uno schema (utenti esperti).

Decisione	Numero di colonne di destinazione dalla colonna di origine <' name-of-column '>?	Tipo di colonna di destinazione: [c]cleartext, [f] fingerprint o [s]? sealed	Nome dell'intestazione della colonna di destinazione <default 'name-of-column'>	Aggiungi il suffisso <suffix>all'intestazione per indicare come è stata crittografata, [y] sì o [n] no <default 'yes'>	<' name-of-column _sealed'> tipo di imbottitura: [n] one, [f] fissa o [m] max <default 'max'>
Crittografa la colonna sia come siafingerprint. sealed	2	Inserisci la prima colonna di destinazione: f. Inserisci la seconda colonna di destinazione: s.	Scegli le intestazioni di destinazione per ogni colonna di destinazione.	Inserisci y per scegliere il valore predefinito o inserisci n.	Scegli il tipo di spaziatura (solo per sealed le colonne). Per ulteriori informazioni, consulta (Facoltativo) Creare uno schema (utenti esperti).

Di seguito sono riportati due esempi di come creare schemi di crittografia. Il contenuto esatto dell'interazione dipende dal file di input e dalle risposte fornite.

Esempi

- Esempio: generazione di uno schema di crittografia per una fingerprint colonna e una cleartext colonna
- Esempio: generazione di uno schema di crittografia con sealedfingerprint, e colonne cleartext

Esempio: generazione di uno schema di crittografia per una fingerprint colonna e una cleartext colonna

In questo esempio, per`ads.csv`, ci sono solo due colonne: `username` e`ad_variant`. Per queste colonne, vogliamo quanto segue:

- Affinché la `username` colonna venga crittografata come `fingerprint` colonna
- Perché la `ad_variant` colonna sia una `cleartext` colonna

Per generare uno schema di crittografia per una fingerprint colonna e una cleartext colonna

1. (Facoltativo) Per garantire la presenza del c3r-cli.jar file e del file da crittografare:

   a. Accedere alla directory desiderata ed eseguire `ls` (se si utilizza un Mac oUnix/Linux) o `dir` se si utilizzaWindows).

   b. Visualizza l'elenco dei file di dati tabulari (ad esempio, .csv) e scegli un file da crittografare.

      In questo esempio, `ads.csv` è il file che vogliamo crittografare.

2. Dalla CLI, esegui il comando seguente per creare uno schema in modo interattivo.

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

   > **Note**
   >
   > - Puoi correre. `java --jar PATH/TO/c3r-cli.jar` Oppure, se l'hai aggiunta `PATH/TO/c3r-cli.jar` alla variabile di ambiente CLASSPATH, puoi anche eseguire il nome della classe. Il client di crittografia C3R cercherà nel CLASSPATH per trovarla (ad esempio,). `java com.amazon.psion.cli.Main`
   > - Il `--interactive` flag seleziona la modalità interattiva per lo sviluppo dello schema. Questo guida l'utente attraverso una procedura guidata per la creazione dello schema. Gli utenti con competenze avanzate possono creare il proprio schema JSON senza utilizzare la procedura guidata. Per ulteriori informazioni, consulta (Facoltativo) Creare uno schema (utenti esperti).
   > - Il `--output` flag imposta un nome di output. Se non includi il `--output` flag, il client di crittografia C3R tenta di scegliere un nome di output predefinito (ad esempio `<input>.out.csv` o per lo schema,`<input>.json`).

3. Per**`Number of target columns from source column 'username'?`**, inserisci **`1`** e poi premi Invio.
4. Per`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, inserisci **`f`** e poi premi Invio.
5. Per`Target column headername <default 'username'>`, premi Invio.

   Viene utilizzato il nome predefinito `username` ".
6. Per`Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, inserisci **`y`** e poi premi Invio.

   > **Note**
   >
   > La modalità interattiva suggerisce suffissi da aggiungere alle intestazioni delle colonne crittografate (`_fingerprint`per fingerprint colonne e `_sealed` per sealed colonne). I suffissi possono essere utili quando si eseguono attività come il caricamento di dati o la creazione di collaborazioni. Servizi AWS AWS Clean Rooms Questi suffissi possono aiutare a indicare cosa si può fare con i dati crittografati in ogni colonna. Ad esempio, le cose non funzioneranno se si crittografa una colonna come sealed colonna (`_sealed`) e si tenta di inserirla o si tenta il JOIN contrario.
7. Per`Number of target columns from source column 'ad_variant'?`, inserisci **`1`** e poi premi Invio.
8. Per`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, inserisci **`c`** e poi premi Invio.
9. Per`Target column headername <default 'username'>`, premi Invio.

   Viene utilizzato il nome predefinito `ad_variant` ".

   Lo schema viene scritto in un nuovo file chiamato`ads.json`.

   > **Note**
   >
   > È possibile visualizzare lo schema aprendolo in qualsiasi editor di testo, ad esempio Notepad on Windows or TextEdit onmacOS.
10. Ora sei pronto per crittografare i dati.

Esempio: generazione di uno schema di crittografia con sealedfingerprint, e colonne cleartext

In questo esempio, for`sales.csv`, sono presenti tre colonne:`username`,`purchased`, e`product`. Per queste colonne, vogliamo quanto segue:

- Perché la `product` colonna sia una `sealed` colonna
- Perché la `username` colonna venga crittografata come `fingerprint` colonna
- Perché la `purchased` colonna sia una `cleartext` colonna

Per generare uno schema di crittografia con sealedfingerprint, e cleartext colonne

1. (Facoltativo) Per garantire la presenza del c3r-cli.jar file e del file da crittografare:

   a. Accedere alla directory desiderata ed eseguire `ls` (se si utilizza un Mac oUnix/Linux) o `dir` se si utilizzaWindows).

   b. Visualizza l'elenco dei file di dati tabulari (.csv) e scegli un file da crittografare.

      In questo esempio, `sales.csv` è il file che vogliamo crittografare.

2. Dalla CLI, esegui il comando seguente per creare uno schema in modo interattivo.

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

   > **Note**
   >
   > - Il `--interactive` flag seleziona la modalità interattiva per lo sviluppo dello schema. Questo guida l'utente attraverso un flusso di lavoro guidato per la creazione dello schema.
   > - Se sei un utente esperto, puoi creare il tuo schema JSON senza utilizzare il flusso di lavoro guidato. Per ulteriori informazioni, consulta (Facoltativo) Creare uno schema (utenti esperti).
   > - Per i file.csv senza intestazioni di colonna, consulta il `--noHeaders` flag per il comando schema disponibile nella CLI.

- Il `--output` flag imposta un nome di output. Se non includi il `--output` flag, il client di crittografia C3R tenta di scegliere un nome di output predefinito (ad esempio `<input>.out` o per lo schema,`<input>.json`).

3. Per**`Number of target columns from source column ‘username’?`**, inserisci **`1`** e poi premi Invio.
4. Per`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, inserisci **`f`** e poi premi Invio.
5. Per`Target column headername <default 'username'>`, premi Invio.

   Viene utilizzato il nome predefinito `username` ".
6. Per`Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`, inserisci **`y`** e poi premi Invio.
7. Per`Number of target columns from source column ‘purchased’?`, inserisci **`1`** e poi premi Invio.
8. Per`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, inserisci **`c`** e poi premi Invio.
9. Per`Target column headername <default 'purchased'>`, premi Invio.

   Viene utilizzato il nome predefinito `purchased` ".
10. Per`Number of target columns from source column ‘product’?`, inserisci **`1`** e poi premi Invio.
11. Per`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`, inserisci **`s`** e poi premi Invio.
12. Per`Target column headername <default 'product'>`, premi Invio.

    Viene utilizzato il nome predefinito `product` ".
13. Per`‘product_sealed’ padding type: [n]one, [f]ixed, or [m]ax <default ’max’?>`, premi Invio per scegliere il valore predefinito.
14. Per `Byte-length beyond max length to pad cleartext to in ‘product_sealed’ <default ‘0’>?` premere Invio per scegliere l'impostazione predefinita.

    Lo schema viene scritto in un nuovo file chiamato`sales.json`.
15. Ora sei pronto per crittografare i dati.

Fase 5: Creare una chiave segreta condivisa

Per crittografare le tabelle di dati, i partecipanti alla collaborazione devono concordare e condividere in modo sicuro una chiave segreta condivisa.

La chiave segreta condivisa deve essere di almeno 256 bit (32 byte). Puoi specificare una chiave più grande, ma non ti offrirà alcuna sicurezza aggiuntiva.

> **Important**
>
> Ricorda che la chiave e l'ID di collaborazione utilizzati per la crittografia e la decrittografia devono essere identici per tutti i partecipanti alla collaborazione.

Le sezioni seguenti forniscono esempi di comandi da console per generare una chiave segreta condivisa salvata `secret.key` nella directory di lavoro corrente del rispettivo terminale.

Argomenti

- Esempio: generazione di chiavi utilizzando OpenSSL
- Esempio: generazione di chiavi sull'Windowsutilizzo PowerShell

Esempio: generazione di chiavi utilizzando OpenSSL

Per una libreria crittografica generica comune, esegui il comando seguente per creare una chiave segreta condivisa.

```
openssl rand 32 > secret.key
```

Se stai utilizzando Windows e non l'hai OpenSSL installata, puoi generare chiavi utilizzando l'esempio descritto in Esempio: generazione di chiavi sull'Windowsutilizzo PowerShell.

Esempio: generazione di chiavi sull'Windowsutilizzo PowerShell

Per PowerShell un'applicazione terminale disponibile suWindows, esegui il seguente comando per creare una chiave segreta condivisa.

```
$bs = New-Object Byte[](32);
[Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($bs); Set-
Content 'secret.key' -Encoding Byte -Value $bs
```

Passaggio 6: memorizza la chiave segreta condivisa in una variabile di ambiente

Una variabile di ambiente è un modo comodo ed estensibile per gli utenti di fornire una chiave segreta da vari archivi di chiavi AWS Secrets Manager e passarla al client di crittografia C3R.

Il client di crittografia C3R può utilizzare le chiavi archiviate in Servizi AWS se si utilizza il AWS CLI per memorizzare tali chiavi nella variabile di ambiente pertinente. Ad esempio, il client di crittografia C3R può utilizzare una chiave di. AWS Secrets Manager Per ulteriori informazioni, consulta Creare e gestire segreti AWS Secrets Manager nella Guida per l'AWS Secrets Manager utente.

> **Note**
>
> Tuttavia, prima di utilizzare un dispositivo Servizio AWS come supporto AWS Secrets Manager per conservare le chiavi C3R, verificate che il vostro caso d'uso lo consenta. Alcuni casi d'uso potrebbero richiedere che la chiave venga nascosta. AWS Questo per garantire che i dati crittografati e la chiave non siano mai detenuti dalla stessa terza parte.

Gli unici requisiti per una chiave segreta condivisa sono che la chiave segreta condivisa sia base64 codificata e memorizzata nella variabile di ambiente. `C3R_SHARED_SECRET`

Le sezioni seguenti descrivono i comandi della console per convertire un `secret.key` file base64 e archiviarlo come variabile di ambiente. Il `secret.key` file potrebbe essere stato generato da uno qualsiasi dei comandi elencati in Fase 5: Creare una chiave segreta condivisa ed è solo una fonte di esempio.

Memorizza la chiave in una variabile di ambiente durante Windows l'utilizzo PowerShell

Per convertire base64 e impostare la variabile di ambiente in Windows usoPowerShell, esegui il seguente comando.

```
$Bytes=[IO.File]::ReadAllBytes((Get-Location).ToString()+'\secret.key');
 $env:C3R_SHARED_SECRET=[Convert]::ToBase64String($Bytes)
```

Memorizza la chiave in una variabile di ambiente su Linux o macOS

Per convertire base64 e impostare la variabile di ambiente su Linux omacOS, esegui il comando seguente.

```
export C3R_SHARED_SECRET="$(cat secret.key | base64)"
```

Fase 7: Crittografare i dati

Per eseguire questo passaggio, è necessario acquisire l'ID di AWS Clean Rooms collaborazione e la chiave segreta condivisa. Per ulteriori informazioni, consultare Prerequisiti.

Nell'esempio seguente, eseguiamo la crittografia utilizzando lo schema che abbiamo creato chiamato`ads.json`. `ads.csv`

Per crittografare i dati

1. Memorizza la chiave segreta condivisa per la collaborazione inPassaggio 6: memorizza la chiave segreta condivisa in una variabile di ambiente.
2. Dalla riga di comando, inserisci il seguente comando.

   ```
   java -jar c3r-cli.jar encrypt <name of input .csv file> --schema=<name of schema .json file> --id=<collaboration id> --output=<name of output.csv file> <optional flags>
   ```
3. Per<name of input .csv file>, inserisci il nome del file.csv di input.
4. Per`schema=`, inserisci il nome del file dello schema di crittografia .json.
5. Per`id=`, inserisci l'ID di collaborazione.
6. Per`output=`, inserisci il nome del file di output (ad esempio,`ads-output.csv`).
7. Includete tutti i flag della riga di comando descritti in Parametri di calcolo crittografico andFlag opzionali in Cryptographic Computing per Clean Rooms.
8. Esegui il comando .

Nell'esempio per`ads.csv`, eseguiamo il comando seguente.

java -jar c3r-cli.jar encrypt ***ads.csv*** --schema=***ads.json*** --id=***123e4567-e89b-42d3-a456-556642440000*** --output=***ads-output.csv***

Nell'esempio persales.csv, eseguiamo il comando seguente.

java -jar c3r-cli.jar encrypt ***sales.csv*** --schema=***sales.json*** --id=***123e4567-e89b-42d3-a456-556642440000***

> **Note**
>
> In questo esempio, non specifichiamo il nome del file di output (`--output=`*`sales-output.csv`*). Di conseguenza, è `name-of-file.out.csv` stato generato il nome del file di output predefinito.

Ora sei pronto per verificare i dati crittografati.

Fase 8: Verifica della crittografia dei dati

Per verificare che i dati siano stati crittografati

1. Visualizza il file di dati crittografato (ad esempio,`sales-output.csv`).
2. Verifica le seguenti colonne:
   a. Colonna 1: crittografata (ad esempio,`username_fingerprint`).

      Per le fingerprint colonne (HMAC), dopo il prefisso di versione e tipo (ad esempio,`01:hmac:`), ci sono 44 caratteri di dati codificati in base 64.
   b. Colonna 2: non crittografata (ad esempio,). `purchased`
   c. Colonna 3: crittografata (ad esempio,`product_sealed`).

      Per le colonne criptate (SELECT), la lunghezza della spaziatura cleartext più l'eventuale spaziatura dopo la versione e il prefisso di tipo (ad esempio,`01:enc:`) è direttamente proporzionale alla lunghezza del prefisso cleartext crittografato. Cioè, la lunghezza è la dimensione dell'input più circa il 33 percento del sovraccarico dovuto alla codifica.

Ora sei pronto per:

1. Carica i dati crittografati su S3.
2. Crea una AWS Glue tabella.
3. Crea una tabella configurata in AWS Clean Rooms.

Il client di crittografia C3R creerà file temporanei che non contengono dati non crittografati (a meno che tali dati non vengano crittografati anche nell'output finale). Tuttavia, alcuni valori crittografati potrebbero non essere inseriti correttamente. Le colonne di impronte digitali potrebbero contenere valori duplicati, anche se l'impostazione di collaborazione lo è. `allowRepeatedFingerprintValue` `false` Questo problema si verifica perché il file temporaneo viene scritto prima della verifica delle corrette lunghezze di riempimento e delle proprietà di rimozione dei duplicati.

Se il client di crittografia C3R fallisce o viene interrotto durante la crittografia, potrebbe interrompersi dopo la scrittura del file temporaneo ma prima di verificare queste proprietà ed eliminare i file temporanei. Pertanto, questi file temporanei potrebbero essere ancora sul disco. In tal caso, il contenuto di questi file non protegge i dati in chiaro agli stessi livelli dell'output. In particolare, questi file temporanei potrebbero rivelare dati in chiaro ad analisi statistiche che non influirebbero sull'output finale. L'utente deve eliminare questi file (in particolare un SQLite database) per evitare che cadano in mani non autorizzate.

(Facoltativo) Creare uno schema (utenti esperti)

La creazione manuale di uno schema è riservata agli utenti esperti.

Di seguito è riportata una descrizione del formato di file dello schema JSON per i file di input con o senza intestazioni di colonna. Gli utenti esperti possono scrivere o modificare direttamente lo schema, se lo desiderano.

> **Note**
>
> Il client di crittografia C3R può aiutarti a creare uno schema tramite il processo interattivo descritto in Esempio: generazione di uno schema di crittografia con sealedfingerprint, e colonne cleartext o tramite la creazione di un modello di stub.

Schemi di tabelle mappati e posizionali

La sezione seguente descrive due tipi di schemi di tabelle:

- Schema di tabella mappato: questo schema viene utilizzato per crittografare i file.csv con una riga di intestazione e file. Apache Parquet

- Schema della tabella posizionale: questo schema viene utilizzato per crittografare i file.csv senza una riga di intestazione.

Il client di crittografia C3R può crittografare un file tabulare per una collaborazione. A tale scopo, deve disporre di un file di schema corrispondente che specifichi in che modo l'output crittografato deve essere derivato dall'input.

Il client di crittografia C3R può aiutare a generare uno schema per un `INPUT` file eseguendo il comando schema del client di crittografia C3R nella riga di comando. Un esempio di comando è. `java -jar c3r-cli.jar schema --interactive INPUT`

Lo schema specifica le seguenti informazioni:

1. Quali colonne di origine vengono mappate a quali colonne trasformate nel file di output tramite i nomi di intestazione (schemi mappati) o la posizione (schemi posizionali)
2. Quali colonne di destinazione devono rimanere cleartext
3. Quali colonne di destinazione devono essere crittografate per le SELECT query
4. Quali colonne di destinazione devono essere crittografate per le query JOIN

Queste informazioni sono codificate in un file di schema JSON specifico della tabella, che consiste in un singolo oggetto il cui `headerRow` campo è un valore booleano. Il valore deve riguardare Parquet i file e `true` i file.csv con una riga di intestazione e altro. `false`

Schema della tabella mappata

Lo schema mappato ha la forma seguente.

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": STRING,
      "targetHeader": STRING,
      "type": TYPE,
      "pad": PAD
    },
    ...
  ]
```

```
}
```

In caso `headerRow` affermativo`true`, il campo successivo nell'oggetto è`columns`, che contiene una matrice di schemi di colonne che mappano le intestazioni di origine alle intestazioni di destinazione (ovvero oggetti JSON che descrivono cosa devono contenere le colonne di output).

- `sourceHeader`— Il nome dell'`STRING`intestazione della colonna di origine da cui derivano i dati.

  > **Note**
  >
  > La stessa colonna di origine può essere utilizzata per più colonne di destinazione. Una colonna del file di input non elencata in `sourceHeader` nessun punto dello schema non viene visualizzata nel file di output.

- `targetHeader`— Il nome dell'`STRING`intestazione della colonna corrispondente nel file di output.

  > **Note**
  >
  > Questo campo è facoltativo per gli schemi mappati. Se questo campo viene omesso, `sourceHeader` viene riutilizzato come nome dell'intestazione nell'output. `_sealed`Viene aggiunto `_fingerprint` o se la colonna di output è rispettivamente una colonna o una fingerprint colonna. sealed

- `type`— La colonna TYPE di destinazione nel file di output. Cioè, una delle `cleartext` due o `fingerprint` dipende da come la colonna verrà utilizzata nella collaborazione. `sealed`
- `pad`— Un campo di un oggetto dello schema a colonne che è presente solo quando TYPE è`sealed`. Il valore corrispondente di PAD è un oggetto che descrive come aggiungere i dati prima di essere crittografati.

  ```
  {
    "type": PAD_TYPE,
    "length": INT
  }
  ```

  Per specificare il padding di pre-crittografia, `type` `length` vengono utilizzati come segue:

  - `PAD_TYPE`as`none`: non verrà applicato alcun riempimento ai dati della colonna e il `length` campo non è applicabile (ovvero omesso).

- PAD_TYPEas `fixed` — I dati della colonna vengono aggiunti al numero di byte specificato`length`.
- PAD_TYPEas `max` — I dati della colonna vengono aggiunti alla dimensione della lunghezza in byte del valore più lungo più un byte aggiuntivo. `length`

Di seguito è riportato un esempio di schema mappato, con una colonna di ogni tipo.

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": "FullName",
      "targetHeader": "name",
      "type": "cleartext"
    },
    {
      "sourceHeader": "City",
      "targetHeader": "city_sealed",
      "type": "sealed",
      "pad": {
        "type": "max",
        "length": 16
      }
    },
    {
      "sourceHeader": "PhoneNumber",
      "targetHeader": "phone_number_fingerprint",
      "type": "fingerprint"
    },
    {
      "sourceHeader": "PhoneNumber",
      "targetHeader": "phone_number_sealed",
      "type": "sealed",
      "pad": {
        "type": "fixed",
        "length": 20
      }
    }
  ]
}
```

Come esempio più complesso, quello che segue è un esempio di file.csv con intestazioni.

```
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
```

Nel seguente esempio di schema mappato, le colonne e sono colonne`FirstName`. `LastName` `cleartext` La `State` colonna viene crittografata come `fingerprint` colonna e come `sealed` colonna con una spaziatura di. `none` Le colonne rimanenti vengono omesse.

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

```
}
```

Di seguito è riportato il file.csv che risulta dallo schema mappato.

```
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=
```

Schema della tabella posizionale

Lo schema posizionale ha la forma seguente.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      },
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      }
    ],
    [],
    ...
  ]
```

```
}
```

In caso `headerRow` affermativo`false`, il campo successivo nell'oggetto è`columns`, che contiene una matrice di voci. Ogni voce è a sua volta una matrice di zero o più schemi di colonne posizionali (nessun `sourceHeader` campo), che sono oggetti JSON che descrivono cosa deve contenere l'output.

- `sourceHeader`— Il nome dell'`STRING`intestazione della colonna di origine da cui derivano i dati.

  > **Note**
  >
  > Questo campo deve essere omesso negli schemi posizionali. Negli schemi posizionali, la colonna di origine viene dedotta dall'indice corrispondente della colonna nel file di schema.

- `targetHeader`— Il nome dell'`STRING`intestazione della colonna corrispondente nel file di output.

  > **Note**
  >
  > Questo campo è obbligatorio per gli schemi posizionali.

- `type`— La colonna TYPE di destinazione nel file di output. Cioè, una delle `cleartext` due o `fingerprint` dipende da come la colonna verrà utilizzata nella collaborazione. `sealed`
- `pad`— Un campo di un oggetto dello schema a colonne che è presente solo quando TYPE è`sealed`. Il valore corrispondente di PAD è un oggetto che descrive come aggiungere i dati prima di essere crittografati.

  ```
  {
    "type": PAD_TYPE,
    "length": INT
  }
  ```

  Per specificare il padding di pre-crittografia, `type` `length` vengono utilizzati come segue:

  - PAD_TYPEas`none`: non verrà applicato alcun riempimento ai dati della colonna e il `length` campo non è applicabile (ovvero omesso).
  - PAD_TYPEas `fixed` — I dati della colonna vengono aggiunti al numero di byte specificato`length`.
  - PAD_TYPEas `max` — I dati della colonna vengono aggiunti alla dimensione della lunghezza in byte del valore più lungo più un byte aggiuntivo. `length`

> **Note**
>
> `fixed`è utile se si conosce in anticipo il limite superiore della dimensione in byte dei dati della colonna. Viene generato un errore se i dati in quella colonna sono più lunghi di quelli `length` specificati.
> `max`è utile quando la dimensione esatta dei dati di input non è nota perché funziona indipendentemente dalla dimensione dei dati. Tuttavia, `max` richiede tempi di elaborazione aggiuntivi perché crittografa i dati due volte. `max`crittografa i dati una volta quando vengono letti nel file temporaneo e una volta dopo che è nota l'immissione dei dati più lunga nella colonna.
> Inoltre, la lunghezza del valore più lungo non viene salvata tra le chiamate del client. Se prevedi di crittografare i dati in batch o di crittografare periodicamente nuovi dati, tieni presente che le lunghezze del testo cifrato risultanti potrebbero variare da un batch all'altro.

Di seguito è riportato un esempio di schema posizionale.

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

Come esempio complesso, quello che segue è un esempio di file.csv se non aveva la prima riga con le intestazioni.

```
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
```

Lo schema posizionale ha la forma seguente.

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": "GivenName",
        "type": "cleartext"
      }
    ],
    [
      {
        "targetHeader": "Surname",
        "type": "cleartext"
      }
    ],
```

```
    [],
    [],
    [
      {
        "targetHeader": "State_Join",
        "type": "fingerprint"
      },
      {
        "targetHeader": "State",
        "type": "sealed",
        "pad": {
          "type": "none"
        }
      }
    ],
    [],
    [],
    [],
    []
  ]
}
```

Lo schema precedente produce il seguente file di output con una riga di intestazione contenente le intestazioni di destinazione specificate.

```
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=
```

Creazione di una tabella configurata in AWS Clean Rooms

Una tabella configurata è un riferimento a una tabella esistente in AWS Glue Data Catalog. Contiene una regola di analisi che determina in che modo i dati possono essere interrogati. AWS Clean Rooms Le tabelle configurate possono essere associate a una o più collaborazioni. Per ulteriori informazioni AWS Glue, consulta la AWS Glue Developer Guide.

Utilizza la generazione di statistiche fornita da AWS Glue per calcolare statistiche a livello di colonna per le tabelle. AWS Glue Data Catalog Una volta AWS Glue generate le statistiche per le tabelle nel catalogo dati, Amazon Redshift Spectrum utilizza automaticamente tali statistiche per ottimizzare il piano di query. Per ulteriori informazioni sull'utilizzo delle statistiche a livello di colonna AWS Glue, consulta la Guida all'utilizzo delle statistiche a livello di colonna.

Creare una tabella configurata

In questo passaggio, crei una tabella configurata AWS Clean Rooms da utilizzare nella collaborazione.

Per creare una tabella configurata in AWS Clean Rooms

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Nell'angolo in alto a destra, scegli Configura nuova tabella.
4. Per Configura nuova tabella, per Scegli AWS Glue tabella:
    a. Scegli il database che desideri configurare dall'elenco a discesa.
    b. Scegli la tabella che desideri configurare dall'elenco a discesa.

> **Note**
>
> Per verificare che questa sia la tabella corretta, esegui una delle seguenti operazioni:
>
> - Scegliete Visualizza in AWS Glue.
> - Attiva Visualizza schema per visualizzare lo schema.

5. Per Colonne consentite nelle collaborazioni, scegli Tutte le colonne o Elenco personalizzato.

Se scegli...	Quindi...
Tutte le colonne	È consentito l'uso di tutte le colonne in AWS Clean Rooms (in base alle regole di analisi).
Elenco personalizzato	Scegli una o più colonne che desideri consentire dall'elenco a discesa Specificare le colonne consentite.

6. Per i dettagli della tabella configurata,

   a. Immettere un nome per la tabella configurata.

      È possibile utilizzare il nome predefinito o rinominare questa tabella.

   b. Inserire una descrizione della tabella.

      La descrizione aiuta a distinguere tra altre tabelle configurate con nomi simili.

   c. Se desideri abilitare i tag per la risorsa della tabella configurata, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.

7. Scegli Configura nuova tabella.

Passaggi successivi

Ora che hai creato una tabella configurata, sei pronto per:

- Configurare una regola di analisi nella tabella configurata
- Associa la tabella configurata a una collaborazione

Configurazione di una regola di analisi in una tabella configurata

Le sezioni seguenti descrivono come configurare una regola di analisi nella tabella configurata. Definendo le regole di analisi, è possibile autorizzare il membro che può eseguire query a eseguire query che corrispondono a una regola di analisi specifica supportata da. AWS Clean Rooms

AWS Clean Roomssupporta i seguenti tipi di regole di analisi: aggregazione, elenco e personalizzata.

Può esserci una sola regola di analisi per tabella configurata.

> **Important**
>
> Se si utilizza Cryptographic Computing per la collaborazione Clean Rooms e la collaborazione prevede tabelle di dati crittografate, la regola di analisi aggiunta alla tabella configurata crittografata deve essere coerente con il modo in cui i dati sono stati crittografati. Ad esempio, se hai crittografato i dati per SELECT (regola di analisi di aggregazione), non dovresti aggiungere la regola di analisi per JOIN (regola di analisi dell'elenco).

Per comprendere i tipi di regole di analisi disponibili inAWS Clean Rooms, vedereRegole di analisi in AWS Clean Rooms.

Per ulteriori informazioni sulla regola di analisi di aggregazione, vedereRegola di analisi di aggregazione.

Per ulteriori informazioni sulla regola di analisi degli elenchi, vedereRegola di analisi delle liste.

Per ulteriori informazioni sulla regola di analisi personalizzata, vedereRegola di analisi personalizzata in AWS Clean Rooms.

Dopo aver esaminato e compreso queste sezioni, è possibile eseguire le seguenti procedure:

Argomenti

- Configurazione di una regola di analisi di aggregazione in una tabella (flusso guidato)
- Configurazione di una regola di analisi dell'elenco su una tabella (flusso guidato)
- Configurazione di una regola di analisi personalizzata su una tabella (flusso guidato)

Configurazione di una regola di analisi di aggregazione in una tabella (flusso guidato)

La regola di analisi di aggregazione consente di eseguire query che aggregano le statistiche senza rivelare informazioni a livello di riga utilizzando COUNT funzioni e dimensioni opzionali. SUM AVG

Questa procedura descrive il processo di aggiunta di una regola di analisi di aggregazione alla tabella configurata utilizzando l'opzione Flusso guidato nella console. AWS Clean Rooms

Per aggiungere la regola di analisi di aggregazione a una tabella (flusso guidato)

1. Accedi AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Scegli la tabella configurata.
4. Nella pagina di dettaglio della tabella configurata, scegli Configura regola di analisi.
5. Nel Passaggio 1: Scegli il tipo, in Tipo, lascia selezionata l'opzione Aggregazione per impostazione predefinita.
6. In Metodo di creazione, seleziona Flusso guidato, quindi scegli Avanti.
7. Nella Fase 2: Specificate i controlli di interrogazione, per le funzioni di aggregazione:

    a. Scegli una funzione di aggregazione dal menu a discesa:

        - CONTARE
        - CONTA DISTINTO
        - SUM
        - SOMMA DISTINTA
        - AVG

    b. Scegli quali colonne possono essere utilizzate nella funzione Aggregate dal menu a discesa Colonne.

    c. (Facoltativo) Scegli Aggiungi un'altra funzione per aggiungere un'altra funzione di aggregazione e associare una o più colonne a quella funzione.

> **Note**
>
> È richiesta almeno una funzione di aggregazione.

d. (Facoltativo) Scegliete Rimuovi per rimuovere una funzione aggregata.

8. Per i controlli Join,

a. Scegli un'opzione per Consenti alla tabella di essere interrogata da sola:

Se scegli...	Quindi...
No, è possibile interrogare solo la sovrapposizione	La tabella può essere interrogata solo se unita a una tabella di proprietà del membro che può eseguire la query.
Sì	La tabella può essere interrogata da sola o quando è unita ad altre tabelle.

b. In Specificare le colonne di unione, scegliete le colonne di cui desiderate consentire l'uso nell'INNERJOINistruzione.

Questo è facoltativo se hai selezionato Sì nel passaggio precedente.

c. In Specificare gli operatori consentiti per la corrispondenza, scegli quali operatori, se presenti, possono essere utilizzati per la corrispondenza su più colonne di unione. Se selezioni due o più JOIN colonne, è necessario uno di questi operatori.

Se scegli...	Quindi...
E	Puoi includere `AND` nelle condizioni di `INNER JOIN` partita per unire una colonna a un'altra colonna tra le tabelle.
OPPURE	Puoi includere `OR` nelle condizioni di `INNER JOIN` partita per combinare più corrispondenze di colonne tra tabelle. Questo operatore logico è utile per

Se scegli...	Quindi...
	ottenere un tasso di corrispondenza più elevato.

9. (Facoltativo) Per i controlli Dimension, nel menu a discesa Specificare le colonne di dimensione, scegli le colonne di cui desideri consentire l'utilizzo nell'istruzione SELECT e nelle ORDER BY parti della query. WHERE GROUP BY

> **Note**
>
> La funzione di aggregazione o le colonne di unione non possono essere utilizzate come colonne Dimension.

10. Per le funzioni scalari, scegli un'opzione per Quali funzioni scalari vuoi consentire?

Se scegli...	Quindi...
Il tutto attualmente supportato da AWS Clean Rooms	Sono consentite tutte le funzioni scalari attualmente supportate daAWS Clean Rooms. • Puoi scegliere Visualizza elenco per visualizzare l'intero elenco di funzioni scalari supportate in. AWS Clean Rooms
Un elenco personalizzato	È possibile personalizzare le funzioni scalari da consentire. • Scegli una o più opzioni dal menu a discesa Specificare le funzioni scalari consentite.
Nessuno	Non vuoi consentire alcuna funzione scalare.

Per ulteriori informazioni, consulta Funzioni scalari.

11. Seleziona Next (Successivo).
12. Nel Passaggio 3: Specificare i controlli dei risultati delle query, per i vincoli di aggregazione:

a. Seleziona l'elenco a discesa per ogni nome di colonna.

b. Seleziona l'elenco a discesa per ogni Numero minimo di valori distinti che devono essere soddisfatti per ogni riga di output da restituire, dopo l'applicazione della COUNT DISTINCT funzione.

c. Scegli Aggiungi vincolo per aggiungere altri vincoli di aggregazione.

d. (Facoltativo) Scegliete Rimuovi per rimuovere un vincolo di aggregazione.

13. Seleziona Avanti.
14. Nel Passaggio 4: revisione e configurazione, rivedi le selezioni effettuate per i passaggi precedenti, modifica se necessario, quindi scegli Configura regola di analisi.

Viene visualizzato un messaggio di conferma che hai configurato correttamente una regola di analisi di aggregazione nella tabella.

Configurazione di una regola di analisi dell'elenco su una tabella (flusso guidato)

La regola di analisi degli elenchi consente di eseguire query che generano elenchi a livello di riga della sovrapposizione tra la tabella associata e una tabella del membro che può eseguire l'interrogazione.

Questa procedura descrive il processo di aggiunta della regola di analisi dell'elenco alla tabella configurata utilizzando l'opzione Flusso guidato nella console. AWS Clean Rooms

Per aggiungere una regola di analisi dell'elenco a una tabella (flusso guidato)

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Scegli la tabella configurata.
4. Nella pagina di dettaglio della tabella configurata, scegli Configura regola di analisi.
5. Nel Passaggio 1: Scegli il tipo, in Tipo, scegli l'opzione Elenco.
6. In Metodo di creazione, seleziona Flusso guidato, quindi scegli Avanti.
7. Nel Passaggio 2: Specificare i controlli di interrogazione, per i controlli Join:

a. In Specificare le colonne di unione, scegliete le colonne di cui desiderate consentire l'uso nell'INNERJOINistruzione.

b. In Specificare gli operatori consentiti per la corrispondenza, scegli quali operatori, se presenti, possono essere utilizzati per la corrispondenza su più colonne di unione. Se selezioni due o più JOIN colonne, è necessario uno di questi operatori.

Se scegli...	Quindi...
E	Puoi includere `AND` nelle condizioni di `INNER JOIN` partita per unire una colonna a un'altra colonna tra le tabelle.
OPPURE	Puoi includere `OR` nelle condizioni di `INNER JOIN` partita per combinare più corrispondenze di colonne tra tabelle. Questo operatore logico è utile per ottenere un tasso di corrispondenza più elevato.

8. (Facoltativo) Per i controlli List, nel menu a discesa Specificare le colonne dell'elenco, scegliete quali colonne desiderate che vengano utilizzate nell'output della query (ovvero, utilizzate nell'SELECTistruzione) o utilizzate per filtrare i risultati (ovvero, l'WHEREistruzione).
9. Seleziona Avanti.
10. Nel Passaggio 3: revisione e configurazione, rivedi le selezioni effettuate per i passaggi precedenti, modificale se necessario, quindi scegli Configura regola di analisi.

Viene visualizzato un messaggio di conferma che è stata configurata correttamente una regola di analisi dell'elenco per la tabella.

Configurazione di una regola di analisi personalizzata su una tabella (flusso guidato)

La regola di analisi personalizzata abilita query SQL personalizzate su una tabella configurata. La regola di analisi personalizzata è necessaria se si utilizzano modelli di analisi o privacy differenziale.

Questa procedura descrive il processo di aggiunta della regola di analisi personalizzata alla tabella configurata utilizzando l'opzione Flusso guidato nella AWS Clean Rooms console.

Per aggiungere una regola di analisi personalizzata a una tabella (flusso guidato)

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Scegli la tabella configurata.
4. Nella pagina di dettaglio della tabella configurata, scegli Configura regola di analisi.
5. Nel Passaggio 1: Scegli il tipo, in Tipo, scegli l'opzione Personalizzata.
6. In Metodo di creazione, seleziona Flusso guidato, quindi scegli Avanti.
7. Nel Passaggio 2: Imposta la privacy differenziale, stabilisci se desideri attivare o disattivare la privacy differenziale. La privacy differenziale è una tecnica matematicamente collaudata per proteggere i dati dagli attacchi di reidentificazione.

    a. Per la privacy differenziale:

Se tu...	Allora scegli...
Disponi di dati a livello utente e desideri proteggerli dai tentativi di reidentificazione	Accendi
Non dispongono di dati a livello utente o non necessitano di protezione contro i tentativi di reidentificazione	Spegnere

    b. Se hai scelto di attivare la privacy differenziale, seleziona la colonna Identificatore utente che contiene l'identificatore univoco degli utenti, ad esempio la `user_id` colonna di cui desideri proteggere la privacy. Se desideri attivare la privacy differenziale per due o più tabelle in una collaborazione, devi configurare la stessa colonna della colonna User identifier in entrambe le regole di analisi per mantenere una definizione coerente degli utenti tra le tabelle. In caso di configurazione errata, il membro che può eseguire la query riceve un messaggio di errore indicante che ci sono due colonne tra cui scegliere per calcolare il numero di contributi degli utenti (ad esempio, il numero di impressioni pubblicate da un utente) durante l'esecuzione della query.

    c. Seleziona Avanti.

8. Nel passaggio 3: Specificare i controlli di interrogazione,

   a. Per il tipo di controllo:

Se vuoi ...	Quindi scegli...
Esamina ogni nuovo modello di analisi prima che venga eseguito sulla tabella configurata	Esamina ogni nuova analisi prima che possa essere eseguita su questa tabella
Consenti l'esecuzione di qualsiasi modello di analisi o interrogazione diretta sulla tabella configurata	Consenti l'esecuzione senza revisione di tutte le query create da collaboratori specifici su questa tabella

   b. Seleziona una delle seguenti opzioni:

Se hai scelto...	Quindi...
Esamina ogni nuova analisi prima di consentirne l'esecuzione su questa tabella	In Modelli di analisi consentiti, scegli Aggiungi modello di analisi, quindi scegli il modello di collaborazione e di analisi appropriato dagli elenchi a discesa.
Consenti l'esecuzione senza revisione di tutte le query create da collaboratori specifici su questa tabella	In Account AWSConsentito creare qualsiasi query, scegli Aggiungi Account AWS, quindi scegli l'ID appropriatoAccount AWS.

9. Seleziona Avanti.
10. Nel Passaggio 4: revisione e configurazione, rivedi le selezioni effettuate per i passaggi precedenti, modifica se necessario, quindi scegli Configura regola di analisi.

Viene visualizzato un messaggio di conferma che è stata configurata correttamente una regola di analisi personalizzata per la tabella.

Configurazione della regola di analisi su una tabella (editor JSON)

La procedura seguente mostra come aggiungere una regola di analisi a una tabella utilizzando l'opzione dell'editor JSON nella console. AWS Clean Rooms

Per configurare un'aggregazione, un elenco o una regola di analisi personalizzata a una tabella (editor JSON)

1. Accedi AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Scegli la tabella configurata.
4. Nella pagina di dettaglio della tabella configurata, scegli Configura regola di analisi.
5. Nel Passaggio 1: Scegli il tipo, in Tipo, scegli l'opzione Aggregazione, Elenco o Personalizzata.
6. In Metodo di creazione, seleziona Editor JSON, quindi scegli Avanti.
7. Nel Passaggio 2: Specificazione dei controlli, puoi scegliere di inserire una struttura di query (Inserisci modello) o inserire un file (Importa da file).

Se scegli...	Quindi...
Inserisci modello	1. Specificate i parametri per la regola di analisi selezionata nella definizione della regola di analisi. 2. Puoi premere Ctrl + Barra spaziatrice per abilitare il completamento automatico. Per ulteriori informazioni sui parametri delle regole di analisi di aggregazione, vedere. Regola di analisi dell'aggregazione: controlli di interrogazione Per ulteriori informazioni sui parametri delle regole di analisi degli elenchi, vedereRegola di analisi delle liste: controlli di interrogazione.

Se scegli...	Quindi...
Importazione da file	1. Seleziona il tuo file JSON dall'unità locale. 2. Seleziona Apri. La definizione della regola di analisi mostra la regola di analisi del file caricato.

8. Seleziona Avanti.
9. Nel Passaggio 3: revisione e configurazione, rivedi le selezioni effettuate per i passaggi precedenti, modifica se necessario, quindi scegli Configura regola di analisi.

Riceverai un messaggio di conferma che hai configurato correttamente una regola di analisi per la tabella.

Passaggi successivi

Ora che hai configurato una regola di analisi per la tabella configurata, sei pronto per:

- Associare una tabella configurata a una collaborazione
- Interroga le tabelle di dati (come membro che può eseguire interrogazioni)

Associazione di una tabella configurata a una collaborazione

Dopo aver creato una tabella configurata e avervi aggiunto una regola di analisi, puoi associarla a una collaborazione.

Important

Prima di associare le AWS Glue tabelle configurate alla collaborazione, la posizione della AWS Glue tabella deve puntare a una cartella Amazon Simple Storage Service (Amazon S3) e non a un singolo file. Puoi verificare questa posizione visualizzando la tabella nella AWS Glue console all'indirizzo https://console.aws.amazon.com/glue/.

Note

Se hai configurato la crittografia AWS Glue e creato un ruolo di servizio, devi concedere a quel ruolo l'accesso da utilizzare per decrittografare AWS KMS keys AWS Glue le tabelle. Se hai associato una tabella configurata supportata da un set di dati Amazon S3 AWS KMS crittografato, devi concedere al ruolo l'accesso per utilizzare la chiave KMS per decrittografare i dati di Amazon S3.
Per ulteriori informazioni, consulta Configurare la crittografia nella Guida per gli sviluppatori. AWS GlueAWS Glue

I seguenti argomenti descrivono come associare una tabella configurata a una collaborazione utilizzando la AWS Clean Rooms console:

Argomenti

Per informazioni su come associare le tabelle configurate alla collaborazione utilizzando gli AWS SDK, consulta l'AWS Clean Rooms API Reference.

Associa una tabella configurata dalla pagina di dettaglio della tabella configurata

Per associare AWS Glue tabelle alla collaborazione dalla pagina di dettaglio della tabella configurata

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Scegli la tabella configurata.
4. Nella pagina di dettaglio della tabella configurata, scegli Associa alla collaborazione.
5. Per la finestra di dialogo Associa tabella alla collaborazione, scegli Collaborazione dall'elenco a discesa.
6. Scegli Scegli la collaborazione.

   Nella pagina Associa tabella, il nome della tabella configurata che hai scelto viene visualizzato nella sezione Scegli la tabella configurata.
7. Per Scegli la tabella configurata, procedi come segue:

Se vuoi...	Quindi...
Configura una nuova tabella	Scegli Configura tabella e segui le istruzioni nella pagina Configura tabella.
Visualizza lo schema e la regola di analisi per la tabella configurata	Attiva Visualizza schema e regola di analisi.

8. Specificate le autorizzazioni di accesso al servizio selezionando Crea e utilizza un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

Se scegli...	Quindi...
Crea e usa un nuovo ruolo di servizio	• AWS Clean Rooms crea un ruolo di servizio con la politica richiesta per questa tabella. • Il nome del ruolo di servizio predefinito è `cleanrooms-<timestamp>`

Se scegli...	Quindi...
	• È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. • Se i dati di input sono crittografati, puoi selezionare Questi dati sono crittografati con una chiave KMS e quindi inserirne una AWS KMS key che verrà utilizzata per decrittografare i dati in ingresso.

Se scegli...	Quindi...
Usa un ruolo di servizio esistente	1. Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. L'elenco dei ruoli viene visualizzato se si dispone delle autorizzazioni per elencare i ruoli. Se non disponi delle autorizzazioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. 2. Visualizza il ruolo del servizio scegliendo il link esterno View in IAM. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibile. Per impostazione predefinita, AWS Clean Rooms non tenta di aggiornare la politica esistente sui ruoli per aggiungere le autorizzazioni necessarie. 3. (Facoltativo) Seleziona la casella di controllo Aggiungi una politica preconfig urata con le autorizzazioni necessarie a questo ruolo per aggiungere allegare le autorizzazioni necessarie al ruolo. È necessario disporre delle autorizzazioni per modificare i ruoli e creare politiche.

> **Note**
>
> - AWS Clean Rooms richiede le autorizzazioni per eseguire interrogazioni in base alle regole di analisi. Per ulteriori informazioni sulle autorizzazioni per AWS Clean Rooms, vedere. AWS politiche gestite per AWS Clean Rooms
> - Se il ruolo non dispone di autorizzazioni sufficienti per AWS Clean Rooms, riceverai un messaggio di errore che indica che il ruolo non dispone di autorizzazioni sufficienti per. AWS Clean Rooms La politica del ruolo deve essere aggiunta prima di procedere.
> - Se non è possibile modificare la politica del ruolo, viene visualizzato un messaggio di errore che indica che non è AWS Clean Rooms stato possibile trovare la politica per il ruolo di servizio.

9. Se desideri abilitare i tag per la risorsa di associazione tra tabelle configurata, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.
10. Scegli Associa tabella.

Associa una tabella configurata dalla pagina dei dettagli della collaborazione

Per associare AWS Glue tabelle alla collaborazione dalla pagina dei dettagli della collaborazione

1. Accedi AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Nella scheda Tabelle, scegli Associa tabella.
5. Per Scegli la tabella configurata, procedi come segue:

Se vuoi...	Quindi...
Scegli una tabella configurata esistente	Scegli il nome della tabella configurata che desideri associare alla collaborazione dall'elenco a discesa.
Configura una nuova tabella	Scegli Configura tabella e segui le istruzioni nella pagina Configura tabella.
Visualizza lo schema e la regola di analisi per la tabella configurata	Attiva Visualizza schema e regola di analisi.

6. Per i dettagli sull'associazione delle tabelle,

   a. Immettete un nome per la tabella associata.

      È possibile utilizzare il nome predefinito o rinominare questa tabella.

   b. (Facoltativo) Inserire una descrizione della tabella.

      La descrizione aiuta a scrivere domande.

7. Specificate le autorizzazioni di accesso al servizio selezionando Crea e utilizza un nuovo ruolo di servizio o Usa un ruolo di servizio esistente.

Se scegli...	Quindi...
Crea e usa un nuovo ruolo di servizio	• AWS Clean Rooms crea un ruolo di servizio con la politica richiesta per questa tabella. • Il nome del ruolo di servizio predefinito è`cleanrooms-<timestamp>` . • È necessario disporre delle autorizzazioni per creare ruoli e allegare politiche. • Se i dati di input sono crittografati, puoi selezionare Questi dati sono crittografati con una chiave KMS e quindi inserirne

Se scegli...	Quindi...
	una AWS KMS key che verrà utilizzata per decrittografare i dati in ingresso.
Usa un ruolo di servizio esistente	1. Scegli il nome di un ruolo di servizio esistente dall'elenco a discesa. L'elenco dei ruoli viene visualizzato se si dispone delle autorizzazioni per elencare i ruoli. Se non disponi delle autorizzazioni per elencare i ruoli, puoi inserire l'Amazon Resource Name (ARN) del ruolo che desideri utilizzare. 2. Visualizza il ruolo del servizio scegliendo il link esterno View in IAM. Se non ci sono ruoli di servizio esistenti, l'opzione Usa un ruolo di servizio esistente non è disponibile. Per impostazione predefinita, AWS Clean Rooms non tenta di aggiornare la politica esistente sui ruoli per aggiungere le autorizzazioni necessarie. 3. (Facoltativo) Seleziona la casella di controllo Aggiungi una politica preconfig urata con le autorizzazioni necessarie a questo ruolo per aggiungere allegare le autorizzazioni necessarie al ruolo. È necessario disporre delle autorizzazioni per modificare i ruoli e creare politiche.

> **Note**
>
> - AWS Clean Rooms richiede le autorizzazioni per eseguire interrogazioni in base alle regole di analisi. Per ulteriori informazioni sulle autorizzazioni per AWS Clean Rooms, vedere. AWS politiche gestite per AWS Clean Rooms
> - Se il ruolo non dispone di autorizzazioni sufficienti per AWS Clean Rooms, riceverai un messaggio di errore che indica che il ruolo non dispone di autorizzazioni sufficienti per. AWS Clean Rooms La politica del ruolo deve essere aggiunta prima di procedere.
> - Se non è possibile modificare la politica del ruolo, viene visualizzato un messaggio di errore che indica che non è AWS Clean Rooms stato possibile trovare la politica per il ruolo di servizio.

8. Se desideri abilitare i tag per la risorsa di associazione tra tabelle configurata, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.
9. Scegli Associa tabella.

Passaggi successivi

Ora che hai associato la tabella di dati configurata alla collaborazione, sei pronto per:

- Modifica la collaborazione, se sei il creatore della collaborazione
- Interroga le tabelle di dati (come membro che può eseguire interrogazioni)

Configurazione dell'informativa sulla privacy differenziale

Questa procedura descrive il processo di configurazione dell'informativa sulla privacy differenziale in una collaborazione utilizzando l'opzione Flusso guidato nella console. AWS Clean Rooms Si tratta di un passaggio unico per tutte le tabelle con protezione differenziale della privacy.

Per configurare le impostazioni di privacy differenziali (flusso guidato)

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Nella scheda Tabelle della pagina di collaborazione, scegli Configura l'informativa sulla privacy differenziale.
5. Nella pagina Configura l'informativa sulla privacy differenziale, scegli i valori per le seguenti proprietà:

   - Budget per la privacy
   - Aggiorna mensilmente il budget per la privacy
   - Rumore aggiunto per ogni query

   Puoi utilizzare i valori predefiniti o inserire valori personalizzati che supportano il tuo caso d'uso specifico. Dopo aver scelto i valori per Privacy budget e Noise aggiunti per query, puoi visualizzare in anteprima l'utilità risultante in termini di numero di aggregazioni possibili tra tutte le query sui tuoi dati.
6. Scegli Configura.

Vedrai un messaggio di conferma che hai configurato correttamente l'informativa sulla privacy differenziale per la collaborazione.

Passaggi successivi

Ora che hai configurato la privacy differenziale, sei pronto per:

- Interroga le tabelle di dati (come membro che può eseguire interrogazioni)

- Gestisci la collaborazione (se sei il creatore della collaborazione)

Utilizzo dei modelli di analisi

I modelli di analisi funzionano conRegola di analisi personalizzata in AWS Clean Rooms. Con un modello di analisi, puoi definire parametri per aiutarti a riutilizzare la stessa interrogazione. AWS Clean Rooms supporta un sottoinsieme di parametrizzazione con valori letterali.

I modelli di analisi sono specifici per la collaborazione. Per ogni collaborazione, i membri possono vedere solo le domande relative a quella collaborazione. Se si prevede di utilizzare la privacy differenziale in una collaborazione, è necessario assicurarsi che i modelli di analisi siano compatibili con la struttura di query generica di Differential Privacy. AWS Clean Rooms

Argomenti

- Creazione di un modello di analisi
- Revisione di un modello di analisi
- Interrogazione di tabelle configurate utilizzando un modello di analisi

Creazione di un modello di analisi

Per informazioni su come creare un modello di analisi utilizzando gli AWS SDK, consulta l'AWS Clean Rooms API Reference.

Per creare un modello di analisi utilizzando la console AWS Clean Rooms

1. Accedi AWS Management Console e apri la AWS Clean Rooms console con il programma Account AWS che fungerà da creatore della collaborazione.
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Nella scheda Modelli, vai alla sezione Modelli di analisi creati da te.
5. Scegli Crea modello di analisi.
6. Nella pagina Crea modello di analisi, in Dettagli, inserisci un nome e una descrizione facoltativa.
7. Per Tabelle, visualizza le tabelle configurate associate alla collaborazione.
8. Per definizione,
    a. Immettete la definizione per il modello di analisi.
    b. Scegliete Importa da per importare una definizione.

c. (Facoltativo) Specificate un parametro nell'editor SQL inserendo i due punti (`:`) davanti al nome del parametro.

   Per esempio:

   ```
   WHERE table1.date + :date_period > table1.date
   ```

9. Se avete aggiunto dei parametri in precedenza, in Parametri - opzionale, per ogni nome di parametro, scegliete il tipo e il valore predefinito (opzionale).
10. Se desideri abilitare i tag per la risorsa della tabella configurata, scegli Aggiungi nuovo tag e inserisci la coppia Chiave e Valore.
11. Scegli Crea.

Ora sei pronto per:

- Informa il tuo collaboratore che può esaminare un modello di analisi. (Facoltativo se desideri interrogare i tuoi dati).

Revisione di un modello di analisi

Dopo che un membro della collaborazione ha creato un modello di analisi, puoi esaminarlo e approvarlo. Dopo che il modello di analisi è stato approvato, può inserire una query in AWS Clean Rooms.

Per rivedere un modello di analisi utilizzando la AWS Clean Rooms console

1. Accedi AWS Management Console e apri la AWS Clean Rooms console con il programma Account AWS che fungerà da creatore della collaborazione.
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Nella scheda Modelli, vai alla sezione Modelli di analisi creati da altri membri.
5. La scelta del modello di analisi con lo stato Può essere eseguito su No richiede la tua revisione.
6. Scegli Rivedi.
7. Esamina la panoramica, la definizione e i parametri della regola di analisi (se presenti).
8. Esamina le tabelle configurate elencate in Tabelle a cui si fa riferimento nella definizione.

   Lo stato accanto a ciascuna tabella riporterà la dicitura Modello non consentito.

9. Scegliere una tabella .

Se tu	Quindi scegli
Approva il modello di analisi	modello sulla tabella. Conferma la tua approvazione scegliendo.
Non approvare il modello di analisi	Non consentire

Ora sei pronto per utilizzare il modello di analisi per interrogare le tabelle di dati (come membro che può eseguire query).

Interrogazione di tabelle configurate utilizzando un modello di analisi

Questa procedura dimostra come utilizzare un modello di analisi nella AWS Clean Rooms console per interrogare le tabelle configurate con la regola di analisi personalizzata.

Per utilizzare un modello di analisi per interrogare tabelle configurate con la regola di analisi personalizzata

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione con lo status di Query relativo alle abilità dei membri.
4. Nella scheda Query, in Tabelle, visualizza le tabelle e il tipo di regola di analisi associato (Regola di analisi personalizzata).

> **Note**
>
> Se non vedi le tabelle che ti aspetti nell'elenco, potrebbe essere per i seguenti motivi:
>
> - Le tabelle non sono state associate.
> - Le tabelle non hanno una regola di analisi configurata.

5. Nella sezione Analisi, seleziona il modello di analisi dall'elenco a discesa.

6. Immettete il valore dei parametri dal modello di analisi che desiderate utilizzare nella query. Il valore deve essere nel tipo di dati specificato dal parametro. È possibile utilizzare valori diversi ogni volta che si esegue il modello di analisi. NULLI valori vuoti o per il parametro non sono supportati. Inoltre, l'utilizzo dei parametri nella LIMIT clausola non è supportato.
7. Seleziona Esegui.

> **Note**
>
> Non è possibile eseguire la query se il membro che può ricevere i risultati non ha configurato le impostazioni dei risultati della query.

8. Continua a modificare i parametri ed esegui nuovamente la query oppure scegli il pulsante + per iniziare una nuova query in una nuova scheda.

Interrogazione dei dati in una collaborazione

In qualità di membro che può eseguire le interrogazioni, puoi eseguire una delle seguenti operazioni:

- Crea manualmente una query SQL utilizzando l'editor di codice SQL.
- Utilizza l'interfaccia utente di Analysis Builder per creare una query senza dover scrivere codice SQL.
- Utilizza un modello di analisi approvato.

Quando il membro che può eseguire una query SQL sulle tabelle della collaborazione, AWS Clean Rooms assume i ruoli pertinenti per accedere alle tabelle per suo conto. AWS Clean Rooms applica le regole di analisi necessarie alla query di input e al relativo output.

AWS Clean Rooms supporta query SQL che possono essere diverse dagli altri motori di query. Per le specifiche, vedere AWS Clean Rooms SQL Reference. Se desideri eseguire query su tabelle di dati protette con privacy differenziale, devi assicurarti che le query siano compatibili con la struttura di query generica di Differential Privacy. AWS Clean Rooms

> **Note**
>
> Quando si utilizza Cryptographic Computing for Clean Rooms, non tutte le operazioni SQL generano risultati validi. Ad esempio, è possibile eseguire un comando COUNT su una colonna crittografata, ma eseguire un comando SUM su numeri crittografati genera errori. Inoltre, le interrogazioni potrebbero produrre risultati errati. Ad esempio, le interrogazioni con colonne SUM sigillate producono errori. Tuttavia, un'GROUPBYinterrogazione su colonne sigillate sembra avere esito positivo, ma produce gruppi diversi da quelli prodotti da un'GROUPBYinterrogazione su testo in chiaro.

I seguenti argomenti spiegano come interrogare i dati in una collaborazione utilizzando la AWS Clean Rooms console.

Argomenti

- Utilizzo dell'editor di codice SQL
- Utilizzo del generatore di analisi
- Interrogazione dei dati con privacy differenziale

- Visualizzazione delle query recenti
- Visualizzazione dei dettagli delle query

Per informazioni su come interrogare i dati o visualizzare le query chiamando direttamente l'operazione AWS Clean Rooms `StartProtectedQuery` API o utilizzando gli AWS SDK, consulta l'AWS Clean Rooms API Reference.

Per informazioni sulla registrazione delle query, consulta. Registrazione delle query AWS Clean Rooms

> **Note**
>
> Se si esegue una query su tabelle di dati crittografate, i risultati delle colonne crittografate vengono crittografati.

Per informazioni sulla ricezione dei risultati delle query, vedereRicezione dei risultati delle query.

Utilizzo dell'editor di codice SQL

In qualità di membro in grado di eseguire query, puoi creare una query manualmente scrivendo codice SQL nell'editor di codice SQL. L'editor di codice SQL si trova nella sezione Analisi della scheda Query della AWS Clean Rooms console.

L'editor di codice SQL viene visualizzato per impostazione predefinita. Se desideri utilizzare il generatore di analisi per creare query, consulta. Utilizzo del generatore di analisi

> **Important**
>
> Se inizi a scrivere una query SQL nell'editor di codice e poi attivi l'interfaccia utente di Analysis Builder, la query non viene salvata.

AWS Clean Rooms supporta molti comandi, funzioni e condizioni SQL. Per ulteriori informazioni, vedere AWS Clean Rooms SQL Reference.

> **Tip**
>
> Se viene eseguita una manutenzione pianificata mentre è in esecuzione una query, la query viene terminata e ripristinata. È necessario riavviare la query.

Per creare la query manualmente utilizzando l'editor di codice SQL

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione con lo status di Query relativo alle abilità dei membri.
4. Nella scheda Interrogazioni, vai alla sezione Analisi.

   > **Note**
   >
   > La sezione Analisi viene visualizzata solo se il membro che può ricevere i risultati e il membro responsabile del pagamento dei costi di elaborazione delle query hanno aderito alla collaborazione come membri attivi.

5. Nella scheda Interrogazioni, in Tabelle, visualizza l'elenco delle tabelle e il tipo di regola di analisi associato (regola di analisi di aggregazione, regola di analisi dell'elenco o regola di analisi personalizzata).

   > **Note**
   >
   > Se non vedi le tabelle che ti aspetti nell'elenco, potrebbe essere per i seguenti motivi:
   >
   > - Le tabelle non sono state associate.
   > - Le tabelle non hanno una regola di analisi configurata.

6. (Facoltativo) Per visualizzare lo schema e i controlli delle regole di analisi della tabella, espandi la tabella selezionando l'icona del segno più (+).
7. Crea la query digitandola nell'editor di codice SQL.

(Facoltativo) Se desideri utilizzare una query di esempio	(Facoltativo) Se si desidera inserire nomi o funzioni di colonna
1. Seleziona i tre punti verticali accanto alla tabella. 2. In Inserisci nell'editor, scegli Interrogazione di esempio. **Note** L'inserimento di una query di esempio aggiunge la query già presente nell'editor. Viene visualizzato l'esempio di interrogazione. Tutte le tabelle elencate in Tabelle sono incluse nella query. 3. Modificate i valori segnaposto nella query.	1. Seleziona i tre punti verticali accanto a una colonna. 2. In Inserisci nell'editor, scegli Nome colonna. 3. Per inserire manualmente una funzione consentita su una colonna, seleziona i tre punti verticali accanto a una colonna, seleziona Inserisci nell'editor, quindi seleziona il nome della funzione consentita (ad esempio INNER JOIN SUMDISTINCT, SUM oCOUNT). 4. Premi Ctrl + Spazio per visualizzare gli schemi delle tabelle nell'editor di codice. **Note** I membri che possono eseguire query possono visualizzare e utilizzare le colonne delle partizioni in ogni associazione di tabelle configurata. Assicurati che la colonna della partizione sia etichettata come colonna di partizione nella AWS Glue tabella sottostante la tabella configurata.

(Facoltativo) Se desideri utilizzare una query di esempio	(Facoltativo) Se si desidera inserire nomi o funzioni di colonna
	5. Modifica i valori segnaposto nella query.

8. Seleziona Esegui.

> **Note**
>
> Non è possibile eseguire la query se il membro che può ricevere i risultati non ha configurato le impostazioni dei risultati della query.

9. Continua a modificare i parametri ed esegui nuovamente la query oppure scegli il pulsante + per iniziare una nuova query in una nuova scheda.

> **Note**
>
> AWS Clean Rooms mira a fornire messaggi di errore chiari. Se un messaggio di errore non contiene dettagli sufficienti per aiutarti a risolvere il problema, contatta il team dell'account. Fornisci loro una descrizione di come si è verificato l'errore e il messaggio di errore (inclusi eventuali identificatori). Per ulteriori informazioni, consulta Risoluzione dei problemi AWS Clean Rooms.

Utilizzo del generatore di analisi

È possibile utilizzare il generatore di analisi per creare query senza dover scrivere codice SQL. Con Analysis Builder, puoi creare una query per una collaborazione che abbia:

- Una singola tabella che utilizza la regola di analisi di aggregazione senza che sia richiesto JOIN
- Due tabelle (una per ogni membro) che utilizzano entrambe la regola di analisi di aggregazione
- Due tabelle (una per ogni membro) che utilizzano entrambe la regola di analisi delle liste
- Due tabelle (una per ciascun membro) che utilizzano entrambe la regola di analisi di aggregazione e due tabelle (una per ciascun membro) che utilizzano entrambe la regola di analisi dell'elenco

Se desideri scrivere manualmente le query SQL, consulta. Utilizzo dell'editor di codice SQL

Analysis Builder viene visualizzato come opzione dell'interfaccia utente di Analysis Builder nella sezione Analisi della scheda Queries della console. AWS Clean Rooms

> **Important**
>
> Se attivi l'interfaccia utente di Analysis Builder, inizi a creare una query in Analysis Builder e poi disattivi l'interfaccia utente di Analysis Builder, la query non viene salvata.

> **Tip**
>
> Se viene eseguita una manutenzione pianificata mentre una query è in esecuzione, la query viene terminata e ripristinata. È necessario riavviare la query.

I seguenti argomenti spiegano come utilizzare l'Analysis Builder.

Argomenti

- Utilizzate il generatore di analisi per interrogare una singola tabella (aggregazione)
- Utilizza il generatore di analisi per interrogare due tabelle (aggregazione o elenco)

Utilizzate il generatore di analisi per interrogare una singola tabella (aggregazione)

Questa procedura dimostra come utilizzare l'interfaccia utente di Analysis Builder nella AWS Clean Rooms console per creare una query. La query è per una collaborazione che ha una singola tabella che utilizza la regola di analisi di aggregazione senza necessità. JOIN

Per utilizzare il generatore di analisi per interrogare una singola tabella

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione con lo status di Query relativo alle abilità dei membri.
4. Nella scheda Query, in Tabelle, visualizza la tabella e il tipo di regola di analisi associato. (Il tipo di regola di analisi deve essere la regola di analisi di aggregazione.)

> **Note**
>
> Se non vedi la tabella che ti aspetti, potrebbe essere per i seguenti motivi:
>
> - La tabella non è stata associata.
> - La tabella non ha una regola di analisi configurata.

5. Nella sezione Analisi, attiva l'interfaccia utente di Analysis Builder.
6. Crea una query.

   Se desideri visualizzare tutte le metriche di aggregazione, vai al passaggio 9.

   a. Per Scegli le metriche, esamina le metriche aggregate che sono state preselezionate per impostazione predefinita e rimuovi qualsiasi metrica, se necessario.

   b. (Facoltativo) Per Aggiungi segmenti: facoltativo, scegli uno o più parametri.

   > **Note**
   >
   > Aggiungi segmenti: l'opzione opzionale viene visualizzata solo se sono specificate le dimensioni per la tabella.

   c. (Facoltativo) Per Aggiungi filtri: facoltativo, scegliete Aggiungi filtro, quindi scegliete un parametro, un operatore e un valore.

   Per aggiungere altri filtri, scegli Aggiungi un altro filtro.

   Per rimuovere un filtro, scegli Rimuovi.

   > **Note**
   >
   > ORDER BYnon è supportato per le query di aggregazione.
   > Nei filtri è supportato solo AND l'operatore.

   d. (Facoltativo) Per Aggiungi descrizione: facoltativo, inserisci una descrizione per identificare l'interrogazione nell'elenco delle interrogazioni.

7. Espandi il codice SQL di anteprima.

   a. Visualizzate il codice SQL generato dall'Analysis Builder.

b. Per copiare il codice SQL, scegliete Copia.

c. Per modificare il codice SQL, scegli Modifica nell'editor di codice SQL.

8. Seleziona Esegui.

> **Note**
>
> Non puoi eseguire la query se il membro che può ricevere i risultati non ha configurato le impostazioni dei risultati della query.

9. Continua a modificare i parametri ed esegui nuovamente la query oppure scegli il pulsante + per iniziare una nuova query in una nuova scheda.

> **Note**
>
> AWS Clean Rooms mira a fornire messaggi di errore chiari. Se un messaggio di errore non contiene dettagli sufficienti per aiutarti a risolvere il problema, contatta il team dell'account. Fornisci loro una descrizione di come si è verificato l'errore e il messaggio di errore (inclusi eventuali identificatori). Per ulteriori informazioni, consulta Risoluzione dei problemi AWS Clean Rooms.

Utilizza il generatore di analisi per interrogare due tabelle (aggregazione o elenco)

Questa procedura descrive come utilizzare l'Analysis Builder nella AWS Clean Rooms console per creare una query per una collaborazione che abbia:

- Due tabelle (una per ogni membro) che utilizzano entrambe la regola di analisi di aggregazione
- Due tabelle (una per ogni membro) che utilizzano entrambe la regola di analisi delle liste
- Due tabelle (una per ciascun membro) che utilizzano entrambe la regola di analisi di aggregazione e due tabelle (una per ciascun membro) che utilizzano entrambe la regola di analisi dell'elenco

Per utilizzare il generatore di analisi per interrogare due tabelle

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).

2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione per la quale le abilità dei tuoi membri sono impostate sullo stato Query.
4. Nella scheda Query, in Tabelle, visualizza le due tabelle e il tipo di regola di analisi associato (regola di analisi di aggregazione o regola di analisi dell'elenco).

> **Note**
>
> Se non vedi le tabelle che ti aspetti nell'elenco, potrebbe essere per i seguenti motivi:
>
> - Le tabelle non sono state associate.
> - Le tabelle non hanno una regola di analisi configurata.

5. Nella sezione Analisi, attiva l'interfaccia utente di Analysis Builder.
6. Crea una query.

Se la collaborazione contiene due tabelle che utilizzano la regola di analisi di aggregazione e due tabelle che utilizzano la regola di analisi delle liste, scegli prima Aggregazione o Elenco, quindi segui le istruzioni in base alla regola di analisi selezionata.

Se le due tabelle utilizzano la regola di analisi di aggregazione	Se le due tabelle utilizzano la regola di analisi dell'elenco
1. Per Choose metrics, esamina le metriche aggregate che sono state preselezionate per impostazione predefinita e rimuovi qualsiasi metrica, se necessario. 2. Per i record Match, scegli uno o più record. **Note** Quando si utilizza il generatore di analisi, è possibile eseguire la corrispondenza solo su	1. Per Scegli gli attributi, esamina gli attributi dell'elenco che sono stati preselezionati per impostazione predefinita e rimuovi qualsiasi metrica, se necessario. 2. Per i record Match, scegli uno o più record. **Note** Quando si utilizza il generatore di analisi, è possibile eseguire la corrispondenza solo su

Se le due tabelle utilizzano la regola di analisi di aggregazione	Se le due tabelle utilizzano la regola di analisi dell'elenco
una singola coppia di colonne.	una singola coppia di colonne.
3. (Facoltativo) Per Aggiungi segmenti: facoltativo, scegli uno o più parametri. **Note** Aggiungi segmenti: l'opzione opzionale viene visualizzata solo se sono specificate le dimensioni per la tabella.	3. (Facoltativo) Per Aggiungi filtri: facoltativo, scegli Aggiungi filtro, quindi scegli un parametro, un operatore e un valore. Per aggiungere altri filtri, scegli Aggiungi un altro filtro. Per rimuovere un filtro, scegli Rimuovi. **Note** LIMITnon è supportato per le interrogazioni sugli elenchi. Nei filtri è supportato solo AND l'operatore.
4. (Facoltativo) Per Aggiungi filtri: facoltativo, scegli Aggiungi filtro, quindi scegli un parametro, un operatore e un valore. Per aggiungere altri filtri, scegli Aggiungi un altro filtro. Per rimuovere un filtro, scegli Rimuovi. **Note** ORDER BYnon è supportato per le query di aggregazione. Nei filtri è supportato solo AND l'operatore.	4. (Facoltativo) Per Aggiungi descrizione: facoltativo, inserisci una descrizione per identificare l'interrogazione nell'elenco delle interrogazioni recenti.

Se le due tabelle utilizzano la regola di analisi di aggregazione	Se le due tabelle utilizzano la regola di analisi dell'elenco
5. (Facoltativo) Per Aggiungi descrizione: facoltativo, inserisci una descrizione per identificare l'interrogazione nell'elenco delle interrogazioni recenti.	

7. Espandi il codice SQL di anteprima.

   a. Visualizzate il codice SQL generato dall'Analysis Builder.

   b. Per copiare il codice SQL, scegliete Copia.

   c. Per modificare il codice SQL, scegli Modifica nell'editor di codice SQL.

8. Seleziona Esegui.

> **Note**
>
> Non puoi eseguire la query se il membro che può ricevere i risultati non ha configurato le impostazioni dei risultati della query

9. Continua a modificare i parametri ed esegui nuovamente la query oppure scegli il pulsante + per iniziare una nuova query in una nuova scheda.

> **Note**
>
> AWS Clean Rooms mira a fornire messaggi di errore chiari. Se un messaggio di errore non contiene dettagli sufficienti per aiutarti a risolvere il problema, contatta il team dell'account. Fornisci loro una descrizione di come si è verificato l'errore e il messaggio di errore (inclusi eventuali identificatori). Per ulteriori informazioni, consulta Risoluzione dei problemi AWS Clean Rooms.

Interrogazione dei dati con privacy differenziale

In generale, la scrittura e l'esecuzione di query non cambiano quando è attivata la privacy differenziale. Tuttavia, non è possibile eseguire una query se il budget a disposizione per la privacy non è sufficiente. Man mano che esegui le query e utilizzi il budget per la privacy, puoi vedere approssimativamente quante aggregazioni puoi eseguire e in che modo ciò potrebbe influire sulle query future.

Per visualizzare l'impatto della privacy differenziale in una collaborazione

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione per la quale i dati del tuo socio sono impostati sullo stato Esegui interrogazioni.
4. Nella scheda Query, in Tabelle, visualizza il budget residuo per la privacy. Viene visualizzato come il numero stimato di funzioni di aggregazione rimanenti e l'utilità utilizzata (visualizzata come percentuale).

   > **Note**
   >
   > Il numero stimato di funzioni aggregate rimanenti e la percentuale di Utility utilizzata vengono visualizzati solo per il membro che può eseguire la query.

5. Scegliete Visualizza impatto per visualizzare la quantità di rumore iniettata nei risultati e approssimativamente quante funzioni di aggregazione è possibile eseguire.

Visualizzazione delle query recenti

Puoi visualizzare le interrogazioni eseguite negli ultimi 90 giorni nella scheda Interrogazioni recenti.

> **Note**
>
> Se la tua unica abilità di membro è Contribute data e non sei il membro che paga i costi di elaborazione delle query, la scheda Interrogazioni non viene visualizzata sulla console.

Per visualizzare le interrogazioni recenti

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli una collaborazione.
4. Nella scheda Interrogazioni, in Interrogazioni, visualizza le interrogazioni eseguite negli ultimi 90 giorni.
5. Per ordinare le interrogazioni recenti in base allo stato, seleziona uno stato dall'elenco a discesa Tutti gli stati.

   Gli stati sono: Inviato, Avviato, Annullato, Operato correttamente, Non riuscito e Scaduto.

Visualizzazione dei dettagli delle query

È possibile visualizzare i dettagli della query come membro che può eseguire le query o come membro che può ricevere risultati.

Per visualizzare i dettagli dell'interrogazione

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli una collaborazione.
4. Nella scheda Interrogazioni, esegui una delle seguenti operazioni:
   - Scegli il pulsante di opzione per la query specifica che desideri visualizzare, quindi scegli Visualizza dettagli.
   - Scegli l'ID della query protetta.
5. Nella pagina dei dettagli della query,
   - Se sei il membro che può eseguire le query, visualizza i dettagli della query, il testo SQL e i risultati.

     Viene visualizzato un messaggio che conferma che i risultati della query sono stati consegnati al membro che può riceverli.

- Se sei il membro che può ricevere i risultati, visualizza i dettagli della query e i risultati.

Ricezione dei risultati delle query

Comemembro che può ricevere risultati, puoi ricevere l'output della query daAWS Clean Roomsnel bucket Amazon S3 specificato quando hai specificato quando hai specificato all'attivazione della collaborazione.

Nei seguenti argomenti viene specificato come ricevere i risultati delle query utilizzandoAWS Clean Roomsconsole.

Argomenti

- Ricevi i risultati delle query
- Modifica i valori predefiniti per le impostazioni dei risultati delle query
- Utilizzo dell'output delle query in altroServizi AWS

Per informazioni su come interrogare i dati o visualizzare le interrogazioni chiamando ilAWS Clean RoomsAPI direttamente o utilizzando ilAWSSDK, vedi iAWS Clean RoomsRiferimento API.

Per informazioni sulla registrazione delle query, consultareRegistrazione delle query AWS Clean Rooms.

> **Note**
>
> Se si esegue una query su tabelle di dati crittografate, i risultati delle colonne crittografate vengono crittografati.

Ricevi i risultati delle query

I risultati dell'interrogazione si trovano nellaImpostazioni predefinite dei risultati della querysezione e laInterrogazionisezione dellaInterrogazionischeda nellaAWS Clean Roomsconsole.

Per visualizzare i risultati delle query

1. Accedi allaAWS Management Consolee apri ilAWS Clean Roomsplanciacon il tuoAccount AWS(se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegliCollaborazioni.
3. Scegli la collaborazione che haLe abilità dei tuoi membristato diRicevi risultati.

4. Per ricevere i risultati dell'interrogazione direttamente daAWS Clean Rooms, sulInterrogazionitab, sottoInterrogazioni, sotto ilID di interrogazione protettocolonna, seleziona la query.
5. SulDettagli dell'interrogazionepagina, sottorisultati, esegui una delle seguenti operazioni:

Se vuoi...	Allora scegli...
Copia i risultati.	Copia
Scarica i risultati.	Scarica **Note** Per impostazione predefini ta, il nome del file scaricato è il corrispondente`Query id`che è stato visualizzato quando la query è stata eseguita inAWS Clean Rooms.
Visualizza i risultati in Amazon S3.	Visualizza in Amazon S3 La console Amazon S3 si apre in una scheda separata.

6. Se stai utilizzando dati crittografati, ora puoidecifrarele tabelle di dati.

   Per ulteriori informazioni, consulta Decrittografia delle tabelle di dati con il client di crittografia C3R.

Modifica i valori predefiniti per le impostazioni dei risultati delle query

In qualità di membro che può ricevere risultati, è possibile modificare i valori predefiniti per le impostazioni dei risultati delle query nelAWS Clean Roomsconsole.

Per modificare i valori predefiniti per le impostazioni dei risultati delle query

1. Accedi allaAWS Management Consolee apri ilAWS Clean Roomsplanciacon il tuoAccount AWS(se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegliCollaborazioni.
3. Scegli la collaborazione che haLe abilità dei tuoi membristato diRicevi risultati.
4. SulInterrogazionitab, sottoImpostazioni dei risultati della query, scegliModifica.
5. SulModifica le impostazioni predefinite dei risultati delle interrogazionipagina, modifica uno dei seguenti elementi, se necessario:

   a. SottoImpostazioni dei risultati della query, modificare iDestinazione dei risultati in Amazon S3oFormato dei risultati.

   b. SottoAccesso ai servizi, modificare iMetodo di autorizzazioneAWS Clean Roomsper scrivere nel bucket Amazon S3 e nel formato che hai specificato.

   L'aggiornatoImpostazioni dei risultati della queryappaiono nella pagina dei dettagli della collaborazione.

Utilizzo dell'output delle query in altroServizi AWS

Output della query daAWS Clean Roomsè disponibile sulla console (se la console viene utilizzata per eseguire query) e scaricato in un bucket Amazon S3 specificato. Da lì, puoi utilizzare l'output della query in altriServizi AWS, come Amazon QuickSight e Amazon SageMaker, a seconda di come questi servizi utilizzano i dati di Amazon S3.

Per ulteriori informazioni su Amazon QuickSight, vedi iAmazon QuickSightDocumentazione.

Per ulteriori informazioni su Amazon SageMaker, vedi iAmazon SageMakerDocumentazione.

Decrittografia delle tabelle di dati con il client di crittografia C3R

Segui questa procedura per le collaborazioni che utilizzano Cryptographic Computing forClean Roomse il client di crittografia C3R per crittografare le tabelle di dati. Utilizzate questa procedura dopo averdati interrogati nella collaborazione.

La chiave segreta condivisa e l'ID di collaborazione sono necessari per questa procedura.

Il membro che può ricevere i risultati decripta i dati utilizzando la stessa chiave segreta condivisa e lo stesso ID di collaborazione utilizzati per crittografare i dati per la collaborazione.

> **Note**
>
> AWS Clean Roomsle collaborazioni limitano già chi può eseguire e visualizzare i risultati delle query. Per eseguire la decrittografia, chiunque abbia accesso a questi risultati necessita della stessa chiave segreta condivisa e dello stesso ID di collaborazione utilizzati per crittografare i dati.

Per decrittografare una tabella di dati crittografata

1. (Facoltativo)Visualizza i comandi disponibili nel client di crittografia C3R.
2. (Facoltativo) Vai alla directory desiderata ed esegui`ls`(macOS) `odir`(Windows).
   - Verifica che ilc3r-cli.jaril file e il file di dati crittografati dei risultati delle query si trovano nella directory desiderata.

     > **Note**
     >
     > Se i risultati della query vengono scaricati dalAWS Clean Roomsinterfaccia della console, probabilmente si trovano inDownloadcartella del tuo account utente. (Ad esempio, ilDownloadcartella nella tua directory utente suWindowsemacOS). Si consiglia di spostare il file dei risultati della query nella stessa cartella delc3r-cli.jar.
3. Memorizza la chiave segreta condivisa nel`C3R_SHARED_SECRET`variabile d'ambiente. Per ulteriori informazioni, consulta Passaggio 6: memorizza la chiave segreta condivisa in una variabile di ambiente.

4. DalAWS Command Line Interface(AWS CLI), esegui il comando seguente.

   java -jar c3r-cli.jar decrypt ***<name of input .csv file>*** --id=***<collaboration id>*** --output=***<output file name>***

5. Sostituisci ciascuno*segnaposto di input dell'utente*con le tue informazioni:

   a. Per`id=`, inserisci l'ID di collaborazione.

   b. Per`output=`, specifichi il nome del file di output (ad esempio`results-decrypted.csv`).

      Se non specifichi il nome dell'output, viene visualizzato il nome di default nel terminale.

   c. Visualizza i dati decrittografati nel file di output specificato utilizzando il tuo file CSV preferito oParquetapplicazione di visualizzazione (ad esempioMicrosoft Excel, un editor di testo o un'altra applicazione).

Gestire AWS Clean Rooms

I seguenti argomenti descrivono come gestire una collaborazione, i membri e le tabelle configurate AWS Clean Rooms utilizzando la AWS Clean Rooms console.

Per informazioni su come gestire l' AWS Clean Rooms utilizzo degli AWS SDK, consulta l'AWS Clean Rooms API Reference.

Argomenti

Gestione delle collaborazioni in AWS Clean Rooms

I seguenti argomenti descrivono come il creatore della collaborazione può gestire una collaborazione AWS Clean Rooms utilizzando la AWS Clean Rooms console.

Per informazioni su come gestire una collaborazione utilizzando gli AWS SDK, consulta l'AWS Clean RoomsAPI Reference.

Argomenti

Modifica delle collaborazioni

Scopri come modificare le diverse parti di una collaborazione.

Argomenti

Modifica il nome e la descrizione della collaborazione

Dopo aver creato la collaborazione, puoi solo modificare il nome e la descrizione della collaborazione.

> **Note**
>
> Se hai abilitato la registrazione delle query, puoi modificare se i log delle query sono archiviati nel tuo account Amazon CloudWatch Logs.

Per modificare il nome e la descrizione della collaborazione

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione che hai creato.
4. Nella pagina dei dettagli della collaborazione, scegli Azioni, quindi scegli Modifica collaborazione.
5. Per i dettagli, modifica il nome e la descrizione della collaborazione.
6. Seleziona Salvataggio delle modifiche.

Modifica i tag di collaborazione

In qualità di creatore di una collaborazione, dopo aver creato una collaborazione, puoi gestire i tag sulla risorsa di collaborazione.

Per modificare i tag di collaborazione

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione che hai creato.
4. Seleziona una delle seguenti opzioni:

Se hai...	Quindi...
Un membro della collaborazione	Seleziona la scheda Details (Dettagli).
L'autore della collaborazione ma non un membro della collaborazione	Scorri la pagina verso il basso fino alla sezione Tag.

5. Per i dettagli sulla collaborazione, scegli Gestisci tag.
6. Nella pagina Gestisci tag, è possibile:
   - Per rimuovere un tag, scegli Remove (Rimuovi).
   - Per aggiungere un tag, scegliere Add new tag(Aggiungi un nuovo tag).
   - Per salvare le modifiche, scegli Salva modifiche

Modifica i tag di iscrizione

In qualità di creatore di collaborazioni, dopo aver creato una collaborazione, puoi gestire i tag sulla risorsa di appartenenza.

Per modificare i tag di appartenenza

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione che hai creato.
4. Seleziona la scheda Details (Dettagli).
5. Per i dettagli sull'iscrizione, scegli Gestisci tag.
6. Nella pagina Gestisci i tag di iscrizione, puoi effettuare le seguenti operazioni:

- Per rimuovere un tag, scegli Remove (Rimuovi).
- Per aggiungere un tag, scegliere Add new tag(Aggiungi un nuovo tag).
- Per salvare le modifiche, scegliere Save changes (Salva modifiche).

Modifica i tag della tabella associati

In qualità di creatore di una collaborazione, dopo aver associato le tabelle a una collaborazione, puoi gestire i tag sulla risorsa tabellare associata.

Per modificare i tag della tabella associati

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione che hai creato.
4. Scegliere la scheda Tabelle.
5. Per le tabelle associate a te, scegli una tabella.
6. Nella pagina di dettaglio della tabella configurata, per Tag, scegli Gestisci tag.

   Nella pagina Gestisci tag, è possibile:

   - Per rimuovere un tag, scegli Remove (Rimuovi).
   - Per aggiungere un tag, scegliere Add new tag(Aggiungi un nuovo tag).
   - Per salvare le modifiche, scegliere Save changes (Salva modifiche).

Modifica i tag del modello di analisi

In qualità di creatore di collaborazioni, dopo aver creato una collaborazione, puoi gestire i tag sulla risorsa del modello di analisi.

Per modificare i tag di appartenenza

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.

3. Scegli la collaborazione che hai creato.
4. Scegliere la scheda Templates (Modelli).
5. Nella sezione Modelli di analisi creati da te, scegli il modello di analisi.
6. Nella pagina dei dettagli della tabella del modello di analisi, scorri verso il basso fino alla sezione Tag.
7. Scegliere Gestisci tag.
8. Nella pagina Gestisci tag, è possibile:

   - Per rimuovere un tag, scegli Remove (Rimuovi).
   - Per aggiungere un tag, scegliere Add new tag(Aggiungi un nuovo tag).
   - Per salvare le modifiche, scegliere Save changes (Salva modifiche).

Modifica i tag delle norme sulla privacy differenziali

In qualità di creatore di collaborazioni, dopo aver creato una collaborazione, puoi gestire i tag sulla risorsa del modello di analisi.

Per modificare i tag di appartenenza

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione che contiene l'informativa sulla privacy differenziale che desideri modificare.
4. Scegliere la scheda Tabelle.
5. Nella scheda Tabelle, scegli Gestisci tag.
6. Nella pagina Gestisci tag, è possibile:

   - Per rimuovere un tag, scegli Remove (Rimuovi).
   - Per aggiungere un tag, scegliere Add new tag(Aggiungi un nuovo tag).
   - Per salvare le modifiche, scegliere Save changes (Salva modifiche).

Eliminazione delle collaborazioni

In qualità di creatore di una collaborazione, puoi eliminare una collaborazione che hai creato.

> **Note**
>
> Quando elimini una collaborazione, tu e tutti i membri non potete eseguire interrogazioni, ricevere risultati o contribuire con dati. Ogni membro della collaborazione continua ad avere accesso ai propri dati come parte della propria iscrizione.

Per eliminare una collaborazione

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione che desideri eliminare.
4. In Azioni, scegli Elimina collaborazione.
5. Conferma l'eliminazione, quindi scegli Elimina.

Visualizzazione delle collaborazioni

In qualità di creatore di collaborazioni, puoi visualizzare tutte le collaborazioni che hai creato.

Per visualizzare le collaborazioni

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Nella pagina Collaborazioni, in Ultimo utilizzo, visualizza le ultime 5 collaborazioni utilizzate.
4. Nella scheda Con iscrizione attiva, visualizza l'elenco delle collaborazioni con iscrizione attiva.

   Puoi ordinare per nome, data di creazione dell'iscrizione e dettagli del tuo membro.

   Puoi utilizzare la barra di ricerca per cercare una collaborazione.
5. Nella scheda Disponibili per partecipare, visualizza l'elenco delle collaborazioni a cui partecipare.
6. Nella scheda Non più disponibile, visualizza l'elenco delle collaborazioni eliminate e delle iscrizioni per le collaborazioni che non sono più disponibili (iscrizioni rimosse).

Visualizzazione delle tabelle e delle regole di analisi

Per visualizzare le tabelle associate alla collaborazione e alle regole di analisi

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Scegliere la scheda Tabelle.
5. Seleziona una delle seguenti opzioni:
    a. Per visualizzare le tabelle associate alla collaborazione, per le tabelle associate a te, scegli una tabella (testo blu).
    b. Per visualizzare altre tabelle associate alla collaborazione, per Tabelle associate dai collaboratori, scegli una tabella (testo blu).
6. Visualizza i dettagli della tabella e le regole di analisi nella pagina dei dettagli della tabella.

Visualizzazione dei registri di utilizzo della privacy differenziale

In qualità di membro della collaborazione che protegge i dati con privacy differenziale, dopo aver creato una collaborazione con privacy differenziale, puoi monitorare l'utilizzo del budget per la privacy.

Per visualizzare quante aggregazioni sono state eseguite e quanto del budget per la privacy è stato utilizzato

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Scegliere la scheda Tabelle.
5. Scegli Visualizza i registri di utilizzo (testo blu).
6. Visualizza i dettagli di utilizzo, incluso il budget per la privacy e l'utilità fornita.

Monitoraggio dello stato dei membri

In qualità di creatore di una collaborazione, dopo aver creato una collaborazione, puoi monitorare lo stato di tutti i membri nella scheda Membri.

Per verificare lo stato di un membro

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione che hai creato.
4. Scegli la scheda Membri.
5. Visualizza lo stato di membro di ciascun membro.

Rimuovere un membro da una collaborazione

> **Note**
>
> La rimozione di un membro rimuove anche tutti i set di dati associati dalla collaborazione.

Per rimuovere un membro da una collaborazione

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione che hai creato.
4. Scegli la scheda Membri.
5. Seleziona il pulsante di opzione accanto al membro da rimuovere.

   > **Note**
   >
   > Un creatore di collaborazioni non può scegliere l'ID del proprio account.

6. Scegli Rimuovi.

7. Nella finestra di dialogo, conferma la decisione di rimuovere il membro digitando il testo **`confirm`** nel campo di immissione del testo.

> **Note**
>
> Se rimuovi il membro che paga i costi di elaborazione delle query, non sarà più consentita l'esecuzione di query nell'ambito della collaborazione.

Lasciare una collaborazione

In qualità di membro della collaborazione, puoi abbandonare una collaborazione eliminando l'iscrizione. Se sei il creatore della collaborazione, puoi abbandonare una collaborazione solo eliminando la collaborazione.

> **Note**
>
> Quando elimini l'iscrizione, lasci la collaborazione e non puoi rientrarvi. Se sei il membro che paga i costi di elaborazione delle query e elimini la tua iscrizione, non è consentita l'esecuzione di altre query.

Per abbandonare una collaborazione

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Per Con iscrizione attiva, scegli la collaborazione di cui sei membro.
4. Scegli Azioni.
5. Scegli Elimina iscrizione.
6. Nella finestra di dialogo, conferma la decisione di abbandonare la collaborazione digitando **`confirm`** nel campo di immissione del testo, quindi scegli Svuota ed elimina l'appartenenza.

   Sulla console viene visualizzato un messaggio che indica che l'iscrizione è stata eliminata.

   Il creatore della collaborazione vede lo stato di Membro come Sinistro.

Modifica delle associazioni di tabelle configurate

In qualità di membro della collaborazione, puoi modificare le associazioni di tabelle configurate che hai creato.

Per modificare le associazioni di tabelle configurate

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Scegli la scheda Tabelle.
5. Per le tabelle associate a te, scegli una tabella.
6. Nella pagina dei dettagli della tabella, scorri verso il basso per visualizzare i dettagli dell'associazione delle tabelle.
7. Scegli Modifica.
8. Nella pagina Modifica le associazioni tra tabelle configurate, aggiorna la descrizione o le informazioni di accesso al servizio.
9. Seleziona Salvataggio delle modifiche.

Dissociazione delle tabelle configurate

In qualità di membro della collaborazione, puoi dissociare una tabella configurata dalla collaborazione. Questa azione impedisce al membro che può eseguire una query sulla tabella.

Per dissociare una tabella configurata

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Scegli la scheda Tabelle.
5. Per le tabelle da te associate, seleziona il pulsante di opzione accanto alla tabella da cui desideri dissociare.
6. Scegli Dissocia.

7. Nella finestra di dialogo, confermate la decisione di dissociare la tabella configurata e impedite al membro che può eseguire la query di interrogare la tabella scegliendo Dissocia.

Modifica di una politica sulla privacy differenziale

In qualsiasi momento, dopo aver configurato l'informativa sulla privacy differenziale, puoi aggiornarla per riflettere meglio le tue esigenze di privacy.

Per modificare l'informativa sulla privacy differenziale

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Nella scheda Tabelle della pagina di collaborazione, in Tabelle associate a te, scegli Modifica.
5. Nella pagina Modifica privacy differenziale, scegli nuovi valori per le seguenti proprietà:

   - Budget per la privacy: sposta la barra di scorrimento per aumentare o diminuire il budget in qualsiasi momento durante una collaborazione. Non puoi ridurre il budget dopo che il membro che può eseguire la query ha iniziato a interrogare i tuoi dati. Se il budget per la privacy viene aumentato, AWS Clean Rooms continuerà a utilizzare il budget esistente fino a esaurirlo completamente prima di utilizzare il budget per la privacy appena aggiunto.
   - Rumore aggiunto per query: sposta la barra di scorrimento per aumentare o diminuire il rumore aggiunto per query in qualsiasi momento durante una collaborazione.

   > **Note**
   >
   > Puoi scegliere Esempi interattivi per scoprire in che modo i diversi valori di Privacy, budget e Noise aggiunti per query influiscono sul numero di funzioni aggregate che puoi eseguire.

   Non puoi modificare il valore dell'aggiornamento del budget per la privacy. Per modificare la selezione, è necessario eliminare l'informativa sulla privacy differenziale e crearne una nuova.
6. Seleziona Salvataggio delle modifiche.

Viene visualizzato un messaggio di conferma che l'informativa sulla privacy differenziale è stata modificata con successo.

Eliminazione di un'informativa sulla privacy differenziale

È possibile eliminare l'informativa sulla privacy differenziale dalla scheda Tabelle di una collaborazione.

Per eliminare l'informativa sulla privacy differenziale

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Nella scheda Tabelle della pagina di collaborazione, accanto a Informativa sulla privacy differenziale, seleziona Elimina.
5. Se sei sicuro di voler eliminare l'informativa sulla privacy differenziale, scegli Elimina.

Dopo aver eliminato un'informativa sulla privacy differenziale, non puoi accedere ai registri di utilizzo del budget per la privacy relativi a tale politica. Le tabelle con privacy differenziale attivata non possono essere interrogate se l'informativa sulla privacy differenziale viene eliminata.

Visualizzazione dei parametri di privacy differenziali calcolati

Per gli utenti esperti di privacy differenziale, è possibile visualizzare i parametri di privacy differenziale calcolati dalla scheda Query di una collaborazione.

Per visualizzare i parametri di privacy differenziali calcolati

1. Accedi a AWS Management Console e apri la AWS Clean Roomsconsole con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Collaborazioni.
3. Scegli la collaborazione.
4. Nella scheda Interrogazioni, nella sezione Risultati, seleziona Visualizza i parametri di privacy differenziali calcolati.

Nella tabella dei parametri di privacy differenziali calcolati, puoi visualizzare i valori di sensibilità delle funzioni aggregate, che sono definiti come la quantità massima in base alla quale il risultato di una funzione può cambiare se i record di un singolo utente vengono aggiunti, rimossi o modificati. L'elenco include i seguenti parametri di privacy differenziali:

- Il limite di contributo dell'utente (UCL) è il numero massimo di righe inserite da un utente in una query SQL. Ad esempio, se desideri contare il numero totale di impressioni corrispondenti in una determinata campagna in cui ogni utente può avere più impressioni, AWS Clean Rooms Differential Privacy deve limitare il numero di impressioni di un singolo utente per garantire che il calcolo della privacy differenziale sia accurato. In altre parole, se un utente ha più impressioni del limite, prende AWS Clean Rooms automaticamente un campione casuale uniforme delle impressioni di quell'utente in base al valore UCL calcolato ed esclude le impressioni rimanenti di quell'utente durante l'esecuzione della query. Il valore UCL è uguale a 1 se si sta contando il numero di utenti unici. Questo perché l'aggiunta, la rimozione o la modifica di un singolo utente può modificare il numero di utenti distinti al massimo di 1.
- Il valore minimo è il limite inferiore di un'espressione utilizzata all'interno di una funzione aggregata come. `sum()` Ad esempio, se l'espressione è una colonna nota come`purchase_value`, il valore minimo è il limite inferiore della colonna.
- Il valore massimo è il limite superiore di un'espressione utilizzata all'interno di una funzione di aggregazione come`sum()`. Ad esempio, se l'espressione è una colonna nota come`purchase_value`, il valore massimo è il limite superiore della colonna.

Nella tabella Parametri di privacy differenziali calcolati, puoi utilizzare questi parametri per comprendere meglio la quantità totale di rumore nei risultati delle query. Ad esempio, quando il Noise configurato aggiunto per query è di 30 utenti e viene eseguita una `COUNT DISTINCT (user_id)` query, AWS Clean Rooms Differential Privacy aggiunge un rumore casuale compreso tra -30 e 30 con alta probabilità perché la sensibilità di `COUNT DISTINCT` è 1. Nel caso di una `COUNT` query con la stessa configurazione, AWS Clean Rooms Differential Privacy aggiunge un disturbo statistico che viene ridimensionato in base al limite di contributo dell'utente, poiché un singolo utente potrebbe contribuire con più righe al risultato della query. Nel caso di una `SUM` query come quella in `SUM (purchase_value)` cui tutti i valori delle colonne sono positivi, il rumore totale viene ridimensionato in base al limite di contributo dell'utente moltiplicato per il valore massimo. AWS Clean Rooms Differential Privacy calcola automaticamente i parametri di sensibilità per aggiungere rumore in fase di esecuzione della query e riduce il budget per la privacy. L'esaurimento del budget dedicato alla privacy è necessario perché i parametri di sensibilità dipendono dai dati.

Gestione delle tabelle configurate in AWS Clean Rooms

I seguenti argomenti descrivono come gestire le tabelle configurate AWS Clean Rooms utilizzando la AWS Clean Rooms console.

Per informazioni su come gestire le tabelle configurate utilizzando gli AWS SDK, consulta l'AWS Clean Rooms API Reference.

Argomenti

Modifica dei dettagli delle tabelle configurate

In qualità di membro della collaborazione, puoi modificare i dettagli della tabella configurata.

Per modificare i dettagli della tabella configurata

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Scegli la tabella configurata che hai creato.
4. Nella pagina dei dettagli della tabella configurata, scorri verso il basso fino a Dettagli della tabella configurata.
5. Scegli Modifica.
6. Aggiorna il nome o la descrizione della tabella configurata.
7. Seleziona Salvataggio delle modifiche.

Modifica dei tag della tabella configurati

Come membro della collaborazione, dopo aver creato una tabella configurata, puoi gestire i tag nella risorsa della tabella configurata nella scheda Tabelle configurate.

Per modificare i tag della tabella configurati

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Scegli la tabella configurata che hai creato.
4. Nella pagina dei dettagli della tabella configurata, scorri verso il basso fino alla sezione Tag.
5. Scegliere Gestisci tag.
6. Nella pagina Gestisci tag, è possibile:
   - Per rimuovere un tag, scegli Remove (Rimuovi).
   - Per aggiungere un tag, scegliere Add new tag(Aggiungi un nuovo tag).
   - Per salvare le modifiche, scegliere Save changes (Salva modifiche).

Modifica della regola di analisi della tabella configurata

Per modificare la regola di analisi delle tabelle configurata

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Scegli la tabella configurata che hai creato.
4. Nella pagina dei dettagli della tabella configurata, scorri verso il basso fino alla sezione Regola di analisi di aggregazione, Regola di analisi dell'elenco o Regola di analisi personalizzata. (La scelta dipende dal tipo di regola di analisi scelto per la tabella configurata.)
5. Scegli Modifica.
6. Nella pagina Modifica regola di analisi, puoi:
   - Modificare la definizione della regola di analisi nei seguenti modi:
     - Modifica dell'editor JSON.
     - Scegliete Importa da file per caricare una nuova definizione di regola di analisi.
   - Visualizza in anteprima ciò che i membri vedranno in una collaborazione selezionando una delle seguenti opzioni:
     - Visualizzazione della tabella

- JSON
- Query di esempio

7. Per salvare le modifiche, scegliere Salva modifiche.

Eliminazione della regola di analisi delle tabelle configurata

> **Warning**
>
> Questa azione non può essere annullata e ha un impatto su tutte le risorse correlate.

Per eliminare la regola di analisi della tabella configurata

1. Accedi a AWS Management Console e apri la AWS Clean Rooms console con il tuo Account AWS (se non l'hai ancora fatto).
2. Nel riquadro di navigazione a sinistra, scegli Tabelle configurate.
3. Scegli la tabella configurata che hai creato.
4. Nella pagina dei dettagli della tabella configurata, scorri verso il basso fino alla sezione Regola di analisi di aggregazione, Regola di analisi dell'elenco o Regola di analisi personalizzata. (La scelta dipende dal tipo di regola di analisi scelto per la tabella configurata.)
5. Scegli Elimina.
6. Se sei sicuro di voler eliminare la regola di analisi, scegli Elimina.

Risoluzione dei problemi AWS Clean Rooms

Questa sezione descrive alcuni problemi comuni che potrebbero insorgere durante l'utilizzo AWS Clean Rooms e come risolverli.

Problemi

Una o più tabelle a cui fa riferimento la query non sono accessibili in base al ruolo di servizio associato. Il proprietario della tabella/ruolo deve concedere al ruolo di servizio l'accesso alla tabella.

- Verificare che le autorizzazioni per il ruolo di servizio siano configurate come richiesto. Per ulteriori informazioni, vedereConfigurazione AWS Clean Rooms.

Uno dei set di dati sottostanti ha un formato di file non supportato.

- Assicurati che il set di dati sia in uno dei formati di file supportati:
  - Parquet
  - RCFile
  - TextFile
  - SequenceFile
  - RegexSerde
  - OpenCSV
  - AVRO
  - JSON

Per ulteriori informazioni, consulta Formati di dati per AWS Clean Rooms.

I risultati delle query non sono quelli previsti quando si utilizza Cryptographic Computing for. Clean Rooms

Se utilizzi Cryptographic Computing for Clean Rooms (C3R), verifica che la tua query utilizzi correttamente le colonne crittografate:

- Le sealed colonne vengono utilizzate solo nelle clausole. SELECT
- Le fingerprint colonne vengono utilizzate solo nelle JOIN clausole (e nelle clausole in determinate GROUP BY condizioni).
- Che siete JOINing fingerprint colonne con lo stesso nome solo se le impostazioni di collaborazione lo richiedono.

Per ulteriori informazioni, consultare Calcolo crittografico e the section called “Tipi di colonne”.

Sicurezza in AWS Clean Rooms

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili AWS Clean Rooms, consulta AWS Services in Scope by Compliance Program .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i tuoi requisiti aziendali e le leggi e le normative applicabili

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Clean Rooms. Ti mostra come configurare per AWS Clean Rooms soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS Clean Rooms le tue risorse.

Indice

Protezione dei dati in AWS Clean Rooms

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS Clean Rooms. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori o Servizi AWS utilizzi la console, l'API AWS Clean Rooms o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati a riposo

AWS Clean Rooms crittografa sempre tutti i metadati del servizio inattivi senza richiedere alcuna configurazione aggiuntiva. Questa crittografia è automatica quando si utilizza. AWS Clean Rooms

Clean Rooms ML crittografa tutti i dati archiviati all'interno del servizio in uso con AWS KMS. Se scegli di fornire la tua chiave KMS, i contenuti dei tuoi modelli simili e dei lavori di generazione di segmenti simili vengono crittografati con la tua chiave KMS.

> **Note**
>
> Puoi utilizzare le opzioni di crittografia di Amazon S3 per proteggere i dati archiviati. Per ulteriori informazioni, consulta Specificare la crittografia di Amazon S3 nella Amazon S3 User Guide.

Crittografia in transito

AWS Clean Rooms utilizza Transport Layer Security (TLS) e la crittografia lato client per la crittografia in transito. La comunicazione con AWS Clean Rooms avviene sempre tramite HTTPS, quindi i dati sono sempre crittografati in transito. Ciò include tutti i dati in transito quando si utilizza Clean Rooms ML.

Crittografia dei dati sottostanti

Per ulteriori informazioni su come crittografare i dati sottostanti, consulta. Elaborazione crittografica per Clean Rooms

Conservazione dei dati in AWS Clean Rooms

Quando crei un modello simile, Clean Rooms ML legge i dati di addestramento, li trasforma in un formato adatto al nostro modello ML e memorizza i parametri del modello addestrato all'interno di Clean Rooms ML. Clean Rooms ML non conserva una copia dei dati di allenamento. AWS Clean Rooms Le query SQL non conservano alcun dato dopo l'esecuzione della query. Clean Rooms ML utilizza quindi il modello addestrato per riepilogare il comportamento di tutti gli utenti. Clean Rooms ML memorizza un set di dati a livello utente per ogni utente nei dati per tutto il tempo in cui il modello di somiglianza è attivo.

Quando si avvia un processo di generazione di segmenti simili, Clean Rooms ML legge i dati iniziali, legge i riepiloghi dei comportamenti dal modello di somiglianza associato e crea un segmento simile archiviato all'interno del servizio. AWS Clean Rooms Clean Rooms ML non conserva una copia dei dati iniziali. Clean Rooms ML memorizza l'output a livello utente del lavoro finché il lavoro è attivo.

Se desideri rimuovere i dati relativi al lavoro relativo al modello simile o alla generazione di segmenti simili, utilizza l'API per eliminarli. Clean Rooms ML elimina in modo asincrono tutti i dati associati al modello o al lavoro. Una volta completato questo processo, Clean Rooms ML elimina i metadati per il modello o il lavoro e non sono più visibili nell'API. Clean Rooms ML conserva i dati eliminati per 3 giorni per la prevenzione del disaster recovery. Una volta che il lavoro o il modello non sono più visibili nell'API e sono trascorsi 3 giorni, tutti i dati associati al modello o al lavoro sono stati eliminati definitivamente.

Le migliori pratiche per la collaborazione sui dati in AWS Clean Rooms

Questo argomento descrive le migliori pratiche per condurre collaborazioni sui dati in. AWS Clean Rooms

AWS Clean Rooms segue il modello di responsabilitàAWS condivisa. AWS Clean Rooms offre regole di analisi che è possibile configurare per rafforzare la capacità di proteggere i dati sensibili in una collaborazione. Le regole di analisi configurate AWS Clean Rooms applicheranno le restrizioni (controlli di query e controlli di output delle query) che avete configurato. Sei responsabile della determinazione delle restrizioni e della configurazione delle regole di analisi di conseguenza.

Le collaborazioni sui dati potrebbero comportare qualcosa di più del semplice utilizzo di. AWS Clean Rooms Per aiutarti a massimizzare i vantaggi delle collaborazioni sui dati, ti consigliamo di eseguire le seguenti best practice utilizzando AWS Clean Rooms e in particolare con le regole di analisi.

Argomenti

Le migliori pratiche con AWS Clean Rooms

Sei responsabile della valutazione del rischio di ogni collaborazione sui dati e del confronto con i requisiti di privacy, come i programmi e le politiche di conformità esterni e interni. Ti consigliamo di

intraprendere azioni aggiuntive con l'utilizzo di AWS Clean Rooms. Queste azioni possono aiutare a gestire ulteriormente i rischi e a prevenire i tentativi di terze parti di reidentificare i dati (ad esempio, attacchi di differenziazione o attacchi side-channel).

Ad esempio, valuta la possibilità di condurre una due diligence sugli altri collaboratori e di stipulare accordi legali con loro prima di avviare una collaborazione. Per monitorare l'uso dei tuoi dati, prendi in considerazione anche l'adozione di altri meccanismi di controllo che prevedano l'utilizzo di. AWS Clean Rooms

Le migliori pratiche per l'utilizzo delle regole di analisi in AWS Clean Rooms

Le regole di analisi AWS Clean Rooms consentono di limitare le query che possono essere eseguite impostando i controlli di interrogazione su una tabella configurata. Ad esempio, è possibile impostare un controllo di interrogazione su come unire una tabella configurata e quali colonne possono essere selezionate. È inoltre possibile limitare l'output della query impostando i controlli dei risultati delle query, ad esempio le soglie di aggregazione sulle righe di output. Il servizio rifiuta qualsiasi query e rimuove le righe che non rispettano le regole di analisi impostate dai membri nelle tabelle configurate nella query.

Consigliamo le seguenti 10 best practice per l'utilizzo delle regole di analisi nella tabella configurata:

- Crea tabelle configurate separate per casi d'uso di query diversi (ad esempio, pianificazione dell'audience o attribuzione). È possibile creare più tabelle configurate con la stessa AWS Glue tabella sottostante.
- Specificate le colonne nella regola di analisi (ad esempio, colonne di dimensione, colonne di elenco, colonne di unione) necessarie per le query in una collaborazione. Ciò potrebbe aiutare a mitigare il rischio di attacchi differenziati o consentire ad altri membri di decodificare i dati. Usa la funzionalità delle colonne consentite per annotare altre colonne che potresti voler rendere interrogabili in futuro. Per personalizzare le colonne che possono essere utilizzate per una determinata collaborazione, crea tabelle configurate aggiuntive con la stessa tabella sottostante. AWS Glue
- Specificate nella regola di analisi le funzioni necessarie per l'analisi nella collaborazione. Questo può aiutare a mitigare il rischio derivante da errori funzionali rari che possono presentare informazioni su un singolo punto dati. Per personalizzare le funzioni che possono essere utilizzate per una determinata collaborazione, crea tabelle configurate aggiuntive con la stessa AWS Glue tabella sottostante.
- Aggiungi vincoli di aggregazione su tutte le colonne i cui valori a livello di riga sono sensibili. Ciò include le colonne della tabella configurata che esistono anche nelle tabelle degli altri membri

della collaborazione e nelle regole di analisi come vincolo di aggregazione. Ciò include anche le colonne della tabella configurata che non sono interrogabili, ovvero le colonne che si trovano nella tabella configurata ma non sono incluse nella regola di analisi. I vincoli di aggregazione possono aiutare a mitigare il rischio derivante dalla correlazione dei risultati delle query con i dati esterni alla collaborazione.

- Crea collaborazioni di test e regole di analisi per testare le restrizioni create con regole di analisi specifiche.
- Esamina le tabelle configurate dal collaboratore e le regole di analisi dei membri sulle tabelle configurate per verificare che corrispondano a quanto concordato per la collaborazione. Questo può aiutare a mitigare il rischio derivante dall'ingegnerizzazione dei propri dati da parte di altri membri per eseguire query non concordate.
- Controlla la query di esempio fornita (solo console) che è abilitata nella tabella configurata dopo aver impostato la regola di analisi.

> **Note**
>
> Oltre alla query di esempio fornita, sono possibili altre query basate sulla regola di analisi e su altre tabelle e regole di analisi dei membri della collaborazione.

- È possibile aggiungere o aggiornare una regola di analisi per una tabella configurata in una collaborazione. Quando lo fai, esamina tutte le collaborazioni a cui è associata la tabella configurata e il relativo impatto. Questo aiuta a garantire che nessuna collaborazione utilizzi regole di analisi obsolete.
- Esamina le query eseguite nella collaborazione per verificare che corrispondano ai casi d'uso o alle query concordate per la collaborazione. (Le interrogazioni sono disponibili nei log delle interrogazioni quando la funzionalità di registrazione delle interrogazioni è attivata.) Questo può aiutare a mitigare il rischio derivante dall'esecuzione di analisi non concordate da parte dei membri e da potenziali attacchi come gli attacchi sui canali laterali.
- Esamina le colonne della tabella configurate utilizzate nelle regole di analisi dei membri della collaborazione e nelle query per verificare che corrispondano a quanto concordato nella collaborazione. (Le interrogazioni sono disponibili nei registri delle interrogazioni quando tale funzionalità è attivata.) Questo può aiutare a mitigare il rischio derivante dall'ingegnerizzazione dei propri dati da parte di altri membri per eseguire domande non concordate.

Identity and Access Management per AWS Clean Rooms

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Clean Rooms IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS Clean Rooms svolgi.

Utente del servizio: se utilizzi il AWS Clean Rooms servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS Clean Rooms funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS Clean Rooms, consulta Risoluzione dei problemi di AWS Clean Rooms identità e accesso.

Amministratore del servizio: se sei responsabile delle AWS Clean Rooms risorse della tua azienda, probabilmente hai pieno accesso a AWS Clean Rooms. È tuo compito determinare a quali AWS Clean Rooms funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS Clean Rooms, consultaCome AWS Clean Rooms funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS Clean Rooms. Per visualizzare esempi di policy AWS Clean Rooms basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per AWS Clean Rooms

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center) o l'autenticazione Single Sign-On della tua azienda sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per firmare personalmente le richieste, consulta la sezione Processo di firma con Signature Version 4 nella Riferimenti generali di AWS.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. È vivamente consigliato di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali

dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Utente root dell'account AWS le credenziali e le identità IAM in. Riferimenti generali di AWS

Identità federata

Come best practice, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli

utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua

una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

Ogni entità IAM (utente o ruolo) inizialmente non dispone di autorizzazioni. Di default, gli utenti non possono eseguire alcuna operazione, neppure modificare la propria password. Per autorizzare un utente a eseguire operazioni, un amministratore deve allegare una policy di autorizzazioni a tale utente. In alternativa, l'amministratore può aggiungere l'utente a un gruppo che dispone delle autorizzazioni desiderate. Quando un amministratore fornisce le autorizzazioni a un gruppo, le autorizzazioni vengono concesse a tutti gli utenti in tale gruppo.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, indipendentemente dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le politiche AWS gestite includono politiche gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei

servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i suoi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS Clean Rooms funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS Clean Rooms, scopri con quali funzionalità IAM è disponibile l'uso AWS Clean Rooms.

Funzionalità IAM che puoi utilizzare con AWS Clean Rooms

Funzionalità IAM	AWS Clean Rooms supporto
Policy basate su identità	Sì
Policy basate su risorse	Parziale
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Parziale
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	No

Per avere una panoramica generale di come AWS Clean Rooms e altri Servizi AWS utilizzi la maggior parte delle funzionalità IAM, consulta la sezione dedicata alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Politiche basate sull'identità per AWS Clean Rooms

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per AWS Clean Rooms

Per visualizzare esempi di politiche basate sull' AWS Clean Rooms identità, vedere. Esempi di policy basate sull'identità per AWS Clean Rooms

Politiche basate sulle risorse all'interno AWS Clean Rooms

Supporta le policy basate su risorse	Parziale

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Cross Account Resource Access in IAM nella IAM User Guide.

Il AWS Clean Rooms servizio supporta solo un tipo di policy basata sulle risorse, denominata policy gestita delle risorse con modello simile configurato, che è collegata a un modello di lookalike configurato. Questa politica definisce quali principali possono eseguire azioni sul modello di somiglianza configurato.

Per informazioni su come collegare una policy basata sulle risorse a un modello simile configurato, consulta. Comportamenti IAM per il machine learning AWS Clean Rooms

Azioni politiche per AWS Clean Rooms

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AWS Clean Rooms azioni, vedere Azioni definite da AWS Clean Rooms nel Service Authorization Reference.

Le azioni politiche in AWS Clean Rooms uso utilizzano il seguente prefisso prima dell'azione.

```
cleanrooms
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "cleanrooms:action1",
      "cleanrooms:action2"
         ]
```

Per visualizzare esempi di politiche AWS Clean Rooms basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Clean Rooms

Risorse politiche per AWS Clean Rooms

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di AWS Clean Rooms risorse e dei relativi ARN, consulta Resources defined by AWS Clean Rooms nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da AWS Clean Rooms.

Per visualizzare esempi di politiche AWS Clean Rooms basate sull'identità, vedere. Esempi di policy basate sull'identità per AWS Clean Rooms

Chiavi relative alle condizioni delle politiche per AWS Clean Rooms

Supporta le chiavi di condizione delle policy specifiche del servizio	Parziale

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per scoprire come AWS Clean Rooms ML utilizza le chiavi delle condizioni delle policy, consulta Comportamenti IAM per il machine learning AWS Clean Rooms.

ACL in AWS Clean Rooms

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AWS Clean Rooms

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AWS Clean Rooms

Supporta le credenziali temporanee	Sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per AWS Clean Rooms

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per AWS Clean Rooms

Supporta i ruoli di servizio	Sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. AWS Clean Rooms Modifica i ruoli di servizio solo quando viene AWS Clean Rooms fornita una guida in tal senso.

Ruoli collegati ai servizi per AWS Clean Rooms

Supporta i ruoli collegati ai servizi	No

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per AWS Clean Rooms

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS Clean Rooms . Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o l'API. AWS Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AWS Clean Rooms, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione AWS Clean Rooms nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console di AWS Clean Rooms
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS Clean Rooms risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA

quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console di AWS Clean Rooms

Per accedere alla AWS Clean Rooms console, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS Clean Rooms risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la AWS Clean Rooms console, allega anche la policy AWS Clean Rooms *FullAccess* o la policy *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
```

```
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiche gestite per AWS Clean Rooms

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: **AWSCleanRoomsReadOnlyAccess**

Puoi collegarti `AWSCleanRoomsReadOnlyAccess` ai tuoi principi IAM.

Questa policy concede autorizzazioni di sola lettura alle risorse e ai metadati in una collaborazione. `AWSCleanRoomsReadOnlyAccess`

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `CleanRoomsRead`— Consente ai principali l'accesso in sola lettura al servizio.
- `ConsoleDisplayTables`— Consente ai principali di accedere in sola lettura ai AWS Glue metadati necessari per mostrare i dati sulle tabelle sottostanti sulla console. AWS Glue
- `ConsoleLogSummaryQueryLogs`— Consente ai responsabili di visualizzare i log delle interrogazioni.
- `ConsoleLogSummaryObtainLogs`— Consente ai responsabili di recuperare i risultati del registro.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CleanRoomsRead",
   "Effect": "Allow",
   "Action": [
    "cleanrooms:BatchGet*",
    "cleanrooms:Get*",
    "cleanrooms:List*"
   ],
   "Resource": "*"
  },
  {
   "Sid": "ConsoleDisplayTables",
   "Effect": "Allow",
   "Action": [
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:GetTable",
    "glue:GetTables",
    "glue:GetPartition",
```

```
    "glue:GetPartitions",
    "glue:GetSchema",
    "glue:GetSchemaVersion",
    "glue:BatchGetPartition"
   ],
   "Resource": "*"
  },
  {
   "Sid": "ConsoleLogSummaryQueryLogs",
   "Effect": "Allow",
   "Action": [
    "logs:StartQuery"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
   "Sid": "ConsoleLogSummaryObtainLogs",
   "Effect": "Allow",
   "Action": [
    "logs:GetQueryResults"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politica gestita: **AWSCleanRoomsFullAccess**

Puoi collegarti `AWSCleanRoomsFullAccess` ai tuoi principi IAM.

Questa policy concede autorizzazioni amministrative che consentono l'accesso completo (lettura, scrittura e aggiornamento) alle risorse e ai metadati in una collaborazione. AWS Clean Rooms Questa politica include l'accesso per eseguire interrogazioni.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `CleanRoomsAccess`— Garantisce l'accesso completo a tutte le azioni su tutte le risorse per. AWS Clean Rooms
- `PassServiceRole`— Concede l'accesso per assegnare un ruolo di servizio solo al servizio (`PassedToService`condizione) che ha "cleanrooms" nel nome.

- `ListRolesToPickServiceRole`— Consente ai responsabili di elencare tutti i loro ruoli per poter scegliere un ruolo di servizio durante l'utilizzo. AWS Clean Rooms
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Consente ai dirigenti di visualizzare il ruolo del servizio e la politica corrispondente in IAM.
- `ListPoliciesToInspectServiceRolePolicy`— Consente ai dirigenti di visualizzare il ruolo del servizio e la politica corrispondente in IAM.
- `GetPolicyToInspectServiceRolePolicy`— Consente ai dirigenti di visualizzare il ruolo del servizio e la politica corrispondente in IAM.
- `ConsoleDisplayTables`— Consente ai principali di accedere in sola lettura ai AWS Glue metadati necessari per mostrare i dati sulle tabelle sottostanti AWS Glue sulla console.
- `ConsolePickQueryResultsBucketListAll`— Consente ai mandanti di scegliere un bucket Amazon S3 da un elenco di tutti i bucket S3 disponibili in cui vengono scritti i risultati delle query.
- `SetQueryResultsBucket`— Consente ai responsabili di scegliere un bucket S3 in cui scrivere i risultati delle query.
- `ConsoleDisplayQueryResults`— Consente ai responsabili di mostrare al cliente i risultati delle query, letti dal bucket S3.
- `WriteQueryResults`— Consente ai responsabili di scrivere i risultati della query in un bucket S3 di proprietà del cliente.
- `EstablishLogDeliveries`— Consente ai responsabili di inviare i log delle query al gruppo di log Amazon CloudWatch Logs di un cliente.
- `SetupLogGroupsDescribe`— Consente ai mandanti di utilizzare il processo di creazione dei gruppi di log di Amazon CloudWatch Logs.
- `SetupLogGroupsCreate`— Consente ai mandanti di creare un gruppo di CloudWatch log Amazon Logs.
- `SetupLogGroupsResourcePolicy`— Consente ai responsabili di impostare una politica delle risorse sul gruppo di log di Amazon CloudWatch Logs.
- `ConsoleLogSummaryQueryLogs`— Consente ai responsabili di visualizzare i log delle query.
- `ConsoleLogSummaryObtainLogs`— Consente ai responsabili di recuperare i risultati del registro.

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

```
{
 "Sid": "CleanRoomsAccess",
 "Effect": "Allow",
 "Action": [
  "cleanrooms:*"
 ],
 "Resource": "*"
},
{
 "Sid": "PassServiceRole",
 "Effect": "Allow",
 "Action": [
  "iam:PassRole"
 ],
 "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*",
 "Condition": {
  "StringEquals": {
   "iam:PassedToService": "cleanrooms.amazonaws.com"
  }
 }
},
{
 "Sid": "ListRolesToPickServiceRole",
 "Effect": "Allow",
 "Action": [
  "iam:ListRoles"
 ],
 "Resource": "*"
},
{
 "Sid": "GetRoleAndListRolePoliciesToInspectServiceRole",
 "Effect": "Allow",
 "Action": [
  "iam:GetRole",
  "iam:ListRolePolicies",
  "iam:ListAttachedRolePolicies"
 ],
 "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*"
},
{
 "Sid": "ListPoliciesToInspectServiceRolePolicy",
 "Effect": "Allow",
 "Action": [
  "iam:ListPolicies"
```

```
    ],
    "Resource": "*"
   },
   {
    "Sid": "GetPolicyToInspectServiceRolePolicy",
    "Effect": "Allow",
    "Action": [
     "iam:GetPolicy",
     "iam:GetPolicyVersion"
    ],
    "Resource": "arn:aws:iam::*:policy/*cleanrooms*"
   },
   {
    "Sid": "ConsoleDisplayTables",
    "Effect": "Allow",
    "Action": [
     "glue:GetDatabase",
     "glue:GetDatabases",
     "glue:GetTable",
     "glue:GetTables",
     "glue:GetPartition",
     "glue:GetPartitions",
     "glue:GetSchema",
     "glue:GetSchemaVersion",
     "glue:BatchGetPartition"
    ],
    "Resource": "*"
   },
   {
    "Sid": "ConsolePickQueryResultsBucketListAll",
    "Effect": "Allow",
    "Action": [
     "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
   },
   {
    "Sid": "SetQueryResultsBucket",
    "Effect": "Allow",
    "Action": [
     "s3:GetBucketLocation",
     "s3:ListBucketVersions"
    ],
    "Resource": "arn:aws:s3:::cleanrooms-queryresults*"
```

```
  },
  {
   "Sid": "WriteQueryResults",
   "Effect": "Allow",
   "Action": [
    "s3:ListBucket",
    "s3:PutObject"
   ],
   "Resource": "arn:aws:s3:::cleanrooms-queryresults*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ConsoleDisplayQueryResults",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject"
   ],
   "Resource": "arn:aws:s3:::cleanrooms-queryresults*"
  },
  {
   "Sid": "EstablishLogDeliveries",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogDelivery",
    "logs:GetLogDelivery",
    "logs:UpdateLogDelivery",
    "logs:DeleteLogDelivery",
    "logs:ListLogDeliveries"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "SetupLogGroupsDescribe",
   "Effect": "Allow",
   "Action": [
```

```
    "logs:DescribeLogGroups"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "SetupLogGroupsCreate",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogGroup"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "SetupLogGroupsResourcePolicy",
   "Effect": "Allow",
   "Action": [
     "logs:DescribeResourcePolicies",
    "logs:PutResourcePolicy"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": "cleanrooms.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ConsoleLogSummaryQueryLogs",
   "Effect": "Allow",
   "Action": [
    "logs:StartQuery"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
```

```
  {
   "Sid": "ConsoleLogSummaryObtainLogs",
   "Effect": "Allow",
   "Action": [
    "logs:GetQueryResults"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politica gestita: **AWSCleanRoomsFullAccessNoQuerying**

Puoi allegare `AWSCleanRoomsFullAccessNoQuerying` al tuoIAM principals.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo (lettura, scrittura e aggiornamento) alle risorse e ai metadati in una collaborazione. AWS Clean Rooms Questa politica esclude l'accesso per eseguire interrogazioni.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `CleanRoomsAccess`— Garantisce l'accesso completo a tutte le azioni su tutte le risorse AWS Clean Rooms, ad eccezione delle interrogazioni nelle collaborazioni.
- `CleanRoomsNoQuerying`— Nega `StartProtectedQuery` esplicitamente e impedisce l'interrogazione. `UpdateProtectedQuery`
- `PassServiceRole`— Concede l'accesso per trasferire un ruolo di servizio solo al servizio (`PassedToService`condizione) che ha "cleanrooms" nel nome.
- `ListRolesToPickServiceRole`— Consente ai responsabili di elencare tutti i loro ruoli per poter scegliere un ruolo di servizio durante l'utilizzo. AWS Clean Rooms
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Consente ai dirigenti di visualizzare il ruolo del servizio e la politica corrispondente in IAM.
- `ListPoliciesToInspectServiceRolePolicy`— Consente ai dirigenti di visualizzare il ruolo del servizio e la politica corrispondente in IAM.
- `GetPolicyToInspectServiceRolePolicy`— Consente ai dirigenti di visualizzare il ruolo del servizio e la politica corrispondente in IAM.
- `ConsoleDisplayTables`— Consente ai principali di accedere in sola lettura ai AWS Glue metadati necessari per mostrare i dati sulle tabelle sottostanti AWS Glue sulla console.

- `EstablishLogDeliveries`— Consente ai responsabili di inviare i log delle query al gruppo di log Amazon CloudWatch Logs di un cliente.
- `SetupLogGroupsDescribe`— Consente ai mandanti di utilizzare il processo di creazione dei gruppi di log di Amazon CloudWatch Logs.
- `SetupLogGroupsCreate`— Consente ai mandanti di creare un gruppo di CloudWatch log Amazon Logs.
- `SetupLogGroupsResourcePolicy`— Consente ai responsabili di impostare una politica delle risorse sul gruppo di log di Amazon CloudWatch Logs.
- `ConsoleLogSummaryQueryLogs`— Consente ai responsabili di visualizzare i log delle query.
- `ConsoleLogSummaryObtainLogs`— Consente ai responsabili di recuperare i risultati del registro.
- `cleanrooms`— Gestisci collaborazioni, modelli di analisi, tabelle configurate, appartenenze e risorse associate all'interno del servizio. AWS Clean Rooms Esegui varie operazioni come la creazione, l'aggiornamento, l'eliminazione, l'elenco e il recupero di informazioni su queste risorse.
- `iam`— Passare ruoli di servizio con nomi contenenti "`cleanrooms`" al servizio. AWS Clean Rooms Elenca i ruoli e le politiche e analizza i ruoli di servizio e le politiche relative al AWS Clean Rooms servizio.
- `glue`— Recupera informazioni su database, tabelle, partizioni e schemi da. AWS Glue Ciò è necessario per consentire al AWS Clean Rooms servizio di visualizzare e interagire con le fonti di dati sottostanti.
- `logs`— Gestisci le consegne dei log, i gruppi di log e le politiche delle risorse per CloudWatch Logs. Interroga e recupera i log relativi al servizio. AWS Clean Rooms Queste autorizzazioni sono necessarie per scopi di monitoraggio, controllo e risoluzione dei problemi all'interno del servizio.

La politica nega inoltre esplicitamente le azioni `cleanrooms:StartProtectedQuery` e impedisce `cleanrooms:UpdateProtectedQuery` agli utenti di eseguire o aggiornare direttamente le query protette, operazione che dovrebbe avvenire attraverso i meccanismi controllati. AWS Clean Rooms

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CleanRoomsAccess",
   "Effect": "Allow",
   "Action": [
    "cleanrooms:BatchGetCollaborationAnalysisTemplate",
```

```
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
    ],
```

```
    "Resource": "*"
   },
   {
    "Sid": "CleanRoomsNoQuerying",
    "Effect": "Deny",
    "Action": [
     "cleanrooms:StartProtectedQuery",
     "cleanrooms:UpdateProtectedQuery"
    ],
    "Resource": "*"
   },
   {
    "Sid": "PassServiceRole",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*",
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "ListRolesToPickServiceRole",
    "Effect": "Allow",
    "Action": [
     "iam:ListRoles"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GetRoleAndListRolePoliciesToInspectServiceRole",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:ListRolePolicies",
     "iam:ListAttachedRolePolicies"
    ],
    "Resource": "arn:aws:iam::*:role/service-role/*cleanrooms*"
   },
   {
    "Sid": "ListPoliciesToInspectServiceRolePolicy",
```

```
    "Effect": "Allow",
    "Action": [
     "iam:ListPolicies"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GetPolicyToInspectServiceRolePolicy",
    "Effect": "Allow",
    "Action": [
     "iam:GetPolicy",
     "iam:GetPolicyVersion"
    ],
    "Resource": "arn:aws:iam::*:policy/*cleanrooms*"
   },
   {
    "Sid": "ConsoleDisplayTables",
    "Effect": "Allow",
    "Action": [
     "glue:GetDatabase",
     "glue:GetDatabases",
     "glue:GetTable",
     "glue:GetTables",
     "glue:GetPartition",
     "glue:GetPartitions",
     "glue:GetSchema",
     "glue:GetSchemaVersion",
     "glue:BatchGetPartition"
    ],
    "Resource": "*"
   },
   {
    "Sid": "EstablishLogDeliveries",
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogDelivery",
     "logs:GetLogDelivery",
     "logs:UpdateLogDelivery",
     "logs:DeleteLogDelivery",
     "logs:ListLogDeliveries"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
```

```
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "SetupLogGroupsDescribe",
    "Effect": "Allow",
    "Action": [
     "logs:DescribeLogGroups"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "SetupLogGroupsCreate",
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogGroup"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
   {
    "Sid": "SetupLogGroupsResourcePolicy",
    "Effect": "Allow",
    "Action": [
      "logs:DescribeResourcePolicies",
     "logs:PutResourcePolicy"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": "cleanrooms.amazonaws.com"
     }
    }
   },
```

```
  {
   "Sid": "ConsoleLogSummaryQueryLogs",
   "Effect": "Allow",
   "Action": [
    "logs:StartQuery"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
  },
  {
   "Sid": "ConsoleLogSummaryObtainLogs",
   "Effect": "Allow",
   "Action": [
    "logs:GetQueryResults"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politica gestita: **AWSCleanRoomsMLReadOnlyAccess**

Puoi collegarti `AWSCleanRoomsMLReadOnlyAccess` ai tuoi principi IAM.

Questa policy concede autorizzazioni di sola lettura alle risorse e ai metadati in una collaborazione. `AWSCleanRoomsMLReadOnlyAccess`

Questa policy include le seguenti autorizzazioni:

- `CleanRoomsConsoleNavigation`— Concede l'accesso alla visualizzazione delle schermate della console. AWS Clean Rooms
- `CleanRoomsMLRead`— Consente ai principali l'accesso in sola lettura al servizio Clean Rooms ML.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CleanRoomsConsoleNavigation",
            "Effect": "Allow",
            "Action": [
                "cleanrooms:GetCollaboration",
                "cleanrooms:GetConfiguredAudienceModelAssociation",
```

```
                "cleanrooms:GetMembership",
                "cleanrooms:ListAnalysisTemplates",
                "cleanrooms:ListCollaborationAnalysisTemplates",
                "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
                "cleanrooms:ListCollaborations",
                "cleanrooms:ListConfiguredTableAssociations",
                "cleanrooms:ListConfiguredTables",
                "cleanrooms:ListMembers",
                "cleanrooms:ListMemberships",
                "cleanrooms:ListProtectedQueries",
                "cleanrooms:ListSchemas",
                "cleanrooms:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CleanRoomsMLRead",
            "Effect": "Allow",
            "Action": [
                "cleanrooms-ml:Get*",
                "cleanrooms-ml:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politica gestita: **AWSCleanRoomsMLFullAccess**

Puoi collegarti `AWSCleanRoomsMLFullAcces` ai tuoi principi IAM. Questa politica concede autorizzazioni amministrative che consentono l'accesso completo (lettura, scrittura e aggiornamento) alle risorse e ai metadati necessari a Clean Rooms ML.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `CleanRoomsMLFullAccess`— Concede l'accesso a tutte le azioni di Clean Rooms ML.
- `PassServiceRole`— Concede l'accesso per assegnare un ruolo di servizio solo al servizio (`PassedToService`condizione) che ha "cleanrooms-ml" nel nome.
- `CleanRoomsConsoleNavigation`— Garantisce l'accesso alla visualizzazione delle schermate della AWS Clean Rooms console.

- `CollaborationMembershipCheck`— Quando si avvia un lavoro di generazione di audience (segmento simile) all'interno di una collaborazione, il servizio Clean Rooms ML chiama `ListMembers` per verificare che la collaborazione sia valida, che il chiamante sia un membro attivo e che il proprietario del modello di pubblico configurato sia un membro attivo. Questa autorizzazione è sempre richiesta; il SID di navigazione della console è richiesto solo per gli utenti della console.
- `AssociateModels`— Consente ai responsabili di associare un modello Clean Rooms ML alla collaborazione dell'utente.
- `TagAssociations`— Consente ai responsabili di aggiungere tag all'associazione tra un modello simile e una collaborazione.
- `ListRolesToPickServiceRole`— Consente ai responsabili di elencare tutti i loro ruoli per poter scegliere un ruolo di servizio durante l'utilizzo. AWS Clean Rooms
- `GetRoleAndListRolePoliciesToInspectServiceRole`— Consente ai dirigenti di visualizzare il ruolo del servizio e la politica corrispondente in IAM.
- `ListPoliciesToInspectServiceRolePolicy`— Consente ai dirigenti di visualizzare il ruolo del servizio e la politica corrispondente in IAM.
- `GetPolicyToInspectServiceRolePolicy`— Consente ai dirigenti di visualizzare il ruolo del servizio e la politica corrispondente in IAM.
- `ConsoleDisplayTables`— Consente ai principali di accedere in sola lettura ai AWS Glue metadati necessari per mostrare i dati sulle tabelle sottostanti AWS Glue sulla console.
- `ConsolePickOutputBucket`— Consente ai mandanti di selezionare i bucket Amazon S3 per gli output del modello di audience configurato.
- `ConsolePickS3Location`— Consente ai mandanti di selezionare la posizione all'interno di un bucket per gli output del modello di audience configurato.

```
{
    "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 aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS Clean Rooms da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS Clean Rooms documenti.

Modifica	Descrizione	Data
AWSCleanRoomsFullAccessNoQuerying: aggiornamento a policy esistente	È stato aggiunto cleanrooms:BatchGetSchemaAnalysisRule a CleanRoomsAccess.	13 maggio 2024
AWSCleanRoomsFullAccess: aggiornamento a policy esistente	L'ID dello Statement è stato aggiornato AWSCleanRoomsFullAccess dal ConsolePickQueryResultsBucket al SetQueryResultsBucket in questo criterio per rappresentare meglio le autorizzazioni, poiché le autorizzazioni sono necessarie per impostare il bucket dei risultati delle query con e senza la console.	21 marzo 2024
AWSCleanRoomsMLReadOnlyAccess: nuova policy AWSCleanRoomsMLFullAccess: nuova policy	Aggiunto AWSCleanRoomsMLReadOnlyAccess e AWSCleanRoomsMLFullAccess per supportare AWS Clean Rooms ML.	29 novembre 2023

Modifica	Descrizione	Data
AWSCleanRoomsFullAccessNoQuerying: aggiornamento a policy esistente	Aggiunto cleanrooms:CreateAnalysisTemplatecleanrooms:GetAnalysisTemplate,cleanrooms:UpdateAnalysisTemplate, cleanrooms:DeleteAnalysisTemplate,cleanrooms:ListAnalysisTemplates, cleanrooms:GetCollaborationAnalysisTemplatecleanrooms:BatchGetCollaborationAnalysisTemplate, e cleanrooms:ListCollaborationAnalysisTemplates a per CleanRoomsAccess abilitare la nuova funzionalità dei modelli di analisi.	31 luglio 2023
AWSCleanRoomsFullAccessNoQuerying: aggiornamento a policy esistente	Aggiunto cleanrooms:ListTagsForResourcecleanrooms:UntagResource, e cleanrooms:TagResource per CleanRoomsAccess abilitare l'etichettatura delle risorse.	21 marzo 2023
AWS Clean Rooms ha iniziato a tenere traccia delle modifiche	AWS Clean Rooms ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	12 gennaio 2023

Risoluzione dei problemi di AWS Clean Rooms identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS Clean Rooms un IAM.

Argomenti

- Non sono autorizzato a eseguire alcuna azione in AWS Clean Rooms
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Clean Rooms risorse

Non sono autorizzato a eseguire alcuna azione in AWS Clean Rooms

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` IAM prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `cleanrooms:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cleanrooms:GetWidget on resource: my-example-widget
```

In questo caso, la policy deve essere aggiornata in modo che Mateo possa accedere alla risorsa *`my-example-widget`* mediante l'operazione `cleanrooms:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS Clean Rooms.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS Clean Rooms. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie AWS Clean Rooms risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Clean Rooms supporta queste funzionalità, consultaCome AWS Clean Rooms funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Prevenzione del problema "confused deputy" tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione tra servizi può causare il problema del sostituto confuso. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Si consiglia di utilizzare le chiavi di contesto della condizione `aws:SourceArn`globale nelle politiche delle risorse per limitare le autorizzazioni che AWSClean Rooms forniscono un altro servizio alla

risorsa. Utilizza `aws:SourceArn` se desideri consentire l'associazione di una sola risorsa all'accesso tra servizi.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Inoltre AWSClean Rooms, devi anche confrontarlo con la chiave di `sts:ExternalId` condizione.

Il valore di `aws:SourceArn` deve essere impostato sull'ARN dell'appartenenza al ruolo assunto.

L'esempio seguente mostra come utilizzare la chiave `aws:SourceArn` global condition context AWSClean Rooms per evitare il confuso problema del vice.

> **Note**
>
> La politica di esempio si applica alla politica di fiducia del ruolo di servizio AWSClean Rooms utilizzato per accedere ai dati dei clienti.
> Il valore di *`MembershipId`* è il tuo ID di AWSClean Rooms iscrizione alla collaborazione.

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

Comportamenti IAM per il machine learning AWS Clean Rooms

Lavori su più account

Clean Rooms ML consente a determinate risorse create da uno di Account AWS essere accessibili in modo sicuro nel proprio account da un altro. Account AWS Quando un client in A richiama Account AWS `StartAudienceGenerationJob` una `ConfiguredAudienceModel` risorsa di proprietà di Account AWS B, Clean Rooms ML crea due ARN per il lavoro. Un ARN in A e Account AWS un altro in B. Account AWS Gli ARN sono identici tranne che per i loro. Account AWS

Clean Rooms ML crea due ARN per il lavoro per garantire che entrambi gli account possano applicare le proprie politiche IAM ai lavori. Ad esempio, entrambi gli account possono utilizzare il controllo degli accessi basato su tag e applicare le politiche della propria AWS organizzazione. Il job elabora i dati di entrambi gli account, in modo che entrambi gli account possano eliminare il lavoro e i dati associati. Nessuno degli account può impedire all'altro account di eliminare il lavoro.

Esiste una sola esecuzione del lavoro ed entrambi gli account possono vedere il lavoro quando `ListAudienceGenerationJobs` chiamano. Entrambi gli account possono chiamare le `Export` API `GetDelete`, e sul posto di lavoro utilizzando l'ARN con il proprio Account AWS ID.

Nessuno dei due Account AWS può accedere al lavoro quando si utilizza un ARN con l'altro Account AWS ID.

Il nome del lavoro deve essere univoco all'interno di un Account AWS. Il nome in Account AWS B è *`$accounta-$name`*. Il nome scelto da Account AWS A è preceduto da A quando il lavoro viene Account AWS visualizzato in B. Account AWS

Affinché un account `StartAudienceGenerationJob` incrociato abbia successo, Account AWS B deve consentire tale azione sia sul nuovo lavoro in Account AWS B che su quello `ConfiguredAudienceModel` in Account AWS B utilizzando una politica delle risorse simile all'esempio seguente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Clean-Rooms-<CAMA ID>",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "accountA"
                ]
            },
            "Action": [
                "cleanrooms-ml:StartAudienceGenerationJob"
            ],
            "Resource": [
                "arn:aws:cleanrooms-ml:us-west-1:AccountB:configured-audience-
model/id",
                "arn:aws:cleanrooms-ml:us-west-1:AccountB:audience-generation-job/*"
            ],
            // optional - always set by AWS Clean Rooms
"Condition":{"StringEquals":{"cleanrooms-ml:CollaborationId":"UUID"}}
        }
    ]
}
```

Se utilizzi l'API AWS Clean Rooms ML per creare un modello simile configurato con `manageResourcePolicies` set to true, AWS Clean Rooms crea questa policy automaticamente.

Inoltre, la politica di identità del chiamante in Account AWS A richiede `StartAudienceGenerationJob` l'autorizzazione. `arn:aws:cleanrooms-ml:us-west-1:AccountA:audience-generation-job/*` Quindi ci sono tre risorse IAM per l'azione`StartAudienceGenerationJob`: il lavoro Account AWS A, il lavoro Account AWS B e il lavoro Account AWS B. `ConfiguredAudienceModel`

> **Warning**
>
> L'utente Account AWS che ha avviato il lavoro riceve un evento del registro di AWS CloudTrail controllo relativo al lavoro. Il proprietario Account AWS di `ConfiguredAudienceModel` non riceve un evento del registro di AWS CloudTrail controllo.

Etichettare i lavori

Quando imposti il `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` parametro di`CreateConfiguredAudienceModel`, tutti i lavori di generazione di segmenti simili all'interno del tuo account e creati a partire da quel modello di somiglianza configurato hanno per impostazione predefinita gli stessi tag del modello di somiglianza configurato. Il modello di somiglianza configurato è il genitore e il processo di generazione di segmenti simili è il processo secondario.

Se stai creando un lavoro all'interno del tuo account, i tag di richiesta del lavoro sostituiscono i tag principali. Le offerte di lavoro create da altri account non creano mai tag nel tuo account. Se imposti `childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE` e un altro account crea un lavoro, ci sono due copie del lavoro. La copia nel tuo account contiene i tag delle risorse principali e la copia nell'account di chi ha inviato il lavoro contiene i tag della richiesta.

Convalida dei collaboratori

Quando si concedono le autorizzazioni ad altri membri di una AWS Clean Rooms collaborazione, la politica delle risorse deve includere la chiave condizionale. `cleanrooms-ml:CollaborationId` Ciò impone che il `collaborationId` parametro sia incluso nella richiesta. StartAudienceGenerationJob Quando il `collaborationId` parametro è incluso nella richiesta, Clean Rooms ML verifica che la collaborazione esista, chi ha inviato il lavoro sia un membro attivo della collaborazione e il proprietario del modello simile configurato sia un membro attivo della collaborazione.

Quando si AWS Clean Rooms gestisce la politica delle risorse del modello Lookalike configurata (il `manageResourcePolicies` parametro è CreateConfiguredAudienceModelAssociation richiesto), questa chiave di condizione verrà impostata `TRUE` nella politica delle risorse. Pertanto, è necessario specificare il `collaborationId` in. StartAudienceGenerationJob

Accesso multi-account

`StartAudienceGenerationJob`Può essere chiamato solo da un account all'altro. Tutte le altre API Clean Rooms ML possono essere utilizzate solo con le risorse del proprio account. Ciò garantisce che i dati di allenamento, la configurazione del modello simile e altre informazioni rimangano private.

Clean Rooms ML non rivela mai Amazon S3 o AWS Glue le posizioni tra gli account. La posizione dei dati di formazione, la posizione di output del modello Lookalike configurato e la posizione iniziale per la generazione di segmenti simili non sono mai visibili su tutti gli account. Se si tratta di `Get` un lavoro di generazione di audience inviato da un altro account, il servizio non mostra l'ubicazione iniziale.

Convalida della conformità per AWS Clean Rooms

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.

- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS Clean Rooms

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Infrastruttura AWS globale.

Sicurezza dell'infrastruttura in AWS Clean Rooms

In quanto servizio gestito, AWS Clean Rooms è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS Clean Rooms attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Sicurezza di rete

Quando viene AWS Clean Rooms letto dal tuo bucket S3 durante l'esecuzione delle query, il traffico tra Amazon S3 e Amazon AWS Clean Rooms S3 viene instradato in modo sicuro attraverso la rete privata. AWS Il traffico in transito viene firmato tramite il protocollo Amazon Signature Version 4 (SIGv4) e crittografato tramite HTTPS. Questo traffico è autorizzato in base al ruolo di servizio IAM che hai impostato per la tabella configurata.

Puoi connetterti a livello di codice AWS Clean Rooms tramite un endpoint. Per un elenco degli endpoint del servizio, consulta AWS Clean Rooms endpoint e quote in. Riferimenti generali di AWS

Tutti gli endpoint del servizio sono solo HTTPS. Puoi utilizzare gli endpoint Amazon Virtual Private Cloud (VPC) nel caso in cui desideri connetterti dal AWS Clean Rooms tuo VPC e non desideri disporre di connettività Internet. Per ulteriori informazioni, consulta Accedere ai AWS servizi AWS PrivateLink nella Guida.AWS PrivateLink

Puoi assegnare policy IAM ai tuoi presidi IAM che utilizzano aws: chiavi di SourceVpce contesto per limitare il tuo principale IAM in modo che sia in grado di effettuare chiamate solo AWS Clean Rooms tramite un endpoint VPC e non su Internet.

Access AWS Clean Rooms o AWS Clean Rooms ML utilizzando un'interfaccia endpoint ()AWS PrivateLink

Puoi utilizzarlo AWS PrivateLink per creare una connessione privata tra il tuo cloud privato virtuale (VPC) e AWS Clean Rooms il machine learning. AWS Clean Rooms Puoi accedere al AWS Clean Rooms nostro AWS Clean Rooms ML come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze del tuo VPC non necessitano di indirizzi IP pubblici per accedervi. AWS Clean Rooms

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Queste sono interfacce di rete gestite dal richiedente che fungono da punto di ingresso per il traffico destinato a AWS Clean Rooms.

Per ulteriori informazioni, consulta la sezione Accesso a Servizi AWS tramite AWS PrivateLink nella Guida di AWS PrivateLink .

Considerazioni per AWS Clean Rooms

Prima di configurare un endpoint di interfaccia per AWS Clean Rooms, consulta le considerazioni nella Guida.AWS PrivateLink

AWS Clean Rooms e AWS Clean Rooms ML supportano l'esecuzione di chiamate a tutte le loro azioni API tramite l'endpoint dell'interfaccia.

Le policy degli endpoint VPC non sono supportate per AWS Clean Rooms il machine learning. AWS Clean Rooms Per impostazione predefinita, l'accesso completo a AWS Clean Rooms e AWS Clean Rooms ML è consentito tramite l'endpoint dell'interfaccia. In alternativa, è possibile associare un gruppo di sicurezza alle interfacce di rete degli endpoint per controllare il traffico verso AWS Clean Rooms o il AWS Clean Rooms machine learning attraverso l'endpoint dell'interfaccia.

Crea un endpoint di interfaccia per AWS Clean Rooms

Puoi creare un endpoint di interfaccia per AWS Clean Rooms o AWS Clean Rooms ML utilizzando la console Amazon VPC o AWS Command Line Interface ().AWS CLI Per ulteriori informazioni, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di AWS PrivateLink .

Crea un endpoint di interfaccia per AWS Clean Rooms utilizzare il seguente nome di servizio.

```
com.amazonaws.region.cleanrooms
```

Crea un endpoint di interfaccia per AWS Clean Rooms ML utilizzando il seguente nome di servizio.

```
com.amazonaws.region.cleanrooms-ml
```

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API AWS Clean Rooms utilizzando il nome DNS regionale predefinito. Ad esempio, `cleanrooms-ml.us-east-1.amazonaws.com`.

Monitoraggio AWS Clean Rooms

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Clean Rooms altre AWS soluzioni esistenti. AWS fornisce i seguenti strumenti di monitoraggio per osservare AWS Clean Rooms, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi file di log da istanze Amazon EC2 e altre AWS CloudTrail fonti. Amazon CloudWatch Logs può monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.

  Clean Rooms ML consente lavori su più account per determinate azioni API. L'utente Account AWS che ha avviato il lavoro riceve l'evento del registro di AWS CloudTrail controllo relativo al lavoro. Per ulteriori informazioni, consulta Comportamenti IAM per il machine learning AWS Clean Rooms
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto tuo Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Registrazione di chiamate API AWS Clean Rooms con AWS CloudTrail

AWS Clean Roomsè integrato conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o unServizio AWS inAWS Clean Rooms. CloudTrail acquisisce tutte le chiamate APIAWS Clean Rooms come eventi. Le chiamate acquisite includono le chiamate dalla console di AWS Clean Rooms e le chiamate di codice alle operazioni delle API AWS Clean Rooms. Se si crea un trail, è possibile abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi perAWS Clean Rooms. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia eventi. Le informazioni raccolte da CloudTrail, consentono di determinare la richiesta effettuata aAWS Clean

Rooms, l'indirizzo IP di origine da cui è stata effettuata la richiesta, l'autore della richiesta, il momento in cui è stata effettuata e altri dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida perAWS CloudTrail l'utente.

AWS Clean Roomsinformazioni in CloudTrail

CloudTrail è abilitato sul tuo alAccount AWS momento della sua creazione. Quando si verifica un'attività inAWS Clean Rooms, questa viene registrata in un CloudTrail evento insieme ad altriServizio AWS eventi nella cronologia eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia CloudTrail eventi.

Per una registrazione continua degli eventi nell'Account AWS che includa gli eventi per AWS Clean Rooms, crea un trail. Un trail consente di CloudTrail distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altriServizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei CloudTrail registri. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione file CloudTrail di file di file di file di Cloud
- Ricezione file CloudTrail di file di file di file di Cloud

TutteAWS Clean Rooms le azioni vengono registrate CloudTrail e documentate nell'AWS Clean RoomsAPI Reference.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle voci dei file di log di AWS Clean Rooms

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di log possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail i file di log non sono una traccia stack ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in base a un ordine specifico.

AWS Clean Rooms CloudTrail Eventi di esempio

I seguenti esempi dimostrano CloudTrail eventi per:

Argomenti

- StartProtectedQuery (riuscito)
- StartProtectedQuery(fallito)

StartProtectedQuery (riuscito)


```
{
    "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(fallito)

```
{
    "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"
}
```

Creazione di AWS Clean Rooms risorse con AWS CloudFormation

AWS Clean Rooms è integrato con AWS CloudFormation, un servizio che ti aiuta a modellare e configurare AWS le tue risorse. Grazie a questa integrazione, puoi dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri e fornisce AWS CloudFormation e configura tali risorse per te. Esempi di risorse includono collaborazioni, tabelle configurate, associazioni di tabelle configurate e appartenenze.

Quando lo utilizzi AWS CloudFormation, puoi riutilizzare il modello per configurare le AWS Clean Rooms risorse in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse più e più volte in più Account AWS e Regioni AWS.

AWS Clean Rooms e AWS CloudFormation modelli

Per fornire e configurare le risorse AWS Clean Rooms e i servizi correlati, è necessario conoscere AWS CloudFormation i modelli. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse che desideri fornire negli AWS CloudFormation stack. Se non conosci JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a usare i modelli. AWS CloudFormation Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation .

AWS Clean Rooms supporta la creazione di collaborazioni, tabelle configurate, associazioni di tabelle configurate e appartenenze a. AWS CloudFormationPer ulteriori informazioni, inclusi esempi di modelli JSON e YAML per collaborazioni, tabelle configurate, associazioni di tabelle configurate e appartenenze, consulta il riferimento ai tipi di AWS Clean Rooms risorse nella Guida per l'utente.AWS CloudFormation

Sono disponibili i seguenti modelli:

- Modello di analisi

  Specificate un modello di AWS Clean Rooms analisi, comprensivo di nome, descrizione, formato, origine, parametri e tag.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  AWS::CleanRooms::AnalysisTemplate nella Guida per l'utente di AWS Clean Rooms

CreateAnalysisTemplate nel documento di riferimento delle API AWS Clean Rooms

- Collaborazione

  Specificate una AWS Clean Rooms collaborazione, inclusi nome, descrizione, tipo, parametri e tag.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  AWS::CleanRooms::Collaboration nella Guida per l'utente di AWS CloudFormation

  CreateCollaboration nel documento di riferimento delle API AWS Clean Rooms

- Tabella configurata

  Specificate una tabella configurata in AWS Clean Rooms, incluse le colonne consentite, il metodo di analisi, la descrizione, il nome, il riferimento alla tabella, il budget per la privacy e i tag. Le tabelle configurate rappresentano un riferimento a una tabella esistente in AWS Glue Data Catalog che è stata configurata per l'uso in AWS Clean Rooms. Una tabella configurata contiene una regola di analisi che determina come i dati possono essere utilizzati.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  AWS::CleanRooms::ConfiguredTable nella Guida per l'utente di AWS CloudFormation

  CreateConfiguredTable nel documento di riferimento delle API AWS Clean Rooms

- Associazione di tabelle configurata

  Specificare un'associazione di tabelle configurata in AWS Clean Rooms, tra cui ID, descrizione, ID di appartenenza, nome, ruolo, Amazon Resource Name (ARN) e tag. Un'associazione di tabelle configurate collega una tabella configurata a una collaborazione.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  AWS::CleanRooms::ConfiguredTableAssociation nella Guida per l'utente di AWS CloudFormation

  CreateConfiguredTableAssociation nel documento di riferimento delle API AWS Clean Rooms

- Appartenenza

  Specificate l'appartenenza a un identificatore di collaborazione specifico e partecipate alla collaborazione. AWS Clean Rooms

  Per ulteriori informazioni, consulta i seguenti argomenti:

AWS::CleanRooms::Membership nella Guida per l'utente di AWS CloudFormation

CreateMembership nel documento di riferimento delle API AWS Clean Rooms

- Modello di budget per la privacy

  Specificate un modello di budget per la AWS Clean Rooms privacy, che includa un budget per la privacy, il rumore aggiunto per ogni query e l'aggiornamento mensile del budget per la privacy.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  AWS::CleanRooms::PrivacyBudgetTemplate nella Guida per l'utente di AWS CloudFormation

  CreatePrivacyBudgetTemplate nel documento di riferimento delle API AWS Clean Rooms
- Crea un set di dati di allenamento

  Specificate un set di dati di addestramento per un modello Clean Rooms ML da una AWS Glue tabella.

  Per ulteriori informazioni, consulta i seguenti argomenti:

  AWS::CleanRoomsML::TrainingDataset nella Guida per l'utente di AWS CloudFormation

  CreateTrainingDatasetnel riferimento all'API Clean Rooms ML

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- AWS CloudFormation Guida per l'utente
- AWS CloudFormation Documentazione di riferimento delle API
- Guida per l'utente dell'interfaccia a riga di comando di AWS CloudFormation

Quote per AWS Clean Rooms

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWS Salvo diversa indicazione, ogni quota è specifica per un. Regione AWS Puoi richiedere aumenti per alcune quote e altre quote non possono essere aumentate.

Per visualizzare le quote per AWS Clean Rooms, apri la console Service Quotas. Nel riquadro di navigazione, scegli Servizi AWS e seleziona AWS Clean Rooms.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo Aumento del limite di servizio.

La tua Account AWS ha le seguenti quote relative a. AWS Clean Rooms

Risorsa	Predefinito	Descrizione
Membri invitati per collaborazione	5	Numero massimo di membri invitati per collaborazione
Iscrizioni per account	100	Numero massimo di iscrizioni per un account
Collaborazioni create per account	10	Numero massimo di collaborazioni create per account
Tabelle configurate per account	60	Numero massimo di tabelle configurate che possono essere create da un account
Associazioni di tabelle per iscrizione	25	Numero massimo di tabelle associate per iscrizione attiva
Query in corso simultanee per iscrizione	5	Numero massimo di richieste contemporanee in corso per iscrizione

Risorsa	Predefinito	Descrizione
Elenco di colonne consentite per tabella configurata	100	Numero massimo di colonne consentite nell'elenco per tabella configurata
Tabelle configurate per query protetta	15	Numero massimo di tabelle configurate in una query protetta
Modelli di analisi per appartenenza	25	Numero massimo di modelli di analisi per iscrizione
Associazioni di modelli simili configurati (modello di pubblico) per appartenenza	5	Numero massimo di associazioni di modelli simili configurate per appartenenza.

Limiti dei parametri delle risorse

Risorsa	Predefinito	Descrizione
Dimensione delle regole di analisi	100 KB	Dimensione massima di JSON per una regola di analisi
Lunghezza del testo della query	90 KB (8 KB per le query differenziali sulla privacy)	Lunghezza massima del testo per un'istruzione di query SQL
Tempo di esecuzione della query	12 ore	Durata massima di esecuzione di una query prima del timeout
Dimensione di output del file di dati di interrogazione	6,2 GB	Dimensione massima di un file di output da una query protetta

Hai Account AWS le seguenti quote di transazioni API al secondo (TPS) per account per endpoint.

Quote di limitazione per le API

Risorsa	Limite frequenza	Descrizione
Frequenza delle richieste `BatchGetCollaborationAnalysisTemplate`	5 TPS	Numero massimo di chiamate `BatchGetCollaborationAnalysisTemplate` API al secondo
Frequenza delle `BatchGetSchema` richieste	5 TPS	Numero massimo di chiamate `BatchGetSchema` API al secondo
Frequenza delle `CreateAnalysisTemplate` richieste	5 TPS	Numero massimo di chiamate `CreateAnalysisTemplate` API al secondo
Frequenza delle `CreateCollaboration` richieste	5 TPS	Numero massimo di chiamate `CreateCollaboration` API al secondo
Frequenza delle `CreateConfiguredAudienceModelAssociation` richieste	5 TPS	Numero massimo di chiamate `CreateConfiguredAudienceModelAssociation` al secondo
Frequenza delle `CreateConfiguredTable` richieste	5 TPS	Numero massimo di chiamate `CreateConfiguredTable` al secondo
Frequenza delle `CreateConfiguredTableAnalysisRule` richieste	5 TPS	Numero massimo di chiamate `CreateConfiguredTableAnalysisRule` al secondo
Frequenza delle `CreateConfiguredTableAssociation` richieste	5 TPS	Numero massimo di chiamate `CreateConfiguredTableAssociation` al secondo

Risorsa	Limite frequenza	Descrizione
Frequenza delle `CreateMembership` richieste	5 TPS	Numero massimo di chiamate `CreateMembership` al secondo
Frequenza delle `CreatePrivacyBudgetTempate` richieste	5 TPS	Numero massimo di chiamate `CreatePrivacyBudgetTemplate` al secondo
Frequenza delle `DeleteAnalysisTemplate` richieste	5 TPS	Numero massimo di chiamate `DeleteAnalysisTemplate` al secondo
Frequenza delle `DeleteCollaboration` richieste	5 TPS	Numero massimo di chiamate `DeleteCollaboration` al secondo
Frequenza delle `DeleteConfiguredAudienceModelAssociation` richieste	5 TPS	Numero massimo di chiamate `DeleteConfiguredAudienceModelAssociation` al secondo
Frequenza delle `DeleteConfiguredTable` richieste	5 TPS	Numero massimo di chiamate `DeleteConfiguredTable` al secondo
Frequenza delle `DeleteConfiguredTableAnalysisRule` richieste	5 TPS	Numero massimo di chiamate `DeleteConfiguredTableAnalysisRule` al secondo
Frequenza delle `DeleteConfiguredTableAssociation` richieste	5 TPS	Numero massimo di chiamate `DeleteConfiguredTableAssociation` al secondo

Risorsa	Limite frequenza	Descrizione
Frequenza delle `DeleteMember` richieste	5 TPS	Numero massimo di chiamate `DeleteMember` al secondo
Frequenza delle `DeleteMembership` richieste	5 TPS	Numero massimo di chiamate `DeleteMembership` al secondo
Frequenza delle `DeletePrivacyBudgetTemplate` richieste	5 TPS	Numero massimo di chiamate `DeletePrivacyBudgetTemplate` al secondo
Frequenza delle `GetAnalysisTemplate` richieste	5 TPS	Numero massimo di chiamate `GetAnalysisTemplate` al secondo
Frequenza delle `GetCollaboration` richieste	5 TPS	Numero massimo di chiamate `GetCollaboration` al secondo
Frequenza delle `GetCollaborationConfiguredAudienceModelAssociation` richieste	5 TPS	Numero massimo di chiamate `GetCollaborationConfiguredAudienceModelAssociation` al secondo
Frequenza delle `GetCollaborationPrivacyBudgetTemplate` richieste	5 TPS	Numero massimo di chiamate `GetCollaborationPrivacyBudgetTemplate` al secondo
Frequenza delle `GetConfiguredAudienceModelAssociation` richieste	5 TPS	Numero massimo di chiamate `GetConfiguredAudienceModelAssociation` al secondo

Risorsa	Limite frequenza	Descrizione
Frequenza delle `GetConfiguredTable` richieste	5 TPS	Numero massimo di chiamate `GetConfiguredTable` al secondo
Frequenza delle `GetConfiguredTableAnalysisRule` richieste	5 TPS	Numero massimo di chiamate `GetConfiguredTableAnalysisRule` al secondo
Frequenza delle `GetConfiguredTableAssociation` richieste	20 TPS	Numero massimo di chiamate `GetConfiguredTableAssociation` al secondo
Frequenza delle `GetMembership` richieste	5 TPS	Numero massimo di chiamate `GetMembership` al secondo
Frequenza delle `GetPrivacyBudgetTemplate` richieste	5 TPS	Numero massimo di chiamate `GetPrivacyBudgetTemplate` al secondo
Frequenza delle `GetProtectedQuery` richieste	20 TPS	Numero massimo di chiamate `GetProtectedQuery` al secondo
Frequenza delle `GetSchema` richieste	5 TPS	Numero massimo di chiamate `GetSchema` al secondo
Frequenza delle `GetSchemaAnalysisRule` richieste	5 TPS	Numero massimo di chiamate `GetSchemaAnalysisRule` al secondo
Frequenza delle `ListAnalysisTemplates` richieste	5 TPS	Numero massimo di chiamate `ListAnalysisTemplates` al secondo

Risorsa	Limite frequenza	Descrizione
Frequenza delle `ListCollaborationConfiguredAudienceModelAssociations` richieste	5 TPS	Numero massimo di chiamate `ListCollaborationConfiguredAudienceModelAssociations` al secondo
Frequenza delle `ListCollaborationPrivacyBudgets` richieste	5 TPS	Numero massimo di chiamate `ListCollaborationPrivacyBudgets` al secondo
Frequenza delle `ListCollaborationPrivacyBudgetTemplates` richieste	5 TPS	Numero massimo di chiamate `ListCollaborationPrivacyBudgetTemplates` al secondo
Frequenza delle `ListCollaborations` richieste	5 TPS	Numero massimo di chiamate `ListCollaborations` al secondo
Frequenza delle `ListConfiguredAudienceModelAssociations` richieste	5 TPS	Numero massimo di chiamate `ListConfiguredAudienceModelAssociations` al secondo
Frequenza delle `ListConfiguredTableAssociations` richieste	5 TPS	Numero massimo di chiamate `ListConfiguredTableAssociations` al secondo
Frequenza delle `ListConfiguredTables` richieste	5 TPS	Numero massimo di chiamate `ListConfiguredTables` al secondo
Frequenza delle `ListMembers` richieste	5 TPS	Numero massimo di chiamate `ListMembers` al secondo

Risorsa	Limite frequenza	Descrizione
Frequenza delle `ListMemberships` richieste	5 TPS	Numero massimo di chiamate `ListMemberships` al secondo
Frequenza delle `ListPrivacyBudgets` richieste	5 TPS	Numero massimo di chiamate `ListPrivacyBudgets` al secondo
Frequenza delle `ListPrivacyBudgetTemplates` richieste	5 TPS	Numero massimo di chiamate `ListPrivacyBudgetTemplates` al secondo
Frequenza delle `ListProtectedQueries` richieste	5 TPS	Numero massimo di chiamate `ListProtectedQueries` al secondo
Frequenza delle `ListSchemas` richieste	5 TPS	Numero massimo di chiamate `ListSchemas` al secondo
Frequenza delle `StartProtectedQuery` richieste	5 TPS	Numero massimo di chiamate `StartProtectedQuery` al secondo
Frequenza delle `UpdateAnalysisTemplate` richieste	5 TPS	Numero massimo di chiamate `UpdateAnalysisTemplate` al secondo
Frequenza delle `UpdateCollaboration` richieste	5 TPS	Numero massimo di chiamate `UpdateCollaboration` al secondo
Frequenza delle `UpdateConfiguredAudienceModelAssociation` richieste	5 TPS	Numero massimo di chiamate `UpdateConfiguredAudienceModelAssociation` al secondo

Risorsa	Limite frequenza	Descrizione
Frequenza delle `UpdateConfiguredTable` richieste	5 TPS	Numero massimo di chiamate `UpdateConfiguredTable` al secondo
Frequenza delle `UpdateConfiguredTableAnalysisRule` richieste	5 TPS	Numero massimo di chiamate `UpdateConfiguredTableAnalysisRule` al secondo
Frequenza delle `UpdateConfiguredTableAssociation` richieste	5 TPS	Numero massimo di chiamate `UpdateConfiguredTableAssociation` al secondo
Frequenza delle `UpdatePrivacyBudgetTemplate` richieste	5 TPS	Numero massimo di chiamate `UpdatePrivacyBudgetTemplate` al secondo

AWS Clean Rooms Quote di limitazione dell'API ML

Risorsa	Limite frequenza	Descrizione
Frequenza delle richieste `CreateAudienceModel`	Velocità 1 TPS, raffica di 3 TPS	Numero massimo di chiamate `CreateAudienceModel` API al secondo
Frequenza delle `CreateConfiguredAudienceModel` richieste	10 TPS	Numero massimo di chiamate `CreateConfiguredAudienceModel` API al secondo
Frequenza delle `CreateTrainingDataset` richieste	10 TPS	Numero massimo di chiamate `CreateTrainingDataset` API al secondo

Risorsa	Limite frequenza	Descrizione
Frequenza delle `DeleteAudienceGenerationJob` richieste	Velocità 2 TPS, raffica di 10 TPS	Numero massimo di chiamate `DeleteAudienceGenerationJob` API al secondo
Frequenza delle `DeleteAudienceModel` richieste	Velocità 2 TPS, raffica di 10 TPS	Numero massimo di chiamate `DeleteAudienceModel` API al secondo
Frequenza delle `DeleteConfiguredAudienceModel` richieste	10 TPS	Numero massimo di chiamate `DeleteConfiguredAudienceModel` API al secondo
Frequenza delle `DeleteConfiguredAudienceModelPolicy` richieste	25 TPS	Numero massimo di chiamate `DeleteConfiguredAudienceModelPolicy` API al secondo
Frequenza delle `DeleteTrainingDataset` richieste	10 TPS	Numero massimo di chiamate `DeleteTrainingDataset` API al secondo
Frequenza delle `GetAudienceGenerationJob` richieste	50 TPS	Numero massimo di chiamate `GetAudienceGenerationJob` API al secondo
Frequenza delle `GetAudienceModel` richieste	50 TPS	Numero massimo di chiamate `GetAudienceModel` API al secondo
Frequenza delle `GetConfiguredAudienceModel` richieste	50 TPS	Numero massimo di chiamate `GetConfiguredAudienceModel` API al secondo

Risorsa	Limite frequenza	Descrizione
Frequenza delle `GetConfiguredAudienceModelPolicy` richieste	50 TPS	Numero massimo di chiamate `GetConfiguredAudienceModelPolicy` API al secondo
Frequenza delle `GetTrainingDataset` richieste	50 TPS	Numero massimo di chiamate `GetTrainingDataset` API al secondo
Frequenza delle `ListAudienceExportJobs` richieste	50 TPS	Numero massimo di chiamate `ListAudienceExportJobs` API al secondo
Frequenza delle `ListAudienceGenerationJobs` richieste	50 TPS	Numero massimo di chiamate `ListAudienceGenerationJobs` API al secondo
Frequenza delle `ListAudienceModels` richieste	50 TPS	Numero massimo di chiamate `ListAudienceModels` API al secondo
Frequenza delle `ListConfiguredAudienceModels` richieste	50 TPS	Numero massimo di chiamate `ListConfiguredAudienceModels` API al secondo
Frequenza delle `ListTagsForResource` richieste	50 TPS	Numero massimo di chiamate `ListTagsForResource` API al secondo
Frequenza delle `ListTrainingDatasets` richieste	50 TPS	Numero massimo di chiamate `ListTrainingDatasets` API al secondo

Risorsa	Limite frequenza	Descrizione
Frequenza delle `PutConfiguredAudienceModelPolicy` richieste	25 TPS	Numero massimo di chiamate `PutConfiguredAudienceModelPolicy` API al secondo
Frequenza delle `StartAudienceExportJob` richieste	Velocità 1 TPS, raffica di 3 TPS	Numero massimo di chiamate `StartAudienceExportJob` API al secondo
Frequenza delle `StartAudienceGenerationJob` richieste	Velocità 1 TPS, raffica di 5 TPS	Numero massimo di chiamate `StartAudienceGenerationJob` API al secondo
Frequenza delle `TagResource` richieste	10 TPS	Numero massimo di chiamate `TagResource` API al secondo
Frequenza delle `UntagResource` richieste	50 TPS	Numero massimo di chiamate `UntagResource` API al secondo
Frequenza delle `UpdateConfiguredAudienceModel` richieste	10 TPS	Numero massimo di chiamate `UpdateConfiguredAudienceModel` API al secondo

Nome	Predefinita	Adattabile	Descrizione
Lavori di esportazione di audience attivi per lavoro di generazione di audience	Ogni regione supportata: 25	No	Il numero massimo di lavori di esportazione di pubblico attivi per un lavoro che genera audience

Nome	Predefinita	Adatta e	Descrizione
Pubblico in sospeso o in corso di esportazione dei lavori per cliente	Ogni regione supportata: 20	No	Il numero massimo di lavori di esportazione del pubblico in sospeso/in corso per cliente
Lavori di generazione di audience in sospeso/in corso per cliente	Ogni regione supportata: 10	Sì	Il numero massimo di lavori di generazione di audience in sospeso/in corso per cliente
Modelli di audience in sospeso/in corso per cliente	Ogni regione supportata: 2	Sì	Il numero massimo di lavori di formazione su modelli di audience in sospeso/in corso per cliente

Quote ML di Clean Rooms

Risorsa	Predefinito	Descrizione
Set di dati	per lavoro	
Numero massimo di interazioni	20 miliardi	Numero massimo di interazioni consentite nei dati di allenamento. Gli input più grandi vengono campionati.
Numero minimo di interazioni	1 milione	
Numero massimo di utenti distinti per la formazione su modelli simili	1 milione	Se ne vengono inclusi altri, vengono utilizzati solo i primi 100 milioni, classificati in base al numero di interazioni.

Risorsa	Predefinito	Descrizione
Numero minimo di utenti distinti per la formazione di modelli simili	100.000	
Numero massimo di utenti per un lavoro in segmenti (audience) simili all'esportazione	10.000	
Numero massimo di elementi distinti utilizzati per l'addestramento dei modelli.	1 milione	È possibile includere fino a 50 milioni di articoli, ma viene utilizzato solo il milione più popolare.
Numero massimo di colonne di funzionalità nel set di dati di addestramento.	10	
Numero minimo di elementi distinti per utente	2	AWS Clean Rooms ML richiede che ogni riga o utente abbia due o più elementi, inclusi gli elementi ripetuti.
Dimensione massima del pubblico iniziale	500.000	
Dimensione minima del pubblico iniziale	500	Il fornitore dei dati di formazione può impostare questo valore a partire da 25.
API	per cliente	
Numero totale di set di dati di formazione attivi	500	
Numero totale di modelli sosia attivi (modelli di audience)	500	

Risorsa	Predefinito	Descrizione
Numero totale di modelli simili configurati attivi (modelli di audience)	10.000	
Numero totale di lavori completati per la generazione di segmenti simili (pubblico)	Nessun limite	
Numero totale di lavori completati nel segmento (pubblico) somigliante all'esportazione	Nessun limite	
Durata massima del lavoro di generazione di un modello simile (modello di audience)	1 giorno (24 ore)	
Durata massima della generazione di un lavoro simile a un segmento (pubblico)	10 ore	Dopo aver fornito un seme, Clean Rooms ML impiega un massimo di 10 ore per generare un segmento simile.
Percentuale minima per un contenitore delle dimensioni di un segmento (pubblico)	1%	
Percentuale massima per un contenitore delle dimensioni di un segmento (pubblico)	20%	
Dimensione minima assoluta per un contenitore delle dimensioni di un segmento (pubblico)	1% del numero di utenti distinti	

Risorsa	Predefinito	Descrizione
Dimensione massima assoluta per un contenitore delle dimensioni di un segmento (pubblico)	20% del numero di utenti distinti	

Cronologia dei documenti per la Guida per AWS Clean Rooms l'utente

La tabella seguente descrive le versioni della documentazione per AWS Clean Rooms.

Per ricevere notifiche sugli aggiornamenti della documentazione, puoi sottoscrivere il feed RSS. Per sottoscrivere gli aggiornamenti RSS, è necessario che un plug-in RSS sia abilitato per il browser in uso.

Modifica	Descrizione	Data
Aggiornamento alla politica esistente	La seguente nuova autorizzazione è stata aggiunta alla politica `AWSCleanRoomsFullAccessNoQuerying` gestita:`cleanrooms:BatchGetSchemaAnalysisRule` .	13 maggio 2024
AWS Clean Rooms ML è ora completamente disponibile	AWS Clean Rooms L'apprendimento automatico offre a due parti un metodo di miglioramento della privacy per identificare utenti simili nei propri dati senza la necessità di condividerli tra loro.	3 aprile 2024
Aggiornamento alla politica esistente	Lo Statement ID nella policy `AWSCleanRoomsFullAccess` gestita è stato aggiornato da ConsolePickQueryResultsBucket SetQueryResultsBucket a per rappresentare meglio le autorizzazioni successive alle autorizzazioni.	21 marzo 2024

Nuove politiche gestite per il machine learning AWS Clean Rooms	Sono state aggiunte due nuove politiche gestite: `AWSCleanRoomsMLReadOnlyAccess` e `AWSCleanRoomsMLFullAccess` .	29 novembre 2023
AWS Clean Rooms ML (anteprima)	AWS Clean Rooms ML offre a due parti un metodo di miglioramento della privacy per identificare utenti simili nei propri dati senza la necessità di condividerli tra loro.	29 novembre 2023
AWS Clean Rooms Privacy differenziale (anteprima)	I clienti possono ora utilizzare AWS Clean Rooms Differential Privacy per proteggere la privacy dei propri utenti.	29 novembre 2023
Configurazione dei pagamenti	L'autore della collaborazione può ora configurare il membro che può eseguire le query o un altro membro della collaborazione a cui fatturare i costi di elaborazione delle query.	14 novembre 2023
Tempo di esecuzione della query: aggiornamento	La durata massima di esecuzione di una query prima del timeout è stata aggiornata da 4 ore a 12 ore.	6 ottobre 2023

AWS CloudFormation risorse: aggiorna	AWS Clean Rooms ha aggiunto le seguenti nuove risorse: `AWS::CleanRooms::MembershipProtectedQueryOutputConfiguration` `AWS::CleanRooms::MembershipProtectedQueryResultConfiguration` , `eAWS::CleanRooms::MembershipProtectedQueryS3OutputConfiguration` .	7 settembre 2023
AWS CloudFormation risorse: aggiorna	AWS Clean Rooms ha aggiunto le seguenti nuove risorse: `AWS::CleanRooms::AnalysisTemplate` `eAWS::CleanRooms::ConfiguredTable AnalysisRuleCustom` .	31 agosto 2023
Abilità separate dei membri	L'autore della collaborazione può ora designare un membro come membro che può eseguire le interrogazioni e un altro membro come membro che può ricevere i risultati. Ciò offre al creatore della collaborazione la possibilità di assicurarsi che il membro che può eseguire la query non abbia accesso ai risultati della query.	30 agosto 2023

AWS Clean Rooms Glossario	Aggiornamento della sola documentazione per aggiungere un glossario di termini. AWS Clean Rooms	30 agosto 2023
Support per Apache Iceberg tabelle (anteprima)	AWS Clean Rooms ora supporta Apache Iceberg le tabelle (anteprima).	25 agosto 2023
Aggiornamento delle quote	La sezione Quote è stata aggiornata per riflettere la nuova quota predefinita per le iscrizioni per account.	9 agosto 2023
Aggiornamento alla politica esistente	Le seguenti nuove autorizzazioni sono state aggiunte alla politica `AWSCleanRoomsFullAccessNoQuerying` gestita:`cleanrooms:CreateAnalysisTemplate` ,`cleanrooms:GetAnalysisTemplate` ,`cleanrooms:UpdateAnalysisTemplate` , `cleanrooms:DeleteAnalysisTemplate` ,`cleanrooms:ListAnalysisTemplates` , `cleanrooms:GetCollaborationAnalysisTemplate` `cleanrooms:BatchGetCollaborationAnalysisTemplate` , e `cleanrooms:ListCollaborationAnalysisTemplates` .	31 luglio 2023

Modelli di analisi e regola di analisi personalizzata	AWS Clean Rooms ora supporta i modelli di analisi e la regola di analisi personalizzata. I modelli di analisi consentono ai collaboratori di creare o importare la propria query SQL personalizzata da utilizzare nella collaborazione. Con la regola di analisi personalizzata, il proprietario della tabella può approvare le query SQL personalizzate sulle tabelle configurate.	31 luglio 2023
Le regole di analisi supportano la condizione logica OR	AWS Clean Rooms le regole di analisi ora supportano la condizione OR logica nella JOIN clausola.	29 giugno 2023
CloudFormation integrazione	AWS Clean Rooms ora si integra con AWS CloudFormation.	15 giugno 2023
Generatore di analisi	I membri che possono eseguire query e ricevere risultati ora hanno la possibilità di eseguire query su alcune tabelle senza scrivere codice SQL utilizzando l'interfaccia utente di Analysis Builder.	15 giugno 2023
Funzioni SQL	Aggiornamento della sola documentazione per chiarire le funzioni SQL supportate.	5 maggio 2023

Risoluzione dei problemi	Aggiornamento della sola documentazione per aggiungere una sezione Risoluzione dei problemi comuni.	27 aprile 2023
Tipi di dati supportati per AWS Clean Rooms	Aggiornamento della sola documentazione per aggiungere una nuova sezione che elenca i tipi di dati supportati AWS Glue Data Catalog .	26 aprile 2023
Esempi di AWS CloudTrail eventi	Aggiornamento della sola documentazione per aggiungere esempi di CloudTrail eventi relativi a StartProtectedQuery (successo) e StartProtectedQuery (fallimento).	20 aprile 2023
Aggiornamento alla politica esistente	Le seguenti nuove autorizzazioni sono state aggiunte alla politica `AWSCleanRoomsFullAccessNoQuerying` gestita: `cleanrooms:ListTagsForResource` `cleanrooms:UntagResource` , `ecleanrooms:TagResource` . Per ulteriori informazioni, consulta le politiche AWS gestite.	21 marzo 2023
Disponibilità generale	AWS Clean Rooms è ora disponibile a livello generale.	21 marzo 2023

Versione di anteprima	Versione di anteprima della Guida AWS Clean Rooms per l'utente	12 gennaio 2023

AWS Clean Rooms Glossario

Consulta questo glossario per acquisire familiarità con la terminologia utilizzata per. AWS Clean Rooms

Regola di analisi dell'aggregazione

La restrizione delle query che consente di eseguire query che aggregano analisi utilizzando o AVG funzioni COUNT lungo SUM dimensioni opzionali. Queste interrogazioni non riveleranno informazioni a livello di riga.

Supporta casi d'uso come la pianificazione delle campagne, la copertura dei media, la frequenza e la misurazione delle conversioni.

Altri tipi di regole di analisi sono personalizzate ed elenchi.

Regole di analisi

Le restrizioni relative alle interrogazioni che autorizzano un tipo specifico di interrogazione.

Il tipo di regola di analisi determina il tipo di analisi che può essere eseguito sulla tabella configurata. Ogni tipo ha una struttura di interrogazione predefinita. Puoi controllare come le colonne della tabella possono essere utilizzate nella struttura tramite i controlli di interrogazione.

I tipi di regole di analisi sono aggregazione, elenco e personalizzazione.

Modello di analisi

Una query preapprovata specifica per la collaborazione che può essere riutilizzata.

Supporta le query SQL personalizzate supportate in. AWS Clean Rooms

Può contenere parametri ovunque in genere un valore letterale possa apparire in una query SQL. Per ulteriori informazioni sui tipi di parametri supportati, vedere Tipi di dati nel riferimento AWS Clean Rooms SQL.

I modelli di analisi funzionano solo con la regola di analisi personalizzata.

Client di crittografia C3R

Il client di crittografia Cryptographic Computing for Clean Rooms (C3R).

Utilizzato per crittografare e decrittografare i dati, C3R è un SDK di crittografia lato client con un'interfaccia a riga di comando.

Colonna Cleartext

Una colonna che non è protetta crittograficamente né per un JOIN costrutto SQL. SELECT

Le colonne Cleartext possono essere utilizzate in qualsiasi parte della query SQL.

Collaborazione

Un limite logico sicuro AWS Clean Rooms in cui i membri possono eseguire query SQL su tabelle configurate.

Le collaborazioni vengono create dal creatore della collaborazione.

Solo i membri che sono stati invitati alla collaborazione possono aderire alla collaborazione.

Una collaborazione può avere un solo membro che può interrogare i dati, un membro che può ricevere risultati e un membro che paga i costi di elaborazione delle query.

Tutti i membri possono visualizzare l'elenco dei partecipanti invitati alla collaborazione prima di aderire alla collaborazione.

Creatore di collaborazioni

Il membro che crea una collaborazione.

Esiste un solo creatore di collaborazione per collaborazione.

Solo l'autore della collaborazione può rimuovere membri dalla collaborazione o eliminare la collaborazione.

Tabella configurata

Ogni tabella configurata rappresenta un riferimento a una tabella esistente in AWS Glue Data Catalog quella che è stata configurata per l'uso in. AWS Clean Rooms Una tabella configurata contiene una regola di analisi che determina come i dati possono essere utilizzati.

Attualmente, AWS Clean Rooms supporta l'associazione di dati archiviati in Amazon Simple Storage Service (Amazon S3) tramite cui sono catalogati. AWS Glue

Per ulteriori informazioni in merito AWS Glue, consulta la Developer Guide AWS Glue .

Le tabelle configurate possono essere associate a una o più collaborazioni.

> **Note**
>
> AWS Clean Rooms attualmente non supporta le bucket location di Amazon S3 registrate con. AWS Lake Formation

Regola di analisi personalizzata

La restrizione delle query che consente un set specifico di query preapprovate (modelli di analisi) o consente un set specifico di account in grado di fornire query che utilizzano i dati dell'utente.

Supporta casi d'uso come l'attribuzione al primo tocco, le analisi incrementali e le analisi dell'audience.

Supporta la privacy differenziale.

Decrittografia

Il processo di trasformazione dei dati crittografati nella loro forma originale. La decrittografia può essere eseguita solo se si ha accesso alla chiave segreta.

Privacy differenziale

Una tecnica matematicamente rigorosa che protegge i dati di collaborazione del membro che può ricevere risultati imparando a conoscere un individuo specifico.

Crittografia

Processo di codifica dei dati in un formato che appare casuale utilizzando un valore segreto chiamato chiave. È impossibile determinare il testo in chiaro originale senza accedere alla chiave.

Colonna di impronte digitali

Una colonna protetta crittograficamente per un JOIN costrutto SQL.

Regola di analisi degli elenchi

La restrizione delle interrogazioni che consente di eseguire interrogazioni che generano un'analisi degli attributi a livello di riga della sovrapposizione tra questa tabella e le tabelle del membro che può eseguire la query.

Supporta casi d'uso come l'arricchimento e la creazione o la soppressione dell'audience.

Membro

Un AWS cliente che partecipa a una collaborazione.

Un membro viene identificato utilizzando il proprio Account AWS.

Tutti i membri possono fornire dati.

Membro che può interrogare

Il membro che può interrogare i dati nella collaborazione.

Esiste un solo membro che può eseguire query per collaborazione e quel membro è immutabile.

Un utente amministrativo può utilizzare le autorizzazioni AWS Identity and Access Management (IAM) per controllare quali dei suoi principali IAM (come utenti o ruoli) possono interrogare i dati nell'ambito della collaborazione. Per ulteriori informazioni, consulta Creare un ruolo di servizio per leggere i dati.

Membro che può ricevere risultati

Il membro che può ricevere i risultati delle interrogazioni. Il membro che può ricevere risultati specifica le impostazioni dei risultati delle query per la destinazione Amazon S3 e il formato dei risultati della query.

C'è solo un membro che può ricevere risultati per collaborazione e quel membro è immutabile.

Il socio paga i costi di elaborazione delle query

Il membro responsabile del pagamento dei costi di elaborazione delle query.

Esiste un solo membro responsabile del pagamento dei costi di elaborazione delle query per collaborazione e tale membro è immutabile.

Se l'autore della collaborazione non ha specificato nessuno come membro che paga i costi di elaborazione delle query, il membro che può effettuare le query è il pagatore predefinito.

Il membro che paga i costi di elaborazione delle query riceve una fattura per le query eseguite nell'ambito della collaborazione.

Appartenenza

Una risorsa creata quando un membro entra a far parte di una collaborazione.

Tutte le risorse che il membro associa a una collaborazione fanno parte dell'appartenenza o sono associate all'appartenenza.

Solo il membro proprietario dell'iscrizione può aggiungere, rimuovere o modificare le risorse in quell'iscrizione.

Colonna sigillata

Una colonna protetta crittograficamente per un costrutto SELECT SQL.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.