使用者指南

AWS Clean Rooms

AWS Clean Rooms: 使用者指南

Table of Contents

什麼是 AWS Clean Rooms？

AWS Clean Rooms 協助您和您的合作夥伴分析您的集體資料集並共同作業，以獲得新的見解，而不會彼此透露基礎資料。您可以使用 AWS Clean Rooms一個安全的協作工作區，在幾分鐘內建立自己的潔淨室，只需幾個步驟即可開始分析您的集體資料集。您可以選擇要與之共同作業的合作夥伴、選取他們的資料集，以及為參與者設定限制。

使用 AWS Clean Rooms，您可以與已經在使用的數千家公司進行協作 AWS。共同作業不需要將資料移出 AWS 或載入其他平台。當您執行查詢時，會從其原始位置 AWS Clean Rooms 讀取資料，並套用內建的分析規則，協助您維持對其資料的控制權。

AWS Clean Rooms 提供您可以設定的內建資料存取控制和稽核支援控制。這些控制項包括：

- 用於限制 SQL 查詢並提供輸出限制的分析規則
- 加密計算，即Clean Rooms使在處理查詢時也能保持數據加密，以遵守嚴格的數據處理政策
- 查詢記錄以檢閱查詢並協助支援稽核
- 微分隱私，以防止用戶識別嘗試。 AWS Clean Rooms 差分隱私是一項完全管理的功能，透過數學支援的技術和直覺式控制項，只要按幾下滑鼠即可套用，保護使用者隱私。
- AWS Clean Rooms ML 允許雙方在他們的數據中識別相似的用戶，而無需彼此共享他們的數據。第一方從訓練資料建立並設定相似模型。第二方將其種子資料帶入共同作業，並建立類似於訓練資料的相似區段。

下面的視頻解釋了更多關於 AWS Clean Rooms.

AWS Clean Rooms

您是第一次 AWS Clean Rooms 使用嗎？

如果您是第一次使用的使用者 AWS Clean Rooms，建議您先閱讀下列章節：

- 如何 AWS Clean Rooms 工作
- 存取 AWS Clean Rooms
- 設定 AWS Clean Rooms
- AWS Clean Rooms 詞彙表

如何 AWS Clean Rooms 工作

下列工作流程假設：

- 協作成員已將其資料表上傳到 Amazon S3，並建立了一個資料 AWS Glue 表。
- (選擇性) 僅針對加密資料表，協同作業成員已使用 C3R 加密用戶端準備加密資料表。

總而言之，的工作 AWS Clean Rooms 流程如下：

1. 協同合作建立者會執行下列任務：
   - 建立協同合作。
   - 邀請一個或多個成員加入協同合作。
   - 指定能力給成員，例如可以查詢的成員以及可以接收結果的成員。

     如果協同合作建立者也是可以接收結果的成員，則他們會指定查詢結果目的地和格式。他們還提供服務角色 Amazon 資源名稱 (ARN)，將結果寫入查詢結果目的地。
   - 設定負責在協同作業中支付查詢運算成本的成員。
2. 受邀的成員透過建立成員資源來加入協同合作。

   如果受邀的成員是可以接收結果的成員，則他們會指定查詢結果目的地和格式。它們也提供服務角色 ARN，以寫入查詢結果目的地。

   如果受邀成員是負責支付查詢運算費用的成員，則他們在加入協同合作之前接受其付款責任。
3. 成員會設定現有的 AWS Glue 表格，以便在中使用。 AWS Clean Rooms(除非使用密碼編譯運算，否則您可以在加入協同作業之前或之後完成此步驟Clean Rooms。)

   > **Note**
   >
   > AWS Clean Rooms 支持 AWS Glue 表。如需取得資料的詳細資訊 AWS Glue，請參閱步驟 3：將您的資料表上傳到 Amazon S3。

   1. 成員會命名已配置的表格，並選擇要在協同合作中使用哪些欄。
   2. 成員將下列其中一個分析規則配置為已配置的表格：
      - 彙總分析規則或清單分析規則 — 控制可在表格上執行的分析類型。

- 自訂分析規則 — 允許一組特定的預先核准查詢或可提供使用您資料之查詢的特定帳戶集。允許成員開啟差異隱私，以防止使用者識別嘗試。

> **Note**
>
> 成員可以在將其已配置的表格與協同合作產生關聯之前，隨時配置分析規則。

4. 成員會將其已配置的表格與協同合作產生關聯，並 AWS Clean Rooms 提供服務角色以存取其 AWS Glue 表格。

> **Note**
>
> 此服務角色具有資料表的權限。只有代表可以查詢的成員執行 AWS Clean Rooms 允許的查詢，才能確定服務角色。任何協同作業成員 (資料擁有者除外) 都無法存取協同合作中的基礎資料表。資料擁有者可以開啟差異隱私權，使其資料表可供其他成員查詢。

5. 可以查詢的成員會在已設定的資料表上執行 SQL 查詢。

   只有在負責支付查詢計算成本的成員已加入協同作業為作用中成員時，才能執行查詢。

   系統會自動強制執行分析規則和輸出限制。 AWS Clean Rooms 僅傳回符合步驟 3.b 中定義的分析規則的結果。

   對於有關加密數據的查詢，可以接收結果的成員必須從中接收加密 AWS Clean Rooms 的輸出進行解密（請參閱步驟 8）。

6. 可以收到結果的成員會在他們指定的 AWS Clean Rooms 主控台或 Amazon S3 儲存貯體中檢閱結果。
7. 支付查詢運算費用的成員會針對在協同合作中執行的查詢收費。
8. (選擇性) 僅針對加密資料表，可接收結果的成員會以解密模式執行 C3R 加密用戶端來解密查詢結果。

相關服務

以下 AWS 服務 是與之相關的 AWS Clean Rooms：

- Amazon Simple Storage Service (Amazon S3)

  協同合作成員可以存放他們 AWS Clean Rooms 在 Amazon S3 中引入的資料。

如需詳細資訊，請參閱下列主題：

準備查詢的資料表 AWS Clean Rooms

什麼是 Amazon S3？ 在 Amazon 簡單存儲服務用戶指南

- AWS Glue

  協同合作成員可以從 Amazon S3 中的資料建立 AWS Glue 表格，以便在中使用 AWS Clean Rooms。

  如需詳細資訊，請參閱下列主題：

  準備查詢的資料表 AWS Clean Rooms

  《AWS Glue 開發人員指南》中的什麼是 AWS Glue？

- AWS CloudFormation

  在中建立下列資源 AWS CloudFormation：協同作業、已設定的表格、已設定的表格關聯以及成員資格

  如需詳細資訊，請參閱 建立 AWS Clean Rooms 資源 AWS CloudFormation。

- AWS CloudTrail

  AWS Clean Rooms 搭配 CloudTrail 記錄使用可增強您對 AWS 服務 活動的分析。

  如需詳細資訊，請參閱 使用 AWS CloudTrail 記錄 AWS Clean Rooms API 呼叫。

存取 AWS Clean Rooms

您可以通 AWS Clean Rooms 過以下選項訪問：

- 直接通過 AWS Clean Rooms 控制台 https://console.aws.amazon.com/cleanrooms/.
- 以編程方式通過 AWS Clean Rooms API。如需詳細資訊，請參閱 AWS Clean Rooms API 參考。

定價 AWS Clean Rooms

如需定價資訊，請參閱 AWS Clean Rooms 定價。

帳單 AWS Clean Rooms

AWS Clean Rooms 讓共同作業建立者能夠設定要支付共同作業中查詢運算成本的成員。

在大多數情況下，可以查詢的成員和支付查詢計算費用的成員是相同的。但是，如果可以查詢的成員和支付查詢運算成本的成員不同，則當可以查詢的成員針對自己的成員資格資源執行查詢時，會向支付查詢計算費用的成員資格資源計費。

支付查詢計算費用的成員不會在其事件歷史記錄中看到執行查詢的任何 CloudTrail 事件，因為付款人既不是執行查詢的人，也不是執行查詢的資源擁有者。不過，付款人確實會看見其成員資格資源上所產生的帳單，以查看可在協同作業中執行查詢的成員所執行的所有查詢。

如需如何建立協同作業及設定支付查詢計算成本的成員的詳細資訊，請參閱建立協同合作。

分析規則 AWS Clean Rooms

協同合作成員必須配置分析規則，在中啟用表格以用 AWS Clean Rooms 於協同合作分析的一部分。

分析規則是每個資料擁有者在已設定資料表上設定的隱私權增強控制項。分析規則決定如何分析已配置的表格。

分析規則是已配置表格 (帳戶層級資源) 上的帳戶層級控制項，且會在與已配置表格相關聯的任何協同作業中強制執行。如果未設定分析規則，則配置的資料表可以與協同合作產生關聯，但無法查詢。查詢只能參考具有相同分析規則類型的已配置表格。

若要配置分析規則，請先選取分析類型，然後指定分析規則。對於這兩個步驟，您都應該考慮要啟用的使用案例以及要如何保護基礎資料。

AWS Clean Rooms 針對查詢中參照的所有已設定資料表強制執行限制性較高的控制項。

下列範例說明限制性控制項。

Example 限制性控制：輸出約束

- 協同合作者 A 在識別碼欄上有 100 個輸出限制。
- 協同合作者 B 在識別碼資料行上有 150 個輸出限制。

  參考這兩個設定資料表的彙總查詢需要在輸出資料列內至少 150 個不同的識別工具值，才能在查詢輸出中顯示。查詢輸出不表示因為輸出限制而移除結果。

Example 限制性控制：分析範本未核准

- 協同合作者 A 已允許包含查詢的分析範本，該範本會在其自訂分析規則中參照「協同作業者 A」和「協同合作者 B」的已設定表格。
- 協作者 B 不允許使用分析範本。

  由於 Collaborator B 不允許使用分析範本，因此可以查詢的成員無法執行該分析範本。

分析規則類型

分析規則有三種類型：彙總、清單和自訂。下表比較分析規則類型。每種類型都有一個單獨的部分，用於描述指定分析規則。

下表顯示分析規則類型的比較摘要。

支援的使用案例

下表顯示每種分析規則類型支援使用案例的比較摘要。

使用案例	聚合	清單	Custom (自訂)
支援的分析	使用 COUNT、SU 和 AVG 函數沿可選維度彙總統計資料的查詢	輸出多個表之間重疊的行級列表的查詢	任何自訂分析，只要分析範本或分析建立者已經過審核並允許
常見使用案例	區段分析、測量、歸因	豐富、區段建立	首次接觸歸因、增量分析、受眾探索
SQL 建構	• JOIN 語句：內部加入 • 彙總函數：計數/計數不同、總和/總和不同，以及 AVG • 標量函數：有限子集	• JOIN 語句：內部加入 • 標量函數：無	SELECT 命令提供的大多數 SQL 函數和 SQL 建構

使用案例	聚合	清單	Custom (自訂)
子查詢和一般資料表運算式 (CTE)	否	否	是
分析模板	否	否	是

支持的控件

下表顯示每個分析規則類型如何保護基礎資料的比較摘要。

控制項	聚合	清單	Custom (自訂)
控制機制	控制如何在查詢中使用資料表中的資料 （例如，允許具有電子郵件列的計數和總和。）	控制如何在查詢中使用資料表中的資料 （例如，只允許使用列 hashed_email 進行加入。）	控制允許在資料表上執行哪些查詢 (例如，僅允許在分析範本「自訂查詢 1」中定義的查詢。)
內建隱私增強技術	• 盲匹配 • 需要彙總 • 最小聚合閾值 >= • 2 預定義的查詢結構	• 盲匹配 • 需要重疊 • 預定義查詢結構	微分隱私

控制項	聚合	清單	Custom (自訂)
檢閱查詢，然後才能執行	否	否	是，使用分析範本

如需有關中可用分析規則的詳細資訊 AWS Clean Rooms，請參閱下列主題。

- 彙總分析規則
- 清單分析規則
- 自訂分析規則 AWS Clean Rooms

彙總分析規則

在中AWS Clean Rooms，彙總分析規則會使用 COUNT、SUM 和/或 AVG 函數沿選用維度來產生彙總統計資料。將彙總分析規則新增至已設定的資料表時，可讓查詢的成員在已設定的資料表上執行查詢。

彙總分析規則支援宣傳活動規劃、媒體觸及率、頻率測量和歸因等使用案例。

支援的查詢結構和語法在中定義聚合查詢結構和語法。

中彙總分析規則-查詢控制項定義的分析規則參數包括查詢控制項和查詢結果控制項。其查詢控制項包括要求將已設定的資料表連結至少一個由成員擁有的已設定資料表，這些資料表可以直接或傳輸進行查詢。此要求允許您確保查詢在您的表和他們的交叉點 (INNERJOIN) 上運行。

聚合查詢結構和語法

對具有彙總分析規則的資料表進行查詢，必須遵循下列語法。

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

下表說明上述語法中列出的每個運算式。

表達式	定義	範例
select_aggregate_function_expression	包含下列運算式的逗號分隔清單： • select_aggregation_function_expression • select_aggregate_expression **Note** 必須至少有一個select_aggregation_function_expression 在select_aggregate_expression .	SELECT SUM(PRICE), user_segment

表達式	定義	範例

select_aggregation_function_expression	套用至一或多個資料行的一或多個受支援的彙總函式。只有列被允許作為聚合函數的參數。
	
	Note
	必須至少有一個`select_aggregation_function_expression` 在`select_aggregate_expression` 。
		`AVG(PRICE)`
		
		`COUNT(DISTINCT user_id)`

select_grouping_column_expression	可以使用以下內容包含任何運算式的運算式：
	• 資料表欄位名稱
	• 支援的純量函數
	• 字符串文字
	• 数字文字
	
	Note
	`select_aggregate_expression` 可以使用或不帶AS參數的別名列。如需詳細資訊，請參閱 AWS Clean RoomsSQL 參考。
		`TRUNC(timestampColumn)`
		
		`UPPER(campaignName)`

表達式	定義	範例
table_expression	用來連接條件運算式的資料表或表格聯結join_condition 。 join_condition 返回一個布爾值。 支table_expression 持： • 特定JOIN類型（INNERJOIN ） • ajoin_condition （=）中的相等比較條件 • 邏輯運算子 (AND、OR)。	FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2
where_expression	傳回布林值的條件運算式。它可能由以下內容組成： • 資料表欄位名稱 • 支援的純量函數 • 數學運算子 • 字符串文字 • 數字文字 支援的比較條件為 (=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL)。 支援的邏輯運算子為 (AND, OR)。 where_expression 是選擇性的。	WHERE where_condition WHERE price > 100 WHERE TRUNC(timestampColumn) = '1/1/2022' WHERE timestampColumn = timestampColumn2 - 14

表達式	定義	範例
group_by_expression	以逗號分隔的運算式清單，符合的需求。select_grouping_column_expression	GROUP BY TRUNC(timestampColumn), UPPER(campaignName), segment
having_expression	傳回布林值的條件運算式。它們具有套用至單一資料行的支援彙總函式 (例如，SUM(price))，並與數字常值進行比較。 支援的條件為 (=, >, <, <=, >=, <>, !=)。 支援的邏輯運算子為 (AND, OR)。 having_expression 是選擇性的。	HAVING SUM(SALES) > 500

表達式	定義	範例
order_by_expression	以逗號分隔的運算式清單，與先前定義的相同需求相容。select_aggregate_expression order_by_expression 是選擇性的。 **Note** order_by_expression 許可證ASC和DESC參數。如需詳細資訊，請參閱《AWS Clean RoomsSQL 參考資料》中的 ASC 描述參數。	ORDER BY SUM(SALES), UPPER(campaignName)

對於彙總查詢結構和語法，請注意下列事項：

- 不支援以外SELECT的其他 SQL 指令。
- 不支援子查詢和一般資料表運算式 (例如WITH)。
- 不支援合併多個查詢的運算子 (例如，UNION)。
- TOPLIMIT、和OFFSET參數不受支援。

彙總分析規則-查詢控制項

使用彙總查詢控制項，您可以控制如何使用資料表中的資料行來查詢資料表。例如，您可以控制哪個資料行用於聯結、哪個資料行可以計算，或是哪個資料行可用於WHERE陳述式。

以下各節將說明每個控制項。

主題

- 彙總控制項
- 加入控制
- 標註控制
- 純量函數

彙總控制項

透過使用彙總控制項，您可以定義要允許哪些彙總函數，以及必須套用到哪些資料行。聚合函數可以在SELECT、HAVING和ORDERBY運算式中使用。

控制項	定義	用量
aggregateColumns	您允許在彙總函數中使用的已設定表格資料欄的資料欄。	aggregateColumns 可以在SELECT、HAVING和運算式中的彙總函ORDERBY式內使用。 有些也aggregate Columns 可以歸類為joinColumn (稍後定義)。 鑑於不aggregateColumn 能也被歸類為dimension Column （稍後定義）。
function	您允許在上方使用的計數、總和和和 AVG 函數aggregate Columns 。	function可套用至與其aggregateColumns 相關聯的。

加入控制

一個JOIN子句用於從兩個或多個表，基於它們之間的相關列合併行。

您可以使用聯結控制項來控制如何將表格連接至中的其他表格table_expression。 AWS Clean Rooms僅支持INNERJOIN。 INNERJOIN陳述式只能使用已在分析規則joinColumn中明確分類為的欄 (視您定義的控制項而定)。

INNERJOIN必須joinColumn從您已配置的表格和協同作業joinColumn中另一個已配置的表格上進行操作。您可以決定表格中的哪些欄可用作joinColumn。

ON子句中的每個匹配條件都需要在兩列之間使用相等比較條件（=）。

條ON款中的多個比對條件可以是：

- 結合使用AND邏輯運算符
- 使用OR邏輯運算符分隔

> **Note**
>
> 所有JOIN符合條件都必須符合每一側的一列JOIN。由OR或AND邏輯運算子連接的所有條件也必須遵守此要求。

以下是具有AND邏輯運算子的查詢範例。

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

以下是具有OR邏輯運算子的查詢範例。

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

控制項	定義	用量
joinColumns	您要允許查詢的成員在INNERJOIN陳述式中使用的資料欄 (如果有的話)。	特定的也joinColumn 可以歸類為 aggregateColumn （請參閱彙總控制項)。 同一列不能同時用作joinColumn 和dimensionColumns （請參閱稍後）。

控制項	定義	用量
		除非它也被歸類為aggregateColumn ，否則 a 不joinColumn 能在查詢的任何其他部分中使用INNERJOIN。
joinRequired	控制您是否需要INNERJOIN來自可查詢之成員的已設定資料表。	如果啟用此參數，INNERJOIN則需要。如果您未啟用這個參數，則 a INNER JOIN 是選擇性的。 假設您啟用此參數，則可以查詢的成員必須在中包含他們擁有的資料表INNERJOIN。他們必須將JOIN您的桌子與他們的桌子一起直接或傳遞（即將其表連接到另一個表格，該表本身已連接到您的桌子）。

以下是傳遞性的一個例子。

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

> **Note**
>
> 可以查詢的成員也可以使用joinRequired參數。在這種情況下，查詢必須將其資料表與至少一個其他資料表聯結。

標註控制

維度控制項會控制可篩選、分組或彙總彙總資料欄的資料欄。

控制項	定義	用量
dimensionColumns	您允許查詢的成員在 SELECT、WHERE、和中使用的欄 (如果有的話) ORDER BY。GROUP BY	A dimensionColumn 可以在 SELECT (select_grouping_column_expression)、WHEREGROUPBY、和中使用 ORDERBY。 相同的資料行不能同時是 a dimensionColumn joinColumn 、a 和/或aggregateColumn .

純量函數

純量函數控制哪些純量函數可以在維度列上使用。

控制項	定義	用量
scalarFunctions	可dimensionColumns 在查詢中使用的純量函數。	指定您允許 (例如) 套用的純量函數 (如果有的話CAST)。dimensionColumns 標量函數不能在其他函數之上或其他函數中使用。標量函數的參數可以是列，字符串文字或數字文字。

支援下列純量函數：

- 數學功能-ABS，天花板，地板，日誌，LN，圓形，SQRT
- 資料類型格式化函數 — CAST, CONVERT, TO_CHAR, TO_DATE, TO_NUMBER, TO_TIMESTAMP
- 字符串函數-下，上，修剪，RTRIM，子字符串
  - 對於 RTRIM，不允許要修剪的自定義字符集。

- 條件運算式 — 合併
- 日期函數-提取，獲取日期，當前日期，日期添加
- 其他功能 — TRUNC

如需詳細資訊，請參閱 AWS Clean RoomsSQL 參考。

彙總分析規則-查詢結果控制項

使用彙總查詢結果控制項，您可以指定每個輸出資料列必須符合才能傳回的一或多個條件，來控制要傳回的結果。 AWS Clean Rooms支援的形式的彙總限制COUNT (DISTINCT column) >= X。此表單要求每個資料列從已設定的資料表彙總至少 X 個不同選擇值 (例如，不同user_id值的最小數目)。即使提交的查詢本身並未使用指定的資料行，這個最小臨界值也會自動強制執行。它們會從協同合作中每個成員的已配置表格中，在查詢中的每個已配置表格中集體強制執行。

每個已配置的表格在其分析規則中必須至少有一個彙總條件約束。已配置的資料表擁有者可以新增多個columnNameminimum與相關聯的資料表擁有者，並

彙總約束

彙總條件約束可控制傳回查詢結果中的哪些資料列。若要傳回，資料列必須符合彙總條件約束中指定之每個資料行中不同值的指定最小數目。即使查詢或分析規則的其他部分未明確提及資料行，此需求也適用。

控制項	定義	用量
columnName	在每個輸出行必須滿足的條件下使用的。aggregate Column	可以是已配置表格中的任何欄。
minimum	要在查詢結果中傳回的輸出資料列必須具有的相關聯aggregateColumn 值的最小數目 (例如 COUNT DISTINCT)。	必minimum須至少為 2 的值。

彙總分析規則結構

下列範例顯示彙總分析規則的預先定義結構。

在下面的例子中，*MyTable*是指您的數據表。您可以使用自己的資訊取代每個*#########*。

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

彙總分析規則-範例

下面的例子演示了兩家公司如何AWS Clean Rooms使用聚合分析進行協作。

A 公司有客戶和銷售數據。A 公司有興趣了解產品退貨活動。B 公司是 A 公司的零售商之一，擁有退貨數據。B 公司還具有對 A 公司有用的客戶的節段屬性 (例如，已購買的相關產品，使用零售商的客戶服務)。B 公司不想提供資料列層級的客戶退貨資料和屬性資訊。B 公司只希望為 A 公司啟用一組查詢，以便以最小聚總閾值取得重疊客戶的彙總統計資料。

A 公司和 B 公司決定合作，以便 A 公司能夠了解產品退貨活動，並在 B 公司和其他渠道提供更好的產品。

若要建立協同作業並執行彙總分析，公司會執行下列動作：

1. 公司 A 會建立協同合作並建立成員資格。該合作將 B 公司作為合作中的另一個成員。公司 A 可在協同作業中啟用查詢記錄，並在其帳戶中啟用查詢記錄。
2. B 公司會在協同合作中建立成員資格。它會在其帳戶中啟用查詢記錄。

3. A 公司創建一個銷售配置表。

4. A 公司將以下彙總分析規則新增至銷售配置表格。

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

```
  ]
}
```

aggregateColumns— A 公司希望計算銷售數據和退貨數據之間重疊的獨特客戶數量。A 公司也希望總結所purchases做的數量比較的數量returns。

joinColumns— A 公司希望用identifier於將銷售數據中的客戶從退貨數據與客戶進行匹配。這將有助於 A 公司的比賽返回正確的購買。它還可以幫助 A 公司細分重疊客戶。

dimensionColumns— A 公司使用dimensionColumns按特定產品進行過濾，比較一段時間內的購買和退貨，確保退貨日期在產品日期之後，並幫助細分重疊的客戶。

scalarFunctions— 公司 A 選取CAST純量函數，以協助根據與協同作業相關聯的已配置表格 A 公司更新資料類型格式。如果需要，它還添加了標量函數，以幫助格式化列。

outputConstraints— A 公司設定最小輸出限制。它不需要限制結果，因為分析師可以從他們的銷售表中查看行級數據

> **Note**
>
> A 公司不包含joinRequired在分析規則中。它提供了靈活性，為他們的分析師單獨查詢銷售表。

5. B 公司會建立退貨組態表格。
6. B 公司將下列彙總分析規則新增至退貨配置表格中。

```
{
  "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— B 公司使 A 公司可returns以與購買數量進行總和。它們至少有一個彙總資料行，因為它們正在啟用彙總查詢。

joinColumns— B 公司使 A 公司能夠加入，從退貨數據identifier到客戶從銷售數據進行匹配。 identifier數據特別敏感，並將其作為joinColumn確保數據永遠不會在查詢中輸出。

joinRequired— B 公司要求退貨數據的查詢與銷售數據重疊。他們不想讓 A 公司查詢其資料集中的所有個人。他們在合作協議中也同意了這項限制。

dimensionColumns— 公司 B 可讓公司 A 篩選和分組依據statepopularpurchases、 ，而customerserviceuser這些屬性是可協助分析 A 公司 B 公司的唯一屬性，可讓公司 A 用returndate來篩選之後發生returndate的輸出purchasedate。透過此篩選，輸出可以更精確地評估產品變更的影響。

scalarFunctions— B 公司啟用以下項目：

- 主線日期
- 如果在其數據中以不同的格式輸入較低和 UPPER producttype
- CAST如果 A 公司需要將銷售中的數據類型轉換為與回報中的數據類型相同

A 公司不啟用其他標量函數，因為他們不認為查詢需要它們。

outputConstraints— B 公司設定最小輸出限制，hashedemail以協助降低重新識別客戶的能力。它還增加了最小輸出限制，producttype以減少重新識別退回的特定產品的能力。根據輸出的尺寸，某些產品類型可能更具主導地位（例如，state）。無論公司 A 向其數據添加的輸出約束如何，它們的輸出約束都將始終強制執行。

7. 公司 A 創建一個銷售表關聯協作。
8. B 公司會建立與協同合作的退貨表關聯。
9. A 公司運行查詢，例如以下示例，以更好地了解 B 公司的退貨數量與 2022 年按地點劃分的總採購量相比。

```
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;
```

10A 公司和 B 公司會複查查詢記錄。B 公司會驗證查詢是否符合合作協議中同意的內容。

疑難排解彙總分析規則問

使用此處的資訊可協助您診斷並修正使用彙總分析規則時的常見問題。

問題

- 我的查詢沒有返回任何結果

我的查詢沒有返回任何結果

當沒有相符結果，或符合結果不符合一或多個最小彙總閾值時，就會發生這種情況。

如需最小聚總臨界值的詳細資訊，請參閱彙總分析規則-範例。

清單分析規則

在中AWS Clean Rooms，清單分析規則會輸出其新增至的已配置資料表與可查詢之成員的已設定表格之間的重疊列層級清單。可以查詢的成員會執行包含清單分析規則的查詢。

清單分析規則類型支援使用案例，例如擴充和受眾建立。

如需有關此分析規則之預先定義的查詢結構和語法的詳細資訊，請參閱列出分析規則預先定義的。

中清單分析規則-查詢控制項定義的清單分析規則的參數具有查詢控制項。其查詢控制項包括選取可在輸出中列出的資料行的功能。查詢必須具有至少一個與可以直接或傳遞進行查詢的成員配置表格的聯結。

沒有像彙總分析規則一樣的查詢結果控制項。

清單查詢只能使用數學運算子。它們不能使用其他函數（例如聚合或標量）。

主題

- 列出查詢結構和語法
- 清單分析規則-查詢控制項

- 列出分析規則預先定義的
- 清單分析規則-範例

列出查詢結構和語法

對具有清單分析規則的資料表進行查詢，必須遵循下列語法。

```
--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]
```

下表說明上述語法中列出的每個運算式。

表達式	定義	範例
select_list_expression	包含至少一個表格資料欄名稱的逗號分隔清單。 DISTINCT參數是必需的。 **Note** select_list_expression 可以使用或不帶AS參數的別名列。 它還支持TOP參數。 如需詳細資訊，請	SELECT DISTINCT segment

表達式	定義	範例
	參閱 AWS Clean RoomsSQL 參考。	
table_expression	用join_condition 來連接到的表格或表格聯結join_condition 。 join_condition 返回一個布爾值。 支table_expression 持： • 一個特定的聯接類型（INNER連接） • ajoin_condition （=）中的相等比較條件 • 邏輯運算子 (AND、OR)。	`FROM consumer_table INNER JOIN provider_table ON consumer_table.identifier1 = provider_table.identifier1 AND consumer_table.identifier2 = provider_table.identifier2`

表達式	定義	範例

where_expression	傳回布林值的條件運算式。它可以由以下內容組成：
	• 資料表欄位名稱
	• 數學運算子
	• 字符串文字
	• 数字文字
	
	支援的比較條件為 (=, >, <, <=, >=, <>, !=, NOT, IN, NOT IN, LIKE, IS NULL, IS NOT NULL)。
	
	支援的邏輯運算子為 (AND, OR)。
	
	where_expression 是選擇性的。
		`WHERE state + '_' + city = 'NY_NYC'`
		
		`WHERE timestampColumn = timestampColumn2 - 14`

limit_expression	這個表達式必須採用正整數。它也可以與 TOP 參數進行交換。 limit_expression 是選擇性的。	`LIMIT 100`

對於清單查詢結構和語法，請注意下列事項：

- 不支援「選取」以外的 SQL 指令。
- 不支援子查詢和一般資料表運算式 (例如WITH)
- 不支援有GROUPBY、和訂單BY子句
- 不支援偏移參數

清單分析規則-查詢控制項

透過清單查詢控制項，您可以控制如何使用資料表中的資料行來查詢資料表。例如，您可以控制哪個資料行用於聯結，或哪個資料行可以在 SELECT 陳述式和WHERE子句中使用。

以下各節將說明每個控制項。

主題

加入控制

使用聯結控制項，您可以控制如何將資料表連接至 table_ expression 中的其他資料表。 AWS Clean Rooms僅支持INNER連接。在清單分析規則中，至少需要一個 INNER JOIN，且可以查詢的成員必須在 INNER JOIN 中包含自己擁有的資料表。這意味著他們必須直接或過渡地將您的桌子與他們的表加入。

以下是傳遞性的一個例子。

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

INNERJOIN 陳述式只能使用已在分析規則joinColumn中明確分類為的資料行。

INNERJOIN 必須在您已配置的表格和協同作業joinColumn中另一個已配置的表格上進行操作。joinColumn您可以決定表格中的哪些欄可用作joinColumn。

ON子句中的每個匹配條件都需要在兩列之間使用相等比較條件（=）。

ON子句中的多個匹配條件可以是：

- 結合使用AND邏輯運算符
- 使用OR邏輯運算符分隔

> **Note**
>
> 所有JOIN符合條件都必須符合每一側的一列JOIN。由OR或AND邏輯運算子連接的所有條件也必須遵守此要求。

以下是具有AND邏輯運算子的查詢範例。

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

以下是具有OR邏輯運算子的查詢範例。

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

控制項	定義	用量
`joinColumns`	您要允許查詢成員在 INNER JOIN 陳述式中使用的資料欄。	同一欄無法同時歸類為`joinColumn` 和 `listColumn` (請參閱清單控制項)。 `joinColumn` 不能用於 INNER JOIN 以外的查詢的任何其他部分。

清單控制項

清單控制項控制項可以列在查詢輸出中 (也就是 SELECT 陳述式中使用) 或用來篩選結果 (也就是說，在WHERE陳述式中使用) 的資料行。

控制項	定義	用量
`listColumns`	您允許可以查詢的成員在 SELECT 和中使用的欄 WHERE	A `listColumn` 可以在選擇和中使用WHERE。 同一列不能同時用作 `listColumn` 和`joinColumn` 。

列出分析規則預先定義的

下列範例包括顯示如何完成清單分析規則的預先定義結構。

在下面的例子中，*MyTable*是指您的數據表。您可以使用自己的資訊取代每個*#########*。

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

清單分析規則-範例

下面的例子演示了如何兩家公司可以AWS Clean Rooms使用列表分析進行協作。

A 公司擁有客戶關係管理（CRM）數據。A 公司希望獲得有關其客戶的其他細分數據，以了解有關其客戶的更多信息，並可能使用屬性作為其他分析的輸入。B 公司的區段資料包含他們根據其第一方資料建立的唯一區段屬性。B 公司只會針對其資料與 A 公司資料重疊的客戶，提供唯一的區段屬性給 A 公司。

公司決定合作，以便 A 公司可以豐富重疊的數據。A 公司是可以查詢的成員，B 公司是貢獻者。

要創建協作並在協作中運行列表分析，公司執行以下操作：

1. 公司 A 會建立協同合作並建立成員資格。該合作將 B 公司作為該合作的另一個成員。公司 A 可在協同作業中啟用查詢記錄，並在其帳戶中啟用查詢記錄。
2. B 公司會在協同合作中建立成員資格。它會在其帳戶中啟用查詢記錄。
3. A 公司創建一個 CRM 配置的表

4. 公司 A 會將分析規則新增至客戶設定的表格，如下列範例所示。

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

joinColumns— A 公司希望使用hashedemail和/或thirdpartyid（從身份供應商那裡獲得）將 CRM 數據中的客戶與客戶從細分數據匹配。這將有助於確保 A 公司為合適的客戶匹配豐富的數據。他們有兩個連接列可能提高分析的匹配率。

listColumns— A 公司用於獲listColumns得豐富的列旁邊internalid他們自己的系統中使用. 它們可customercategory以透過在篩選器中使用它們來新segment1增segment2、並可能將擴充限制到特定區段。

5. B 公司會建立區段設定的表格。
6. B 公司會將分析規則新增至區段設定的表格。

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

joinColumns— B 公司使 A 公司能夠加入，identifier2以將客戶從細分數據到 CRM 數據進行匹配。A 公司和 B 公司與身份供應商合作，以獲得identifier2與此次合作相匹配的產品。他們沒有添加其他標識符，joinColumns因為他們認為identifier2提供了最高和最準確的匹配率，並且查詢不需要其他標識符。

`listColumns`— B 公司使 A 公司能夠豐富他們的數據`segment3`和`segment4`屬性，這些屬性是他們創建，收集和對齊的唯一屬性（與客戶 A）成為數據豐富的一部分。他們希望 A 公司能夠在列層級取得這些重疊區段，因為這是資料豐富協同合作。

7. 公司 A 會建立與共同作業的 CRM 資料表關聯。
8. B 公司會建立與協同合作的區段表格關聯。
9. A 公司會執行查詢，例如下列查詢，以豐富重疊的客戶資料。

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

10A 公司和 B 公司會複查查詢記錄。B 公司會驗證查詢是否符合合作協議中同意的內容。

自訂分析規則 AWS Clean Rooms

在中 AWS Clean Rooms，自訂分析規則是一種新類型的分析規則，允許在已配置的表格上執行自訂查詢。自訂 SQL 查詢仍然僅限於只有`SELECT`命令，但可以使用比彙總和清單查詢更多的 SQL 建構 (例如，視窗函數、OUTER JOIN、CTE 或子查詢；如需完整清單，請參閱 AWS Clean Rooms SQL 參考)。自訂 SQL 查詢不必遵循彙總和清單查詢等查詢結構。

與彙總和清單分析規則支援的使用案例相比，自訂分析規則支援的使用案例更為進階，例如自訂歸因分析、基準測試、增量分析和受眾探索。這是彙總和清單分析規則所支援的使用案例的超集合之外。

自訂分析規則也支援差分隱私。差分隱私是數學上嚴格的數據隱私保護框架。如需詳細資訊，請參閱 AWS Clean Rooms 微分隱私。建立分析範本時，「 AWS Clean Rooms 差分隱私」會檢查範本，以判斷該範本是否與「 AWS Clean Rooms 差分隱私」的一般用途查詢結構相容。此驗證可確保您不會創建不允許使用差異隱私保護表格的分析模板。

若要設定自訂分析規則，資料擁有者可以選擇允許儲存在分析範本中的特定自訂查詢在其已設定的資料表上執行。資料擁有者先檢閱分析範本，然後再將其新增至自訂分析規則中允許的分析控制項。分析範本只能在建立分析範本的協同合作中使用且可見 (即使表格與其他協同合作相關聯)，且只能由可在該協同合作中查詢的成員執行。

或者，成員可以選擇允許其他成員 (查詢提供者) 建立查詢而不檢閱。成員會在自訂分析規則中新增允許查詢提供者控制的查詢提供者帳戶。如果查詢提供者是可以查詢的成員，則他們可以直接在已設定的資料表上執行任何查詢。查詢提供者也可以建立分析範本來建立查詢。查詢提供者所建立的任何查詢都會自動允許在資料表上執行，其中存在並與資料表相關聯的所有共同作業中。 AWS 帳戶

資料擁有者只能允許分析範本或帳戶建立查詢，而不能同時建立兩者。如果資料擁有者將其保留空白，則可以查詢的成員將無法在已設定的資料表上執行查詢。

主題

自訂分析規則預先定義的

下列範例包含預先定義的結構，說明如何在開啟差異隱私的情況下完成自訂分析規則。該`userIdentifier`值是唯一標識您的用戶的列，例如 user_id。如果您在協同作業中開啟了兩個或兩個以上的資料表，則 AWS Clean Rooms 需要您在兩個分析規則中設定與使用者識別碼欄相同的欄，以維持跨資料表的使用者定義一致。

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

您可擇一方法：

- 將分析範本 ARN 新增至允許的分析控制項。在這種情況下，不包括`allowedAnalysisProviders`控制項。

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

- 將成員 AWS 帳戶 ID 新增至控`allowedAnalysisProviders`制項。在這種情況下，您將添加`ANY_QUERY`到`allowedAnalyses`控制項。

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

自訂分析規則範例

以下範例示範兩家公司如何 AWS Clean Rooms 使用自訂分析規則進行協同作業。

A 公司有客戶和銷售數據。A 公司有興趣了解 B 公司網站上廣告活動的銷售增量。B 公司擁有對公司有用的收視數據和細分屬性（例如，他們在查看廣告時使用的設備）。

公司 A 有一個他們想要在協同合作中運行的特定增量查詢。

若要建立協同作業並在協同作業中執行自訂分析，公司會執行下列動作：

1. 公司 A 會建立協同合作並建立成員資格。該合作將 B 公司作為該合作的另一個成員。公司 A 可在協同作業中啟用查詢記錄，並在其帳戶中啟用查詢記錄。
2. B 公司會在協同合作中建立成員資格。它會在其帳戶中啟用查詢記錄。
3. A 公司創建一個 CRM 配置表
4. A 公司將空的自定義分析規則添加到銷售配置表中。
5. 公司 A 將銷售配置表格與協同合作產生關聯。
6. B 公司創建觀眾配置表。
7. B 公司會將空的自訂分析規則新增至觀眾人數設定的資料表。
8. B 公司會將觀眾人數設定表格與協同合作產生關聯。
9. 公司 A 會檢視與協同作業相關聯的銷售資料表和收視率表格，並建立分析範本，並新增促銷活動月份的增量查詢和參數。

```
{
    "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
       "
}
```

10A 公司會將其帳戶 (例如 444455556666) 新增至自訂分析規則中允許的分析提供者控制項。他們使用允許的分析提供程序控件，因為他們希望允許他們創建的任何查詢在其銷售配置的表上運行。

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

11B 公司會在協同合作中看到建立的分析範本，並檢閱其內容，包括查詢字串和參數。

12B 公司會判斷分析範本是否達到增量使用案例，並符合其隱私權要求，以瞭解如何查詢觀眾人數設定的資料表。

13B 公司會將分析範本 ARN 新增至觀眾人數表的自訂分析規則中允許的分析控制項。他們使用允許的分析控制項，因為他們只想允許增量查詢在其觀眾人數設定的資料表上執行。

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

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

14.公司 A 執行分析範本並使用參數值`05-01-2023`。

具有差分隱私的自訂分析規則

在中 AWS Clean Rooms，自訂分析規則支援差分隱私。差分隱私是數學上嚴格的數據隱私保護框架，可幫助您保護數據免受重新識別嘗試的侵害。

差分隱私支持聚合分析，例如廣告活動規劃， post-ad-campaign 衡量，金融機構聯盟中的基準測試以及醫療保健研究的 A/B 測試。

支援的查詢結構和語法在中定義查詢結構和語法。

具有差異隱私的自訂分析規則範例

考慮上一節中介紹的自訂分析規則範例。此範例示範如何使用差異隱私來保護資料免受重新識別嘗試的影響，同時讓合作夥伴從您的資料中學習關鍵業務洞察。假設擁有收視數據的 B 公司希望使用差分隱私來保護其數據。為了完成差分隱私設置，B 公司完成以下步驟：

1. B 公司開啟差異隱私，同時將自訂分析規則新增至觀眾人數設定的資料表。B 公司選擇`viewershipdata.hashedemail`作為用戶標識符列。
2. B 公司在協同合作中新增了差異隱私權政策，讓觀眾人數資料表可供查詢。B 公司會選取預設原則以快速完成設定。

想要瞭解 B 公司網站上廣告活動的銷售增量，A 公司會執行分析範本。由於查詢與 AWS Clean Rooms 差分隱私權的一般用途查詢結構相容，因此查詢會成功執行。

查詢結構和語法

至少包含一個已開啟差分隱私權的資料表的查詢必須遵循下列語法。

```
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**
>
> 對於差異隱私查詢結構和語法，請注意以下事項：
>
> - 不支援子查詢。
> - 如果資料表或 CTE 涉及受差分隱私保護的資料，通用資料表運算式 (CTE) 應該會發出使用者識別碼欄。過濾器，分組和聚合應在用戶級別完成。
> - 最終選擇允許計數不同，計數，總和，平均和和標準開發聚合函數。

如需差異隱私權支援哪些 SQL 關鍵字的詳細資訊，請參閱AWS Clean Rooms 差分隱私的 SQL 功能。

AWS Clean Rooms 微分隱私

AWS Clean Rooms 差分隱私可幫助您通過數學支持的技術保護用戶的隱私，該技術只需單擊幾下即可實現直觀的控件。作為完全託管的功能，不需要事先的差異隱私體驗來幫助您防止重新識別用戶。AWS Clean Rooms 在執行階段會自動新增經過仔細校準的雜訊量以查詢結果，以協助保護您的個人層級資料。

AWS Clean Rooms 差分隱私支援廣泛的分析查詢，非常適合各種使用案例，因為查詢結果中的少量錯誤不會影響您分析的實用性。有了它，您的合作夥伴就可以產生關於廣告活動、投資決策、臨床研究等的業務關鍵洞察，這一切都不需要您的合作夥伴進行額外的設定。

AWS Clean Rooms 差分隱私可防止溢出或無效的轉換錯誤，這些錯誤會以惡意方式使用標量函數或數學運算符符號。

如需 AWS Clean Rooms 差分隱私的相關資訊，請參閱下列主題。

主題

微分隱私

差分隱私僅允許匯總見解，並混淆任何個人數據在這些見解中的貢獻。差分隱私保護協作數據免受可以接收有關特定個人的結果的成員的協作數據。如果沒有差異隱私，可以接收結果的成員可以通過添加或刪除有關個人的記錄並觀察查詢結果的差異來嘗試推斷單個用戶數據。

開啟差分隱私時，會在查詢結果中加入指定數量的雜訊，以混淆個別使用者的貢獻。如果可以接收結果的成員在從資料集中移除個人的記錄後，嘗試觀察查詢結果中的差異，則查詢結果中的變異性有助於防止識別個人的資料。 AWS Clean Rooms 微分隱私使用採SampCert樣器，這是一種由開發的經過驗證的正確採樣器實現。 AWS

差分隱私的 AWS Clean Rooms 工作原理

在中開啟差分隱私的工作流程 AWS Clean Rooms 需要下列額外步驟，才能完成以下工作流程 AWS Clean Rooms：

1. 您可以在新增自訂分析規則時開啟差分隱私。
2. 您可以針對共同作業設定差異隱私權政策，讓您的資料表受到差異隱私保護，以供查詢。

完成這些步驟後，可以查詢的成員就可以開始對受隱私權保護的資料執行查詢。 AWS Clean Rooms 傳回符合差異隱私權政策的結果。 AWS Clean Rooms 「差分隱私」會追蹤您可以執行的估計剩餘查詢次數，類似於顯示汽車目前燃油水平的汽車中的氣體計。可以查詢的成員可以執行的查詢數目受到中設定的「隱私權」預算和「每個查詢新增的雜訊」參數的限制微分隱私政策。

考量事項

在中使用微分隱私時 AWS Clean Rooms，請考慮下列事項：

- 可以接收結果的會員無法使用差異隱私權。他們將配置自定義分析規則，並為其配置的表格關閉差分隱私。
- 可以查詢的成員無法聯結來自兩個或多個資料提供者的資料表時，兩者都已開啟差異隱私權。

微分隱私政策

差異隱私權原則可控制可以查詢的成員在共同作業中執行的彙總函式數目。隱私權預算會定義共同作業中套用所有資料表的共同有限資源。每次查詢新增的雜訊會控制隱私權預算耗盡的比率。

需要微分隱私政策才能使您的差異隱私保護表格可用於查詢。這是協同合作中的一次性步驟，包括兩個輸入：

- 隱私預算 — 根據 epsilon 進行量化，隱私預算控制了隱私保護的級別。這是一種常見的有限資源，適用於在協作中受到差異隱私保護的所有表格，因為其目標是保護用戶的隱私，其信息可以存在於多個表中。

  每次在資料表上執行查詢時，就會使用隱私權預算。當隱私權預算完全用盡時，在增加或重新整理之前，可以查詢的共同作業成員無法執行其他查詢。通過設置更大的隱私預算，可以接收結果的成員可以減少他們對數據中個人的不確定性。選擇隱私預算，以便在與業務決策者諮詢後，根據您的隱私需求來平衡您的協作需求。

如果您計劃定期將新資料納入共同作業，您可以選取「每月重新整理隱私權預算」，以便在每個日曆月自動建立新的隱私權預算。選擇此選項允許在重新整理期間重複查詢時，顯示有關資料列的任意數量資訊。如果在隱私權預算重新整理之間重複查詢相同的資料列，請避免選擇此選項。

- 每個查詢新增的雜訊是根據您想要隱藏其貢獻的使用者數量來衡量的。此值會控制隱私權預算耗盡的比率。較大的雜訊值會降低隱私權預算耗盡的比率，因此可以對您的資料執行更多查詢。但是，這應該與釋放不太準確的數據見解進行平衡。設定此值時，請考慮合作深入解析所需的準確性。

您可以使用預設的差分隱私權政策快速完成設定，或根據您的使用案例自訂您的差異隱私權政策。AWS Clean Rooms 差分隱私提供了直觀的控制來配置策略。 AWS Clean Rooms 「差分隱私」可讓您根據所有資料查詢中可能的彙總數量來預覽公用程式，並估計在資料共同作業中可執行的查詢數量。

您可以使用互動式範例來瞭解不同的隱私權預算和每個查詢新增的雜訊值會對不同類型 SQL 查詢的結果造成什麼影響。通常，您需要在隱私需求與要允許的查詢數量以及這些查詢的準確性之間取得平衡。較小的隱私權預算或每次查詢新增的雜訊可以更好地保護使用者隱私，但為您的協同合作夥伴提供較少意義的見解。

如果您增加隱私權預算，同時保持每個查詢新增的雜訊參數相同，則可以查詢的成員可以在共同作業中對您的資料表執行更多彙總。您可以在協同合作期間隨時增加隱私權預算。如果您降低隱私權預算，同時保持每個查詢新增的雜訊參數相同，則可以查詢的成員可以執行較少的彙總。在可以查詢的會員開始分析您的資料之後，您就無法降低隱私權預算。

如果您增加每個查詢新增的噪音，同時保持隱私權預算輸入相同，則可以查詢的成員可以在共同作業中對您的資料表執行更多彙總。如果您降低每個查詢新增的雜訊，同時保持隱私權預算輸入相同，則可以查詢的成員可以執行較少的彙總。您可以在協同合作期間隨時增加或減少每個查詢新增的雜訊。

差異隱私政策由隱私預算模板 API 操作管理。

AWS Clean Rooms 差分隱私的 SQL 功能

AWS Clean Rooms 差分隱私使用一般用途的查詢結構來支援複雜的 SQL 查詢。自訂分析範本會根據此結構進行驗證，以確保它們可以在受到差異隱私保護的資料表上執行。下表指出支援的功能。如需詳細資訊，請參閱查詢結構和語法。

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
彙總函數	• ANY_VALUE 函數 • APPROXIMATE PERCENTILE_DISC 函數 • AVG 函數 • 計數和計數不同的功能 • LISTAGG 函數 • MAX 函數 • MEDIAN 函數 • MIN 函數 • PERCENTILE_CONT 函數 • STDDEV_SAMP 和 STDDEV_POP 函數 • 總和和不同函數 • VAR_SAMP 和 VAR_POP 函數	支援使用差異隱私保護資料表的 CTE 必須產生具有使用者層級記錄的資料。您應該使用格式在那些 CTE 中寫入 SELECT 運算`SELECT userIdentifierColumn...' 式。	支持的聚合：AVG，計數，不同計數，標準開發和和。
CTE	與子句，WITH 子句子查詢	支援使用差異隱私保護資料表的 CTE 必須產生具有使用者層級記錄的資料。您應該使用格式在那些 CTE 中寫入 SELECT 運算`SELECT userIdentifierColumn...' 式。	N/A

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
子查詢	選擇列表子查詢，FROM 子句子查詢，WHERE 子句子查詢	不支援。不支援查詢中參考已開啟差分隱私權之資料表的子查詢。將子查詢重新撰寫為通用資料表運算式 (CTE)。	
聯結子句	• INNER JOIN • LEFT JOIN • RIGHT JOIN • 完全加入 • [加入] 或運算符 • CROSS JOIN	支援的條件是，只有在使用者識別碼欄上相等聯結的 JOIN 函數才會受到支援，而且在查詢兩個或多個已開啟差異隱私權的資料表時，此功能是強制性的。確保強制性的等值連接條件是正確的。確認資料表擁有者已在所有表格中設定相同的使用者識別碼欄，以便使用者的定義在各個資料表之間保持一致。 將兩個或多個關係與微分隱私相結合時，不支援 CROSS JOIN 功能。	
設定運算子	聯集，全部聯集，交集，除了 | 減號（這些是同義詞）	所有支持	不支援

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
範圍函數	彙總函數 • AVG 範圍函數 • COUNT 範圍函數 • CUME_DIST 範圍函數 • DENSE_RANK 範圍函數 • FIRST_VALUE 範圍函數 • LAG 範圍函數 • LAST_VALUE 範圍函數 • LEAD 範圍函數 • MAX 視窗功能 • 中值視窗函數 • 最小視窗功能 • NTH_VALUE 範圍函數 • RATIO_TO_REPORT 範圍函數 • 標準開發模式和流行視窗功能 (STDDEV_SAMP 和標準開發是同義字) • SUM 視窗函數 • VAR_SAMP 和 VAR_POP 視窗函數 (VAR_SAMP 和方差是同義字)	所有的支援條件是，當您查詢開啟差分隱私的關係時，必須使用 window 函數的 partition 子句中的使用者識別碼欄。	不支援

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
	排名函數 • DENSE_RANK 範圍函數 • NTILE 範圍函數 • PERCENT_RANK 範圍函數 • RANK 範圍函數 • ROW_NUMBER 範圍函數		
條件式運算式	• 案例條件表達式 • 合併表達 • GREATEST 和 LEAST 函數 • NVL 和 COALESCE 函數 • NVL2 函數 • NULLIF 函數	所有支持	所有支持
條件	• 比較條件 • 邏輯條件 • 模式比對條件 • 之間範圍條件 • Null 條件	EXISTS並且IN不能使用，因為它們需要子查詢。所有其他支持。	所有支持

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
日期時間函數	• 交易中日期與時間函數 • 連接運算符 • 增加月份函數 • CONVERT_TIMEZONE 函數 • CURRENT_DATE 函數 • DATEADD 函數 • DATEDIFF 函數 • 日期部分函數 • DATE_TRUNC 函數 • EXTRACT 函數 • GETDATE 函數 • 定時功能 • TO_TIMESTAMP 函數 • 日期或時間戳記函數的日期部分	所有支持	所有支持

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
字串函數	• || (連接) 運算符 • BTRIM 函數 • CHAR_LENGTH 函數 • CHARACTER _LENGTH 函數 • CHARINDEX 函數 • CONCAT 函數 • LEFT 和 RIGHT 函數 • LEN 函數 • LENGTH 函數 • LOWER 函數 • LPAD 和 RPAD 函數 • LTRIM 函數 • 位置功能 • REGEXP_COUNT 函數 • REGEXP_INSTR 函數 • REGEXP_RE PLACE 函數 • REGEXP_SUBSTR 函數 • REPEAT 函數 • REPLACE 函數 • REPLICATE 函數 • REVERSE 函數	所有支持	所有支持

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
	• RTRIM 函數 • SOUNDEX 函數 • SPLIT_PART 函數 • STRPOS 函數 • SUBSTRING 函數 • TEXTLEN 函數 • TRANSLATE 函數 • 修剪功能 • UPPER 函數		
資料類型格式化函數	• CAST 函數 • TO_CHAR • TO_DATE 陣列 • TO_NUMBER • 日期時間格式字串 • 數值格式字串	所有支持	所有支持
雜湊函數	• MD5 函數 • SHA 函數 • SHA1 函數 • SHA2 函數 • MURMUR3_32_HASH	所有支持	所有支持
數學運算子符號	+、-、*、/、% 和 @	所有支持	所有支持

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
數學函數	• ABS 函數 • ACOS 函數 • ASIN 函數 • ATAN 函數 • ATAN2 函數 • CBRT 函數 • CEILING (或 CEIL) 函數 • COS 函數 • COT 函數 • DEGREES 函數 • DEXP 函數 • LTRIM 函數 • DLOG1 函數 • DLOG10 函數 • EXP 函數 • FLOOR 函數 • LN 函數 • LOG 函數 • MOD 函數 • PI 函數 • POWER 函數 • RADIANS 函數 • RANDOM 函數 • ROUND 函數 • SIGN 函數 • SIN 函數 • SQRT 函數	所有支持	所有支持

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
	• TRUNC 函數		
SUPER 類型資訊函數	• DECIMAL_PRECISION 函數 • DECIMAL_SCALE 函數 • IS_ARRAY 函數 • IS_BIGINT 函數 • IS_CHAR 函數 • IS_DECIMAL 函數 • IS_FLOAT 函數 • IS_INTEGER 函數 • IS_OBJECT 函數 • IS_SCALAR 函數 • IS_SMALLINT 函數 • IS_VARCHAR 函數 • JSON_TYPEOF 函數	所有支持	所有支持
VARBYTE 函數	• FROM_HEX 函數 • FROM_VARBYTE 函數 • TO_HEX 函數 • TO_VARBYTE 函數	所有支持	所有支持

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
JSON	• CAN_JSON_ PARSE 函數 • JSON_EXTR ACT_ARRAY _ELEMENT_TEXT 函數 • JSON_EXTR ACT_PATH_TEXT 函數 • JSON_PARSE 函數 • JSON_SERIALIZE 函數 • JSON_ 服務 _ 到 _ 瓦字節函數	所有支持	所有支持
陣列函數	• 陣列函數 • array_concat 函數 • array_flatten 陣列 • get_array_length 陣列 • split_to_array 陣列 • 子陣列函數	不支援	不支援
延伸群組依據	群組集, 彙總, 立方結構	不支援	不支援
排序操作	ORDER BY	支援在查詢開啟差異隱私權的資料表時，僅在視窗函數的分割區子句中支援 ORDER BY 子句。	支援

短名稱	SQL 建構	一般資料表運算式 (CTE)	最終選擇條款
列限制	LIMIT, OFFSET	使用差異隱私保護表格的 CTE 中不支援	所有支持
表格和欄別名		支援	支援
彙總函式上的數學函數		支援	支援
彙總函式中的純量函數		支援	支援

不支援 SQL 建構的常見替代方案

類別	SQL 建構	備用
範圍函數	• LISTAGG • PERCENTILE_CONT • PERCENTILE_DISC	您可以將等效的彙總函式與 GROUP BY 搭配使用。
數學運算子符號	• $ 專欄 • $ 列 |/ 2 • $ 列 ^ 2	• CBRT • SQRT • 功率（$ 列，2）
純量函數	• SYSDATE • $ 列:: 整數 • 轉換（類型，$ 列）	• CURRENT_DATE • 轉換 $ 列作為整數 • 投 $ 列作為類型
文字	間隔 '1 秒'	間隔 '1' 秒
資料列限制	排名前 N	極限 n
Join	• USING • NATURAL	ON 子句應明確包含連接標準。

差分隱私查詢提示和範例

AWS Clean Rooms 「微分隱私」會使用一般用途的查詢結構來支援各種 SQL 建構，例如用於準備資料的通用資料表運算式 (CTE)，以及常用的彙總函式 (例如，或)。COUNT SUM為了通過在運行時添加噪聲來混淆數據中任何可能的用戶的貢獻，以便在運行時對聚合查詢結果進行混淆， AWS Clean Rooms 差分隱私要求最終SELECT statement的聚合函數在用戶級數據上運行。

下列範例會使用socialco_users來自媒體發行者的名為socialco_impressions和的兩個資料表，這些資料表想要在與運動品牌合作的同時使用差異隱私來保護athletic_brand_sales資料。媒體發行者已將該user_id欄設定為使用者識別碼欄，同時在中啟用差異隱私 AWS Clean Rooms。廣告客戶不需要差分隱私保護，並希望對合併數據使用 CTE 運行查詢。由於其 CTE 使用差異隱私保護的資料表，因此廣告客戶會在 CTE 欄清單中納入那些受保護表格的使用者識別碼欄，並在使用者識別碼欄上聯結受保護的資料表。

```
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
```

同樣地，如果您想要在受保護差異隱私權的資料表上執行視窗函式，您必須在PARTITION BY子句中包含使用者識別碼欄。

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

AWS Clean Rooms 微分隱私的局限性

AWS Clean Rooms 差分隱私不能解決以下情況：

1. AWS Clean Rooms 差分隱私不能解決定時攻擊。例如，在個別使用者貢獻大量資料列，而新增或移除此使用者會大幅變更查詢計算時間的情況下，就可能發生這些攻擊。
2. 當 SQL 查詢因使用特定 SQL 建構而導致執行階段溢位或無效轉換錯誤時，AWS Clean Rooms 差異隱私不保證差異隱私。下表是部分 (但不是全部) SQL 建構的清單，這些建構可能會產生執行階段錯誤，並應在分析範本中進行驗證。我們建議您核准分析範本，以盡可能減少發生此類執行階段錯誤的機會，並定期檢閱查詢記錄檔，以判斷查詢是否符合協同合作合約。

   下列 SQL 建構容易受到溢位錯誤的影響：

   - 彙總函數-平均、列表、百分比計數、磁碟、總和/不同
   - 數據類型格式化函數-到 _ 時間戳，到 _ 日期
   - 日期和時間函數-添加月份，日期添加，日期差異
   - 數學函數-+，-，*，/，功率
   - 字符串函數-||，連接，重複，複製
   - 窗口功能-平均，列表，百分比 _ 計數，百分盤，比例到報告，總和

   CAST 資料類型格式化函數容易受到無效轉換錯誤的影響。

AWS Clean Rooms 毫升

AWS Clean Rooms 毫升

AWS Clean Rooms ML 為雙方提供了一種隱私保護方法，以識別其數據中的相似用戶，而無需彼此共享數據。第一方會將訓練資料帶入，以 AWS Clean Rooms 便他們可以建立和設定相似模型，並將其與共同作業產生關聯。然後，第二方將其種子資料帶入， AWS Clean Rooms 並產生類似於訓練資料的相似區段。

如需其運作方式的更詳細說明，請參閱跨帳戶工作。

- 訓練資料提供者 — 提供訓練資料、建立並設定相似模型，然後將相似模型與共同作業建立關聯的一方。
- 種子資料提供者 — 提供種子資料、產生相似區段，以及匯出其相似區段的一方。
- 訓練資料 — 訓練資料提供者的資料，用於產生相似模型。訓練資料用於測量使用者行為的相似性。

  訓練資料必須包含使用者 ID、項目 ID 和時間戳記資料行。或者，訓練資料可以包含其他作為數值或分類特徵的互動。互動範例包括觀看的影片、已購買的項目或已閱讀的文章。
- 種子資料 — 種子資料提供者的資料，用於建立相似區段。相似區段輸出是訓練資料中最類似種子使用者的一組使用者。
- 相似模型 — 訓練資料的機器學習模型，用來尋找其他資料集中的類似使用者。

  使用 API 時，「受眾模型」一詞會等同用於相似模型。例如，您可以使用CreateAudience模型 API 來建立相似模型。
- 相似區段 — 訓練資料的子集，與種子資料最相似。

  使用 API 時，您可以使用 StartAudienceGenerationJobAPI 建立相似區段。

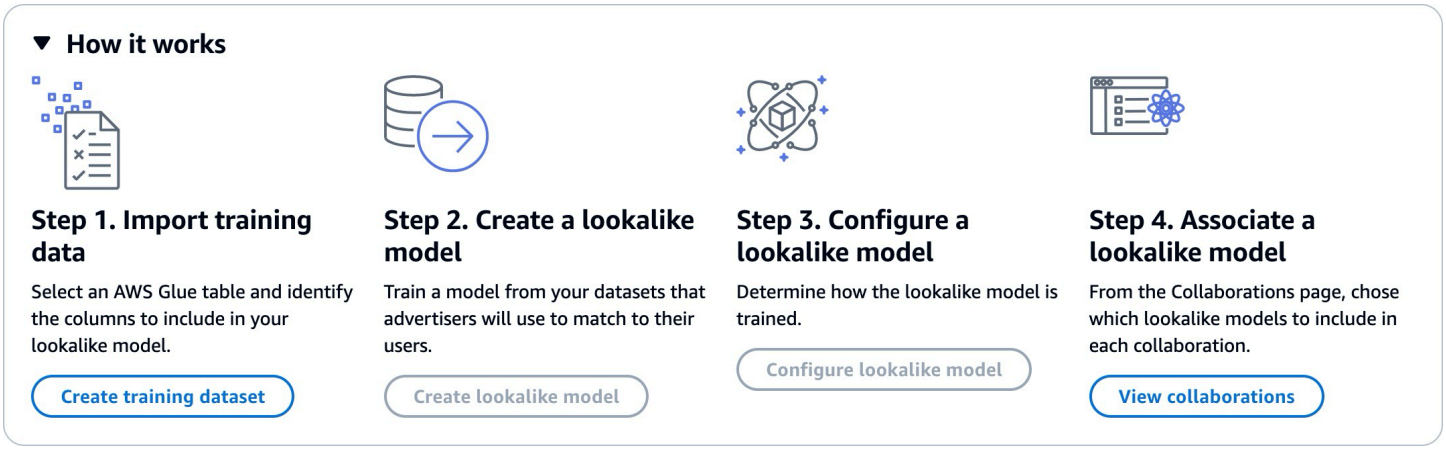
訓練資料提供者的資料絕不會與種子資料提供者共用，而且絕不會與訓練資料提供者共用種子資料提供者的資料。相似區段輸出會與訓練資料提供者共用，但絕不會與種子資料提供者共用。

如需相似模型的詳細資訊，請參閱下列主題。

主題

- AWS Clean Rooms ML 的工作原理

AWS Clean Rooms ML 的工作原理



Clean Rooms ML 要求雙方 (訓練資料提供者和種子資料提供者) 依序進行工作， AWS Clean Rooms 以將其資料納入協同合作中。這是訓練資料提供者必須先完成的工作流程：

1. 訓練資料提供者的資料必須儲存在使用者項目互動的 AWS Glue 資料目錄表格中。訓練資料至少必須包含使用者 ID 欄、互動 ID 資料行和時間戳記資料行。
2. 訓練資料提供者會使用註冊訓練資料 AWS Clean Rooms。
3. 訓練資料提供者會建立可與多個種子資料提供者共用的相似模型。相似模型是一種深度神經網絡，最多可能需要 24 小時才能進行訓練。它不會自動重新訓練，我們建議您每週重新訓練模型。
4. 訓練資料提供者可設定相似模型，包括是否共用相關性指標以及輸出區段的 Amazon S3 位置。訓練資料提供者可以從單一相似模型建立多個已設定的相似模型。
5. 訓練資料提供者會將已設定的受眾模型與與種子資料提供者共用的協同合作產生關聯。

這是種子資料提供者接下來必須完成的工作流程：

1. 種子資料提供者的資料必須存放在 Amazon S3 儲存貯體中。
2. 種子資料提供者會開啟他們與訓練資料提供者共用的共同作業。
3. 種子資料提供者會從協同作業頁面的「清潔室 ML」索引標籤建立相似區段。
4. 種子資料提供者可以評估相關性指標 (如果共用)，並匯出相似區段以供外部 AWS Clean Rooms使用。

ML 的隱私保護 AWS Clean Rooms

Clean Rooms ML 旨在降低會員資格推論攻擊的風險，其中訓練資料提供者可以了解種子資料中的誰，並且種子資料提供者可以了解訓練資料中的人員。採取了幾個步驟來防止這種攻擊。

首先，種子資料提供者不會直接觀察 Clean Rooms ML 輸出和訓練資料提供者永遠無法觀察種子資料。種子資料提供者可以選擇在輸出區段中包含種子資料。

接下來，相似模型是從訓練資料的隨機樣本建立的。此範例包含大量不符合種子對象的使用者。這個過程使得確定用戶是否不在數據中變得更加困難，這是成員資格推斷的另一種途徑。

此外，多個種子客戶可以用於特定種子相似模型培訓的每個參數。這限制了模型可以過度容納多少，因此可以對使用者進行推斷多少。因此，我們建議種子資料的最小大小為 500 個使用者。

最後，永遠不會將使用者層級指標提供給訓練資料提供者，這樣就消除了會員資格推論攻擊的另一個途徑。

AWS Clean Rooms ML 模型評估指標

無塵室 ML 會計算召回和相關性分數，以決定模型的效能。召回比較相似資料和訓練資料之間的相似性。相關性分數用於決定受眾應該有多大，而不是模型是否表現良好。

召回是相似區段與訓練資料有多相似的公正度量。召回是受眾產生工作包含在種子對象中之訓練資料範例中，最相似的使用者 (預設情況下，最相似的 20%) 的百分比。值的範圍從 0-1，較大的值表示更好的受眾。召回值大約等於最大資料桶百分比表示對象模型等於隨機選取。

我們認為這是比準確性、精確度和 F1 分數更好的評估指標，因為 Clean Rooms ML 在建立模型時並未準確地標示真正的負面使用者。

區段層級相關性分數是一種相似度的度量，其值範圍從 -1 (最相似) 到 1 (最相似)。Clean Rooms ML 會針對各種區段大小計算一組相關性分數，以協助您判斷資料的最佳區段大小。相關性分數會隨著區段大小的增加而單調地減少，因此隨著區段大小的增加，它可能與種子資料不太相似。當區段層級相關性分數達到 0 時，模型會預測相似區段中的所有使用者都來自與種子資料相同的分佈。增加輸出大小可能會包括相似區段中的使用者，而這些使用者與種子資料分佈不同。

相關性分數會在單一促銷活動中標準化，不應用於跨宣傳活動進行比較。關聯性分數不應當作任何業務結果的單一來源證據，因為除了相關性之外，這些因素還受到多個複雜因素的影響，例如庫存品質、庫存類型、廣告時間等。

相關性分數不應該用於判斷種子的質量，而應該用於判斷種子的質量是否可以增加或減少。請考量下列範例：

- 所有正數分數 — 這表示預測為類似的輸出使用者多於相似區段中所包含的輸出使用者數。這對於屬於大型市場一部分的種子數據很常見，例如過去一個月購買牙膏的每個人。我們建議您查看較小的種子數據，例如在過去一個月購買牙膏一次以上的每個人。
- 所有負片都會為您想要的相似區段大小評分或負數 — 這表示 Clean Rooms ML 預測所需的相似區段大小中沒有足夠的類似使用者。這可能是因為種子數據太具體或市場太小。我們建議您對種子資料套用較少的篩選器，或是擴大市場。例如，如果原始種子數據是購買嬰兒車和汽車座椅的客戶，則可以將市場擴展到購買多個嬰兒產品的客戶。

訓練資料提供者會決定是否公開相關性分數，以及計算相關性分數的值區資料桶。

使用 AWS Clean Rooms ML

相似模型是訓練資料提供者資料的模型，可讓種子資料提供者建立與其種子資料最相似的訓練資料提供者資料的相似區段。若要建立可用於協同作業的相似模型，您必須匯入訓練資料、建立相似模型、設定該相似模型，然後將其與協同合作產生關聯。

訓練資料提供者建立 ML 模型後，種子資料提供者可以建立和匯出種子區段。

主題

使用相似模型 (訓練資料提供者)

匯入訓練資料

在建立相似模型之前，您必須指定包含訓練資料的 AWS Glue 表格。無塵室 ML 不會儲存此資料的副本，只會儲存允許其存取資料的中繼資料。

若要匯入訓練資料 AWS Clean Rooms

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。

2. 在左側導覽窗格中，選擇 [ML 模型]。
3. 在訓練資料集索引標籤上，選擇建立訓練資料集。
4. 輸入「名稱」與選擇性「說明」。
5. 對於「資料來源」，請選擇 AWS Glue 表格：

   a. 從下拉列表中選擇要配置的數據庫。

   b. 從下拉式清單中選取要設定的「資料庫」和「表格」，以選擇「訓練」資料來源。

   > **Note**
   >
   > 若要確認此表格是否正確，請執行下列任一項作業：
   >
   > - 選擇 [檢視於] AWS Glue。
   > - 開啟 [檢視結構描述] 以檢視結構描述。

6. 對於訓練詳細資料，請從資料中選擇 [使用者識別碼] 欄、[項目識別碼] 欄和 [時間戳記] 欄。訓練資料必須包含這三個欄位。您也可以選取要包含在訓練資料中的任何其他欄。

   「時間戳記」欄中的資料必須是 Unix 紀元時間 (以秒為單位)。

7. 在服務存取中，您必須指定可存取資料的服務角色，並在資料已加密時提供 KMS 金鑰。選擇 [建立並使用新的服務角色]，Clean Rooms ML 就會自動建立服務角色並新增必要的權限原則。如果您有要使用的特定服務角色，請選擇 [使用現有的服務角色]，然後在 [服務角色名稱] 欄位中輸入該角色。

   如果您的資料已加密，請在AWS KMS key欄位中輸入您的 KMS 金鑰，或按一下建立 AWS KMS key以產生新的 KMS 金鑰。

8. 如果您想要啟用訓練資料集的標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。
9. 選擇建立訓練資料集。

如需對應的 API 動作，請參閱CreateTraining資料集。

建立相似模型

建立訓練資料集之後，您就可以建立相似模型了。您可以從單一訓練資料集建立許多相似模型。

您必須在您的中建立預設資料庫， AWS Glue Data Catalog 或在提供的角色中包含`glue:createDatabase`權限。

若要在中建立相似模型 AWS Clean Rooms

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [ML 模型]。
3. 在「相似模型」標籤上，選擇「建立相似模型」。
4. 對於 「建立相似模型」，針對相似模型詳細資料：
    a. 輸入「名稱」與選擇性「說明」。
    b. 從下拉式清單中選擇您要建立模型的訓練資料集。
    c. 輸入選擇性的 「訓練」視窗。
5. 如果您要啟用相似模型的自訂加密設定，請選擇 [自訂加密設定]，然後輸入 KMS 金鑰。
6. 如果您要為相似模型啟用「標籤」，請選擇「新增標籤」，然後輸入「金鑰」和「值」配對。
7. 選擇「建立相似模型」。

如需對應的 API 動作，請參閱CreateAudience模型。

設定相似模型

建立相似模型之後，您就可以將其設定為在協同作業中使用。您可以從單一相似模型建立多個已設定的相似模型。

若要在中設定相似模型 AWS Clean Rooms

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [ML 模型]。
3. 在 [設定的相似模型] 索引標籤上，選擇 [設定相似模型]。
4. 對於配置相似模型，對於已配置的相似模型詳細信息：
    a. 輸入「名稱」與選擇性「說明」。
    b. 從下拉列表中選擇要配置的相似模型。
    c. 選擇您想要的最小匹配種子大小。這是種子資料提供者資料中與訓練資料中使用者重疊的最小使用者數目。此值必須大於 0。
5. 對於要與其他成員共用的指標，請選擇是否要讓共同作業中的種子資料提供者接收模型指標，包括相關性分數。

6. 對於相似區段目的地位置，請輸入要匯出相似區段的 Amazon S3 儲存貯體。此值區必須與其他資源位於相同的區域。
7. 對於「服務」存取，請選擇將用於存取此表格的現有服務角色名稱。
8. 選擇「設定相似模型」。
9. 如果要為已配置的表格資源啟用標籤，請選擇 [新增標籤]，然後輸入 [索引鍵] 和 [值] 配對。

如需相應的 API 動作，請參閱CreateConfiguredAudienceModel。

關聯已設定的相似模型

設定完相似模型之後，您可以將其與協同合作產生關聯。

將已設定的相似模型關聯於 AWS Clean Rooms

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇「合作」。
3. 在 [具有使用中成員資格] 索引標籤上，選擇合作。
4. 在 [ML 建模] 索引標籤上，選擇 [關聯相似模型]。
5. 對於關聯已設定的相似模型，對於關聯相似模型詳細資料：
   a. 為關聯的已設定對象模型輸入「名稱」。
   b. 輸入表格的「摘要」。

      此描述有助於區分具有相似名稱的其他關聯已設定對象模型。
6. 對於「已設定的相似模型」，請從下拉式清單中選擇已設定的相似模型。
7. 選擇關聯。

如需對應的 API 動作，請參閱CreateConfiguredAudienceModel關聯。

更新已設定的相似模型

關聯設定的相似模型後，您可以更新它以變更名稱、要共用的指標或輸出 Amazon S3 位置等資訊。

若要在中更新關聯的已設定相似模型 AWS Clean Rooms

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [ML 模型]。
3. 在「已設定的相似模型」標籤中，選擇已設定的相似模型，然後選取「編輯」。
4. 對於配置相似模型，對於已配置的相似模型詳細信息：
   a. 從下拉列表中選擇要配置的相似模型。
   b. 選擇您想要的最小匹配種子大小。這是種子資料提供者資料中與訓練資料中使用者重疊的最小使用者數目。此值必須大於 0。
5. 對於要與其他成員共用的指標，請選擇是否要讓共同作業中的種子資料提供者接收模型指標，包括相關性分數。
6. 對於相似區段目的地位置，請輸入要匯出相似區段的 Amazon S3 儲存貯體。此值區必須與其他資源位於相同的區域。
7. 對於「服務」存取，請選擇將用於存取此表格的現有服務角色名稱。
8. 對於「進階資料桶大小」設定，請選擇您要如何設定對象資料匣大小。
9. 選擇儲存變更。

如需相應的 API 動作，請參閱UpdateConfiguredAudienceModel。

使用相似區段 (種子資料提供者)

建立相似區段

相似區段是訓練資料的子集，最接近種子資料。

若要在中建立相似區段 AWS Clean Rooms

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇「合作」。
3. 在 [具有使用中成員資格] 索引標籤上，選擇合作。
4. 在 [ML 塑型] 索引標籤上，選擇 [建立相似區段]。
5. 對於「建立相似區段」，對於相似區段詳細資訊，請輸入「名稱」和選用「說明」。

6. 對於種子設定檔，請選擇存放種子資料的 Amazon S3 輸入來源。
7. 對於「服務」存取，請選擇將用於存取此表格的現有服務角色名稱。
8. 如果您想要啟用訓練資料集的標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。
9. 選擇「建立相似區段」。

如需相應的 API 動作，請參閱StartAudienceGenerationJob。

匯出相似區段

建立相似區段後，您可以將該資料匯出到 Amazon S3 儲存貯體。

若要匯出相似區段 AWS Clean Rooms

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇「合作」。
3. 在 [具有使用中成員資格] 索引標籤上，選擇合作。
4. 在 [ML 塑型] 索引標籤上，選取相似區段，然後選擇 [匯出]。
5. 對於「匯出相似模型」，對於「匯出相似模型詳細資訊」，請輸入「名稱」和「描述」。
6. 在「區段大小」中，選擇匯出區段所要的大小。
7. 選擇 Export (匯出)。

如需相應的 API 動作，請參閱StartAudienceExportJob。

後續步驟

現在您已經建立了相似的模型並匯出種子區段，您可以：

- Manage (管理) AWS Clean Rooms

密碼編譯運算 Clean Rooms

Clean Rooms(C3R) 的密碼編譯運算是除了分析規則之外還可以使用的功能。 AWS Clean Rooms透過 C3R，組織可以將敏感資料整合在一起，從資料分析中獲得新的見解，同時以密碼編譯方式限制流程中任何一方可以學到的內容。希望與敏感數據進行協作，但只需在雲中使用加密數據的兩個或多方可以使用 C3R。

C3R 加密用戶端是一種用戶端加密工具，可用來加密資料以供搭配使用。 AWS Clean Rooms當您使用 C3R 加密用戶端時，資料會在共同作業中使用時保持密碼編譯保護。 AWS Clean Rooms 如同一般 AWS Clean Rooms 協同合作，輸入資料是關聯式資料庫資料表，而計算則以 SQL 查詢表示。不過，C3R 僅支援加密資料的有限 SQL 查詢子集。

具體而言，C3R 支援加密保護資料的 SELECT SQL JOIN 和陳述式。輸入資料表中的每個資料行都可以在下列其中一個 SQL 陳述式類型中使用：

- 受密碼編譯保護以便在JOIN陳述式中使用的資料行稱為fingerprint資料行。
- 受密碼編譯保護以便在SELECT陳述式中使用的資料行稱為sealed資料行。
- 未加密保護以用於JOIN或SELECT陳述式的資料行稱為cleartext資料行。

在某些情況下，fingerprint資料行支援GROUP BY陳述式。如需詳細資訊，請參閱 Fingerprint專欄。目前，C3R 不支援在加密資料上使用其他 SQL 建構，例如WHERE子句或彙總函式 (如 SUM AND)AVERAGE，即使相關分析規則會允許這些建構。

C3R 旨在保護表格中個別儲存格中的資料。使用 C3R 的預設組態時，客戶透過協同合作提供給第三方的基礎資料會保持加密狀態，而內容正在使用中。 AWS Clean Rooms C3R 針對所有sealed資料行使用業界標準 AES-GCM 加密，並使用業界標準的偽隨機函數 (稱為雜湊型訊息驗證碼 (HMAC)，以保護資料行。fingerprint

雖然 C3R 會加密資料表中的資料，但仍然可以推斷下列資訊：

- 表格本身的相關資訊，包括資料欄數、欄名稱以及表格中的列數。
- 與大多數標準加密形式一樣，C3R 不會嘗試隱藏加密值的長度。C3R 確實提供了填充加密值的功能，以隱藏明文的確切長度。但是，每列中明文長度的上限仍然可以向另一方顯示。
- 記錄層級資訊，例如將特定資料列新增至加密的 C3R 表格時。

如需 C3R 的相關資訊，請參閱下列主題。

主題

使用密碼編譯運算時的考量 Clean Rooms

Clean Rooms（C3R）的密碼編譯計算力求最大限度地提高數據保護。但是，某些使用案例可能會受益於較低層級的資料保護，以換取其他功能。您可以透過從最安全的組態修改 C3R 來進行這些特定的權衡。身為客戶，您應該瞭解這些權衡，並判斷它們是否適合您的使用案例。要考慮的權衡包括以下幾點：

主題

如需如何為這些案例設定參數的詳細資訊，請參閱密碼計算參數。

在表格中允許混合cleartext和加密資料

將所有資料都用戶端加密，可提供最大的資料保護。不過，這會限制特定類型的查詢 (例如，SUM彙總函式)。允許資cleartext料的風險在於，任何具有加密資料表存取權的人都可以推斷一些有關加密值的資訊。這可以通過對cleartext和相關數據進行統計分析來完成。

例如，假設您有City和的欄State。資City料行是cleartext且資State料行已加密。當您在City列Chicago中看到該值時，可以幫助您確定高概率State是Illinois. 相比之下，如果一列是City，另一列是EmailAddress，a cleartext City 不太可能揭示有關加密的任何內容EmailAddress。

如需有關此案例之參數的詳細資訊，請參閱允許cleartext欄參數。

允許fingerprint列中的重複值

對於最安全的方法，我們假設任何fingerprint列只包含一個變量的一個實例。沒有項目可以在一fingerprint列中重複。C3R 加密用戶端會將這些cleartext值對應到與隨機值無法區分的唯一值。因此，不可能cleartext從這些隨機值推斷出有關的資訊。

fingerprint列中重複值的風險是重複的值將導致重複的隨機外觀值。因此，理論上，任何有權存取加密資料表的人都可以對可能揭示cleartext值相關資訊的資fingerprint料行執行統計分析。

再次，假設該fingerprint列是`State`，並且表格的每一行對應於一個美國家庭。通過進行頻率分析，可以推斷出哪個狀態是哪個狀態以`California`及哪些狀態`Wyoming`具有高概率。這種推斷是可能的，因為`California`有更多的居民比`Wyoming`. 相比之下，假設該fingerprint列位於家庭標識符上，並且每個家庭在數據庫中出現在數百萬條目的數據庫中 1 到 4 次之間。頻率分析不太可能會揭示任何有用的信息。

如需有關此案例之參數的詳細資訊，請參閱允許重複參數。

放鬆fingerprint列的命名方式限制

根據預設，我們假設當兩個資料表使用加密fingerprint資料行聯結時，這些資料行在每個資料表中具有相同的名稱。這個結果的技術原因是，默認情況下，我們得出一個不同的加密密鑰來加密每個fingerprint列。該金鑰衍生自共同作業的共用密碼金鑰與資料行名稱的組合。如果我們嘗試連接具有不同列名的兩列，我們得出不同的鍵，我們不能計算一個有效的連接。

若要解決此問題，您可以關閉從每個欄名稱衍生索引鍵的功能。然後，C3R 加密用戶端會針對所有fingerprint資料行使用單一衍生金鑰。風險是可以進行另一種可能揭示信息的頻率分析。

讓我們再次使用`City`和`State`範例。如果我們為每fingerprint列派生相同的隨機值（通過不合併列名）。 `New York`在`City`和欄中具有相同的隨機`State`值。紐約是美國少數幾個城市之一，其`City`名稱與`State`名稱相同。相反地，如果您的資料集在每個資料欄中具有完全不同的值，則不會洩漏任何資訊。

如需有關此案例之參數的詳細資訊，請參閱允許具有不同名稱參數JOIN的列。

確定NULL值的表示方式

您可以使用的選項是是否像處理任何其他值一樣處理加密（加密和 HMAC）NULL值。如果您不像處理任何其他NULL值一樣處理值，則可能會顯示資訊。

例如，假設NULL在Middle Name欄中cleartext指示沒有中間名的人。如果您不加密這些值，則會洩漏加密資料表中的哪些資料列用於沒有中間名的人員。對於某些人群中的某些人來說，這些信息可能是一種識別信號。但是，如果您執行密碼編譯處理NULL值，則某些 SQL 查詢的行為會有所不同。例如，子GROUP BY句不會將fingerprint欄中的fingerprintNULL值分組在一起。

如需有關此案例之參數的詳細資訊，請參閱保留NULL值參數。

在加密計算中支持的文件和數據類型 Clean Rooms

C3R 加密用戶端可辨識下列檔案類型：

- CSV 檔案
- Parquet檔案

您可以使用 C3R 加密用戶端中的--fileFormat旗標來明確指定檔案格式。明確指定時，檔案格式不會由副檔名決定。

主題

- CSV 檔案
- Parquet檔案
- 加密非字串值

CSV 檔案

副檔名為 .csv 的檔案會假設為 CSV 格式，且包含 UTF-8 編碼文字。C3R 加密用戶端會將所有值視為字串。

.csv 檔案中支援的屬性

C3R 加密用戶端要求 .csv 檔案具有下列內容：

- 可能包含或可能不包含唯一命名每列的初始標題行。
- 以逗號分隔。(目前不支援自訂分隔符號)。
- UTF-8 編碼的文本。

從 .csv 項目修剪空白區域

前導和尾隨空格都會從 .csv 項目中修剪。

.csv 檔案的自訂NULL編碼

.csv 檔案可以使用自訂NULL編碼。

使用 C3R 加密用戶端，您可以使用旗標為輸入資料中的NULL項目指定自訂編碼。`--csvInputNULLValue=<csv-input-null>`C3R 加密用戶端可以使用旗標，在產生的輸出檔案中針對 NULL 項目使用自訂編碼。`--csvOutputNULLValue=<csv-output-null>`

> **Note**
>
> NULL條目被認為是缺少內容，特別是在更豐富的表格格式（如 SQL 表）的上下文中。雖然 .csv 基於歷史原因並未明確支援此特性分析，但考慮只包含空白區域的空白項目是一種常見慣例。NULL因此，這是 C3R 加密用戶端的預設行為，可視需要進行自訂。

C3R 如何解釋 .csv 條目

下表提供了如何根據cleartext為和旗標提供的值 (如果有的話) 封送 .csv 項目的範例 (以cleartext便清楚起見)。`--csvInputNULLValue=<csv-input-null>` `--csvOutputNULLValue=<csv-output-null>`在 C3R 解釋任何值的含義之前，引號外的前導和尾隨空格被修剪。

<csv-input-null>	**<csv-output-null>**	輸入項目	輸出項目
無	無	`,AnyProduct,`	`,AnyProduct,`
無	無	`, AnyProduct ,`	`,AnyProduct,`
無	無	`,"AnyProduct",`	`,AnyProduct,`
無	無	`, "AnyProduct" ,`	`,AnyProduct,`
無	無	`,,`	`,,`
無	無	`, ,`	`,,`

<csv-input-null>	**<csv-output-null>**	輸入項目	輸出項目
無	無	,"",	,,
無	無	," ",	," ",
無	無	, " " ,	," ",
"AnyProduct"	"NULL"	,AnyProduct,	,NULL,
"AnyProduct"	"NULL"	, AnyProduct ,	,NULL,
"AnyProduct"	"NULL"	,"AnyProduct",	,NULL,
"AnyProduct"	"NULL"	, "AnyProduct" ,	,NULL,
無	"NULL"	,,	,NULL,
無	"NULL"	, ,	,NULL,
無	"NULL"	,"",	,NULL,
無	"NULL"	," ",	," ",
無	"NULL"	, " " ,	," ",
""	"NULL"	,,	,NULL,
""	"NULL"	, ,	,NULL,
""	"NULL"	,"",	,"",
""	"NULL"	," ",	," ",
""	"NULL"	, " " ,	," ",
"\"\""	"NULL"	,,	,,
"\"\""	"NULL"	, ,	,,

<csv-input-null>	**<csv-output-null>**	輸入項目	輸出項目
"\"\""	"NULL"	,"",	,NULL,
"\"\""	"NULL"	," ",	," ",
"\"\""	"NULL"	, " " ,	," ",

不含標題的 CSV 檔案

來源 .csv 檔案不需要在第一列中具有唯一命名每一欄的標題。但是，沒有標題列的 .csv 檔案需要位置加密結構描述。需要位置加密結構描述，而不是標題列和Parquet檔案的 .csv 檔案所使用的典型對應結構描述。

位置加密結構描述會依位置而非名稱來指定輸出資料行。對應的加密架構會將來源資料欄名稱對應至目標資料欄名稱。如需詳細資訊，包括兩種結構描述格式的詳細討論和範例，請參閱對映和位置表格資料架構。

Parquet檔案

具有.parquet擴展名的文件被假定為Apache Parquet格式。

支援的Parquet資料類型

C3R 加密客戶端可以處理代表支持的數據類型的Parquet文件中的任何非複雜（也就是原始類型）數據。 AWS Clean Rooms

但是，只有字串資料行可用於sealed欄。

支援下列實木複合地板資料類型：

- Binary具有以下邏輯註釋的原始類型：
  - 如果設定--parquetBinaryAsString為「無」(STRING資料類型)
  - Decimal(scale, precision)(DECIMAL資料類型)
  - String(STRING資料類型)
- Boolean沒有邏輯註釋的原始數據類型（BOOLEAN數據類型）
- Double沒有邏輯註釋的原始數據類型（DOUBLE數據類型）

- Fixed_Len_Binary_Array帶有Decimal(scale, precision)邏輯註釋的原始類型（DECIMAL數據類型）
- Float沒有邏輯註釋的原始數據類型（FLOAT數據類型）
- Int32具有以下邏輯註釋的原始類型：
  - 無 (INT資料類型)
  - Date(DATE資料類型)
  - Decimal(scale, precision)(DECIMAL資料類型)
  - Int(16, true)(SMALLINT資料類型)
  - Int(32, true)(INT資料類型)
- Int64具有以下邏輯註釋的原始數據類型：
  - 無 (BIGINT資料類型)
  - Decimal(scale, precision)(DECIMAL資料類型)
  - Int(64, true)(BIGINT資料類型)
  - Timestamp(isUTCAdjusted, TimeUnit.MILLIS)(TIMESTAMP資料類型)
  - Timestamp(isUTCAdjusted, TimeUnit.MICROS)(TIMESTAMP資料類型)
  - Timestamp(isUTCAdjusted, TimeUnit.NANOS)(TIMESTAMP資料類型)

加密非字串值

目前，欄僅支援字串sealed值。

對於 .csv 檔案，C3R 加密用戶端會將所有值視為 UTF-8 編碼文字，並且在加密之前不會嘗試以不同的方式解譯它們。

對於指紋資料行，類型會分組為對等類別。等價類是一組數據類型，可以通過代表性數據類型明確地比較相等性。

等價類允許將相同的指紋分配給相同的語義值，而不管原始表示。但是，兩個等價類別中的相同值不會產生相同的指紋資料行。

例如，無論該INTEGRAL值原本是、或SMALLINT，INT都42會指派相同的指紋BIGINT。此外，該INTEGRAL值永遠不0會匹配BOOLEAN值FALSE（由值表示0）。

指紋資料行支援下列對等類別和對應的 AWS Clean Rooms 資料類型：

等價類	支援的 AWS Clean Rooms 資料類型
BOOLEAN	BOOLEAN
DATE	DATE
INTEGRAL	BIGINT, INT, SMALLINT
STRING	CHAR, STRING, VARCHAR

密碼編譯計算中的欄名稱 Clean Rooms

根據預設，資料行的名稱在密碼編譯計算中很重要。Clean Rooms

如果 [允許具有不同名稱JOIN的資料行] 參數的值為 false，則在加密資料行期間會使用fingerprint資料行名稱。因此，依預設，協同合作者必須事先協調，並在查詢中使用JOIN陳述式的資料使用相同的目標欄名稱。根據預設，JOIN使用不同名稱加密的資料行無法JOIN在任何值上成功。

如果 [允許具有不同名稱JOIN的資料行] 參數的值為 true，則會在資料行之間加密的JOIN陳述式成功。fingerprint使用此參數加密資料可能會允許對值進行某些推論。cleartext例如，如果資料列在資料行和欄中具有相同的雜湊型訊息驗證碼 (HMAC) `City` `State` 值，則值可能是。`New York`

列標題名稱的標準化

C3R 加密用戶端會標準化欄標頭名稱。任何前導和尾隨空格都會被移除，並且對於轉換的輸出而言，資料行名稱會變成小寫。

標準化應用於所有其他可能受到列名影響的計算，計算或其他操作之前。發出的輸出文件僅包含標準化名稱。

密碼編譯計算中的欄類型 Clean Rooms

本主題提供的Clean Rooms密碼編譯計算中資料行類型的相關資訊。

主題

- Fingerprint專欄

- 密封柱
- Cleartext專欄

Fingerprint專欄

Fingerprint資料行是受密碼編譯保護以便在JOIN陳述式中使用的資料行。

資料fingerprint行中的資料無法解密。只有密封資料行中的資料才能解密。

Fingerprint資料行只能用於下列 SQL 子句和函數：

- JOIN (INNER, OUTER, LEFT, RIGHT, or FULL)針對其他fingerprint欄：
  - 如果將`allowJoinsOnColumnsWithDifferentNames`參數的值設定為`false`，則的兩個fingerprint欄也JOIN必須具有相同的名稱。
- `SELECT COUNT()`
- `SELECT COUNT(DISTINCT )`
- `GROUP BY`(只有在協同作業已將`preserveNulls`參數值設定為時才使用`true`。)

違反這些限制的查詢可能會產生不正確的結果。

密封柱

密封的資料行是受密碼編譯保護以便在SELECT陳述式中使用的資料行。

密封的資料行必須只能用於下列 SQL 子句和函數：

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

> **Note**
>
> 不支援 `SELECT COUNT(DISTINCT )`。

違反這些限制的查詢可能會產生不正確的結果。

在加密之前填補資料sealed欄的資料

當你指定一個列應該是一個sealed列，C3R 會詢問你選擇什麼樣的填充。加密前填補資料是選擇性的。如果沒有填補 (填充類型none)，則加密資料的長度會指出的大小cleartext。在某些情況下，的大小cleartext可能會暴露明文。使用填充 (`fixed`或的填充類型`max`) 時，所有值會先填補成一般大小，然後加密。使用填充時，加密數據的長度不會提供有關原始cleartext長度的信息，除了給出其大小的上限之外。

如果您想要填充列，並且該列中數據的最大字節長度是已知的，請使用`fixed`填充。使用至少與該列中最長`length`值的字節長度一樣大的值。

> **Note**
>
> 如果值超過提供的值，則會發生錯誤且加密失敗`length`。

如果您想要填充列，並且該列中數據的最大字節長度不知道，請使用`max`填充。此填充模式將所有數據填充到最長值的長度加上其他`length`字節。

> **Note**
>
> 您可能想要批次加密資料，或定期使用新資料更新資料表。請注意，`max`填充會將條目填補到給定批次中最長純文本條目的長度（加上`length`字節）。這意味著密文長度可能因批次而異。因此，如果您知道列的最大字節長度，則應該使用`fixed`而不是。`max`

Cleartext專欄

Cleartext資料行是不受密碼編譯保護以便在JOIN或SELECT陳述式中使用的資料行。

Cleartext列可以在 SQL 查詢的任何部分使用。

密碼計算參數

在建立協同作業時，可使用密碼編譯運算參數 Clean Rooms (C3R) 進行共同作業。您可以使用 AWS Clean Rooms 主控台或 `CreateCollaboration` API 作業建立協同作業。在主控台中，您可以在開啟 [Sup port 加密運算] 選項之後，在密碼編譯運算參數中設定參數的值。如需詳細資訊，請參閱下列主題。

主題

允許cleartext欄參數

在主控台中，您可以在建立協同作業時設定「允許cleartext欄」參數，以指定含有加密cleartext資料的資料表中是否允許資料。

下表說明 cleartext[允許欄] 參數的值。

參數值	描述
否	Cleartext加密資料表中不允許使用欄。所有數據均受密碼保護。
是	Cleartext加密資料表中允許使用欄。 Cleartext資料行不受密碼編譯保護且包含為cleartext。您應該注意行的cleartext數據可能會顯示表中其他數據的內容。 若要執行SUM或AVG在特定欄上執行，欄必須位於中cleartext。

對於`dataEncryptionMetadata`參數，您可以使用 `CreateCollaboration` API 作業`allowCleartext`將的值設定為`true`或`false`。如需 API 作業的詳細資訊，請參閱 AWS Clean Rooms API 參考資料。

Cleartext欄對應於在資料表特定結構描述cleartext中分類為的資料行。這些資料行中的資料不會加密，而且可以以任何方式使用。 Cleartext如果數據不敏感和/或需要比加密的列或fingerprint列允許更大的靈活性，sealed列可以很有用。

允許重複參數

在主控台中，您可以在建立協同作業時設定允許重複參數，以指定針對JOIN查詢加密的資料行是否可以包含重複的非NULL值。

> **Important**
>
> [允許重複]、[允許具有不同名稱JOIN的欄] 和 [保留NULL值] 參數具有單獨但相關的效果。

下表說明「允許重複」參數的值。

參數值	描述
否	資料行中不允許重複的fingerprint值。單一fingerprint欄中的所有值都必須是唯一的。
是	列中允許重複的fingerprint值。 如果您需要聯接具有重複值的列，請將此值設置為 Yes。設定為「是」 時，出現在 C3R 表格或結果fingerprint欄中的頻率模式可能會暗示有關資料結構的一些其他資訊。cleartext

使用 `CreateCollaboration` API 作業，您可以將`dataEncryptionMetadata`參數的值設定`allowDuplicates`為`true`或`false`。如需 API 作業的詳細資訊，請參閱 AWS Clean Rooms API 參考資料。

根據預設，如果必須在JOIN查詢中使用加密資料，C3R 加密用戶端會要求這些資料行沒有重複的值。這項要求是為了提高資料保護的努力。此行為有助於確保資料中的重複模式不可觀察。不過，如果您想要在JOIN查詢中處理加密資料，而不擔心重複值，則 [允許重複項目] 參數可以停用此保守檢查。

允許具有不同名稱參數JOIN的列

在主控台中，您可以在建立協同作業時設定允許JOIN具有不同名稱的欄參數，以指定是否支援具有不同名稱的資料行之間的JOIN陳述式。

如需更多資訊，請參閱列標題名稱的標準化

下表說明 [允許具有不同名稱JOIN的資料欄] 參數的值。

參數值	描述
否	不支援不同名稱的fingerprint資料行聯結。 JOIN陳述式只會在具有相同名稱的資料行上提供準確的結果。

參數值	描述
	Important No 值提供更高的資訊安全性，但需要協同合作參與者事先同意欄名稱。如果兩個資料行在加密為資fingerprint料行時具有不同的名稱，且 [允許JOIN具有不同名稱的資料行] 設定為 [否]，則這些資料行上的JOIN陳述式不會產生結 這是因為它們之間不會共用加密後的值。
是	支持不同名稱的fingerprint列的聯接。為了獲得更大的彈性，使用者可以將此值設定為「是」，這樣就可以在欄上JOIN執行陳述式，而不考慮欄名稱。 如果設定為是，C3R 加密用戶端在保護fingerprint資料行時不會考慮資料行名稱。因此，在 C3R 表中可以觀察到跨不同fingerprint列的公共值。 例如，如果資料列在資料行和資料行中具有相同的加密JOINState值，則推斷該值為可能是New York合理的。City

對於dataEncryptionMetadata參數，您可以使用 CreateCollaboration API 作業allowJoinsOnColumnsWithDifferentNames將的值設定為true或false。如需 API 作業的詳細資訊，請參閱 AWS Clean Rooms API 參考資料。

依預設，fingerprint資料行加密會targetHeader受到中設定的該欄的影響步驟 4：為表格檔案產生加密結構描述 。因此，相同cleartext值在加密的每個不同fingerprint資料行中都有不同的加密表示法。

在某些情況下，此參數可用於防止cleartext值的推論。例如，在fingerprint列中看到相同的加密值，City並State可能用於合理地推斷該值是New York。但是，此參數的使用需要事先進行額外的協調，以便要在查詢中連接的所有列都具有共用名稱。

您可以使用允許具有不同名稱JOIN的欄參數來放鬆此限制。當參數值設定為時Yes，它允許任何加密的資料行一起JOIN使用，不論名稱為何。

保留NULL值參數

在主控台中，您可以在建立協同作業時設定「保留NULL值」參數，以指出該欄沒有值。

下表說明「保留值」參數的NULL值。

參數值	描述
否	NULL不會保留值。 NULL值不會顯示為NULL加密資料表中。NULL值在 C3R 表中顯示為唯一的隨機值。
是	NULL值會被保留。 NULL值會顯示NULL在加密資料表中。如果您需要NULL值的 SQL 語意，您可以將此值設定為 [是]。因此，無論資料行是否加密，以及 [允許重複NULL項目] 的參數設定為何，項目都會顯示NULL在 C3R 表格中。

對於`dataEncryptionMetadata`參數，您可以使用 `CreateCollaboration` API 作業`preserveNulls`將的值設定為`true`或`false`。如需 API 作業的詳細資訊，請參閱 AWS Clean Rooms API 參考資料。

當協同合作的「保留NULL值」參數設定為「否」時：

1. NULL`cleartext`欄中的項目不會變更。
2. NULL加密`fingerprint`欄中的項目會以隨機值加密，以隱藏其內容。在加密的資料欄上加NULL入cleartext資料欄並不會產生任何項目相符NULL項目。不進行匹配，因為它們每個人都會收到自己獨特的隨機內容。
3. NULL加密`sealed`欄中的項目會加密。

當協同作業的「保留NULL值」參數值設定為 「是」時，NULL無論資料行是否已加密，所有欄中的NULL項目都會保持為不變。

在資料擴充等情況下，您想要共用缺乏資訊表示為的情況下，「保留NULL值」參數非常有用NULL。如果您想要fingerprint或列中有NULL值，則保留NULL值參數在或 HMAC 格式中也很有用JOIN。GROUP BY

如果 [允許重複項目] 和 [保留NULL值] 參數的值設定為 [否]，則在fingerprint欄中有多個項NULL目會產生錯誤並停止加密。如果任一參數的值設定為「是」，則不會發生此類錯誤。

加密計算中的可選標誌 Clean Rooms

以下各節說明當您使用 C3R 加密用戶端加密資料以進行表格檔案自訂和測試時，可以設定的選用旗標。

主題

--csvInputNULLValue旗

當您使用 C3R 加密用戶端加密資料時，您可以使用--csvInputNULLValue旗標為輸入資料中的NULL項目指定自訂編碼。

下表摘要說明此旗標的用法和參數。

用量	參數
選用。使用者可以為輸入資料中的NULL項目指定自訂編碼。	使用者指定的輸入 CSV 檔案中NULL值的編碼

NULL條目是被認為是缺少內容的條目，特別是在更豐富的表格格式，如 SQL 表的上下文中。雖然 .csv 基於歷史原因並未明確支援此特性分析，但考慮只包含空白區域的空白條目是一種常見慣例。NULL因此，這是 C3R 加密用戶端的預設行為，可視需要進行自訂。

--csvOutputNULLValue旗

當您使用 C3R 加密用戶端加密資料時，您可以使用--csvOutputNULLValue旗標為輸出資料中的NULL項目指定自訂編碼。

下表摘要說明此旗標的用法和參數。

用量	參數
選用。用戶可以在生成的輸出文件中為NULL條目指定自定義編碼。	使用者指定的輸出 CSV 檔案中NULL值的編碼

NULL條目是被認為是缺少內容的條目，特別是在更豐富的表格格式，如 SQL 表的上下文中。雖然 .csv 基於歷史原因並未明確支援此特性分析，但考慮只包含空白區域的空白條目是一種常見慣例。NULL因此，這是 C3R 加密用戶端的預設行為，可視需要進行自訂。

--enableStackTraces旗

當您使用 C3R 加密用戶端加密資料時，請使用--enableStackTraces旗標提供其他內容資訊，以便在 C3R 遇到錯誤時進行錯誤報告。

AWS 不收集錯誤。如果遇到錯誤，請使用堆棧跟踪自己對錯誤進行故障排除，或將堆棧跟踪發送到以獲 AWS Support 取幫助。

下表摘要說明此旗標的用法和參數。

用量	參數
選用。用於在 C3R 加密用戶端發生錯誤時提供錯誤報告的其他內容資訊。	無

--dryRun旗

加密和解密 C3R 加密用戶端命令包含選擇性--dryRun旗標。該標誌採用所有用戶提供的參數，並檢查它們的有效性和一致性。

您可以使用該--dryRun標誌來檢查模式文件是否有效並與其相應的輸入文件一致。

下表摘要說明此旗標的用法和參數。

用量	參數
選用。使 C3R 加密用戶端剖析參數並檢查檔案，但不會執行加密或解密。	無

`--tempDir`旗

您可能想要使用暫存目錄，因為加密檔案有時可能比非加密檔案大，視其設定而定。每次協同合作也必須加密資料集，才能正常運作。

使用 C3R 加密資料時，請使用`--tempDir`旗標來指定在處理輸入時可以建立暫存檔的位置。

下表摘要說明此旗標的用法和參數。

用量	參數
用戶可以指定在處理輸入時可以創建臨時文件的位置。	預設為系統暫存目錄。

使用密碼編譯計算的查詢 Clean Rooms

本主題提供有關撰寫查詢的相關資訊，這些查詢使用已使用的「密碼編譯運算」加密的資Clean Rooms料表。

主題

- 分支的查詢 NULL
- 將一個來源資料欄對映至多個目標資料
- 對JOIN和SELECT查詢使用相同的數據

分支的查詢 NULL

要在語NULL句上有一個查詢分支意味著使用類似的語法`IF x IS NULL THEN 0 ELSE 1`。

查詢總是可以分支cleartext列中的NULL語句。

只有當保留 NULL 值參數 (**`preserveNulls`**) 的值設定為時，查詢才能分支fingerprint資料行和資料行中sealed的NULL陳述式`true`。

違反這些限制的查詢可能會產生不正確的結果。

將一個來源資料欄對映至多個目標資料

一個來源資料行可對應至多個目標資料行。例如，您可能希望在列SELECT上同時使用JOIN和。

如需詳細資訊，請參閱 對JOIN和SELECT查詢使用相同的數據。

對JOIN和SELECT查詢使用相同的數據

如果資料欄中的資料不敏感，它可能會出現在cleartext目標資料欄中，這樣就可以將其用於任何用途。

如果資料行中的資料非常敏感，且必須同時用於JOIN和SELECT查詢，請將該來源資料行對應至輸出檔案中的兩個目標資料行。其中一個資料行會以type作為fingerprint資料行加密，而一個資料行會以密封的資料行加密。typeC3R 加密用戶端的互動式結構描述產生會建議和的標頭尾碼。_fingerprint_sealed這些標題後綴可以是快速區分此類列的有用慣例。

C3R 加密用戶端的準則

C3R 加密用戶端是一種工具，可讓組織將敏感資料整合在一起，從資料分析中獲得新的見解。該工具加密限制了任何一方和過程 AWS 中可以學到的內容。雖然這非常重要，但以密碼方式保護資料安全的程序可能會在運算和儲存資源方面增加顯著的額外負荷。因此，了解使用每個設置的權衡以及如何優化設置，同時仍保持所需的密碼編譯保證是非常重要的。本主題著重於 C3R 加密用戶端和結構描述中不同設定的效能影響。

所有 C3R 加密用戶端加密設定都提供不同的加密保證。在預設情況下，協同作業層級設定最安全。在建立協同作業的同時啟用其他功能會削弱隱私保證，從而允許對密文進行頻率分析等活動。如需有關如何使用這些設定及其含意的更多資訊，請參閱密碼計算。

主題

- 對資料行類型的效能影響
- 疑難排解密文大小意外增加

對資料行類型的效能影響

C3R 使用三種資料行類型：cleartextfingerprint、和。sealed這些欄類型中的每一種都提供不同的密碼編譯保證，並具有不同的預期用途。在下列各節中，我們會討論資料欄類型對效能的影響，以及每個設定對效能的影響。

主題

- Cleartext列
- Fingerprint列
- Sealed列

Cleartext列

Cleartext列不會從其原始格式更改，也不會以任何方式加密處理。此資料行類型無法設定，也不會影響儲存體或運算效能。

Fingerprint列

Fingerprint列是為了用於跨多個表加入數據。為此，產生的密文大小必須始終相同。不過，這些欄會受到協同作業層級設定的影響。 Fingerprint欄可能會對輸出檔案大小產生不同程度的影響，具體取決於輸入中cleartext包含的大小。

主題

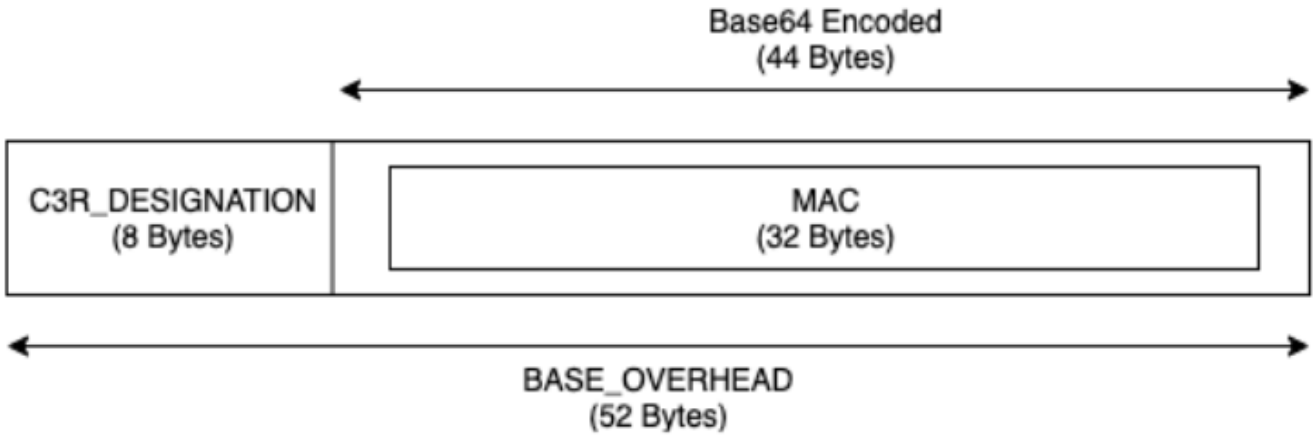
- fingerprint列的基本開銷
- fingerprint欄的協同合作設定
- 資料fingerprint欄的範例資料
- 疑難排解fingerprint欄

fingerprint列的基本開銷

有fingerprint列的基本開銷。這種開銷是恆定的，並代替cleartext字節的大小。

資料行中的資fingerprint料是透過雜湊型訊息驗證碼 (HMAC) 函式以密碼編譯方式處理，該函式會將資料轉換成 32 位元組訊息驗證碼 (MAC)。然後通過 base64 編碼器處理此數據，將字節大小增加了大約 33%。它會預先加上 8 位元組的 C3R 指定，以指定資料所屬的資料行類型以及產生資料行的用戶端版本。最終結果是 52 個字節。然後，將此結果乘以行計數以獲得總基本開銷（如果`preserveNulls`設置為 true，則使用非總`null`值的數量）。

下圖顯示了如何 *`BASE_OVERHEAD = C3R_DESIGNATION + (MAC * 1.33)`*



fingerprint列中的輸出密文將始終是 52 個字節。如果輸入cleartext資料的平均值超過 52 個位元組 (例如，完整的街道位址)，這可能會大幅減少儲存空間。如果輸入cleartext資料的平均值小於 52 個位元組 (例如，客戶年齡)，這可能會大幅增加儲存空間。

fingerprint欄的協同合作設定

`preserveNulls` 設定

當協同作業層級設定`preserveNulls`為 `false` (預設值) 時，每個`null`值都會以唯一的隨機 32 位元組取代，並以不相同的方式進行處理。`null`結果是，每個`null`值現在是 52 個字節。對於包含非常稀疏資料的資料表，這可能會增加顯著的儲存需求，相較於此設定為`true`且`null`值傳遞為`null`時間。

如果您不需要此設定的隱私權保證，而且偏好在資料集中保留`null`值，請在建立共同作業時啟用該`preserveNulls`設定。建`preserveNulls`立共同作業之後，就無法變更設定。

資料fingerprint欄的範例資料

以下是一組輸入和輸出資料的範例集，其fingerprint中包含要重現的設定。其他協作層級的設定，例如`allowCleartext`和`allowDuplicates`不影響結果，可以設定為`true`或`false`嘗試在本機複製。

共用密碼範例：`wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

協同作業 ID 範例：`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`

allowJoinsOnColumnsWithDifferentNames：`True`此設定不會影響效能或儲存需求。但是，當複製下表中顯示的值時，此設定會使欄名稱選擇不相關。

範例 1

輸入	`null`
`preserveNulls`	`TRUE`
輸出	`null`
確定性	`Yes`
輸入字節	0
輸出字節	0

範例 2

輸入	null
preserveNulls	FALSE
輸出	01:hmac:3lkFjthvV3IUu6mMvFc1a+XAHwgw/ElmOq4p3Yg25kk=
確定性	No
輸入字節	0
輸出字節	52

範例 3

輸入	empty string
preserveNulls	-
輸出	01:hmac:oKTgi3Gba+eUb3JteSz2EMgXUkF1WgM77UP0Ydw5kPQ=
確定性	Yes
輸入字節	0
輸出字節	52

範例 4

輸入	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
輸出	01:hmac:kU/IqwG7FMmzzshr0B9scomE0UJUEE7j9keTctplGww=
確定性	Yes

輸入字節	26
輸出字節	52

範例 5

輸入	`abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789`
`preserveNulls`	-
輸出	`01:hmac:ks3htnQbw2vdhCRFF6J NzW5LMndJaHG57uvE26mBtSs=`
确定性	`Yes`
輸入字節	62
輸出字節	52

疑難排解fingerprint欄

為什麼我的fingerprint列中的密文比進入cleartext它的大小大幾倍？

fingerprint列中的密文總是長度為 52 個字節。如果您輸入的數據很小（例如，客戶的年齡），則規模將顯著增加。如果`preserveNulls`設定設定為，也可能發生這種情況`false`。

為什麼我的fingerprint列中的密文比進入cleartext它的大小小小幾倍？

fingerprint列中的密文總是長度為 52 個字節。如果您輸入的數據很大（例如，客戶的完整街道地址），則大小將顯著減少。

我如何知道我是否需要由提供的加密保證？**`preserveNulls`**

不幸的是，答案是，這取決於。至少the section called “參數”應檢閱`preserveNulls`設定如何保護您的資料。不過，我們建議您參考組織的資料處理要求，以及適用於個別協同合作的任何合約。

為什麼我必須承擔 base64 的開銷？

為了允許與表格文件格式（例如 CSV）的兼容性，需要 base64 編碼。雖然某些檔案格式 (例如) Parquet 可能支援資料的二進位表示，但協同合作中的所有參與者都必須以相同的方式表示資料，以確保正確的查詢結果。

Sealed列

Sealed列是為了用於在協作的成員之間傳輸數據。這些資料行中的密碼文字不具決定性，並且會根據資料行的設定方式，對效能和儲存有重大影響。您可以個別設定這些資料行，而且通常會對 C3R 加密用戶端的效能和產生的輸出檔案大小造成最大的影響。

主題

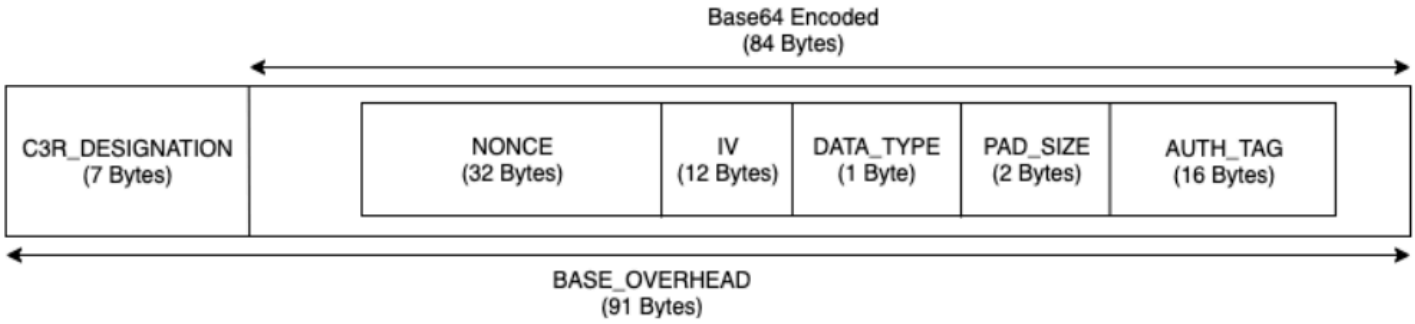
- sealed列的基本開銷
- sealed欄的協同合作設定
- 結構描述設定sealed欄：填補類型
- 資料sealed欄的範例資料
- 疑難排解sealed欄

sealed列的基本開銷

有sealed列的基本開銷。此開銷是恆定的，除了和填充（如果有cleartext的話）字節的大小之外。

在進行任何加密之前，資料行中的資sealed料會預先加上 1 個位元組字元，以指定所包含的資料類型。如果選擇填充，則數據被填充並附加 2 個字節，說明墊大小。新增這些位元組之後，會使用 AES-GCM 以密碼編譯方式處理資料，並使用 IV (12 位元組)、(32 位元組) 和 nonce Auth Tag (16 位元組) 來儲存資料。然後通過 base64 編碼器處理此數據，將字節大小增加了大約 33%。資料會預先加上 7 位元組 C3R 指定，以指定資料所屬的資料行類型，以及用來產生資料行的用戶端版本。結果是 91 個字節的最終基本開銷。然後，該結果可以乘以行計數以獲得總基本開銷（如果`preserveNulls`設置為 true，則使用非空值的總數）。

下圖顯示了如何 *`BASE_OVERHEAD = C3R_DESIGNATION + ((NONCE + IV + DATA_TYPE + PAD_SIZE + AUTH_TAG) * 1.33)`*



sealed欄的協同合作設定

`preserveNulls` 設定

當協同作業層級設定`preserveNulls`為 `false` (預設值) 時，每個`null`值都是唯一的，隨機 32 個位元組，並且會像處理不一樣。`null`結果是，每個`null`值現在是 91 個字節（如果填充更多）。對於包含非常稀疏資料的資料表，這可能會增加顯著的儲存需求，相較於此設定為`true`且`null`值傳遞為`null`時間。

如果您不需要此設定的隱私權保證，而且偏好在資料集中保留`null`值，請在建立共同作業時啟用該`preserveNulls`設定。建`preserveNulls`立共同作業之後，就無法變更設定。

結構描述設定sealed欄：填補類型

主題

- 墊片類型 none
- 墊片類型 fixed
- 墊片類型 max

墊片類型 `none`

選取的焊接類型`none`不會增加任何填充，cleartext並且不會為前面描述的基本開銷增加額外的開銷。沒有填充會產生最節省空間的輸出大小。但是，它不提供`fixed`與和`max`填充類型相同的隱私保證。這是因為底層的大小可以cleartext從密文的大小中辨別出來。

墊片類型 `fixed`

選取的填補類型`fixed`是隱私權保留計量，用於隱藏欄中包含的資料長度。這是通過在加密`pad_length`之前填充所提供的所有內cleartext容來完成的。任何超過該大小的資料都會導致 C3R 加密用戶端失敗。

鑑於填充在加密cleartext之前已添加到填充，因此 AES-GCM 具有對應到密文字節的 1 對 1。cleartext基礎 64 編碼將增加 33%。填充的額外存儲開銷可以通過cleartext從的值中減去的平均長度pad_length並將其乘以 1.33 來計算。其結果是每個記錄填充的平均開銷。然後，該結果可以乘以行數以獲得總填充開銷（如果preserveNulls設置為，則使用非總null值的數量true）。

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

我們建議您選取包pad_length含欄中最大值的最小值。例如，如果最大值為 50 個字節，則 50 pad_length 的 a 就足夠了。大於此值的值只會增加額外的儲存空間負荷。

固定填充不會增加任何顯著的計算開銷。

墊片類型 **max**

選取的填補類型max是隱私權保留計量，用於隱藏欄中包含的資料長度。這是通過在加密pad_length之前cleartext將列中的所有值填充到最大值以及其他值來完成的。通常，max填充提供與單個數據集fixed填充相同的保證，同時允許不知道列中的最大cleartext值。但是，max填充可能不會提供與跨更新fixed填充相同的隱私保證，因為個別資料集中的最大值可能會有所不同。

我們建議您在使用max填充時選取額外pad_length的 0。此長度會填補所有值，使其大小與欄中的最大值相同。大於此值的值只會增加額外的儲存空間負荷。

如果指定欄中已知最大cleartext值，建議您改用fixed墊片類型。使用fixed填補可在更新的資料集間建立一致 使用max填補會導致數據的每個子集被填充到子集中的最大值。

資料sealed欄的範例資料

以下是一組輸入和輸出資料的範例集，其sealed中包含要重現的設定。其他協同作業層級的設定 allowCleartextallowJoinsOnColumnsWithDifferentNames，例如、且allowDuplicates不會影響結果，而且可以設定為true或false嘗試在本機複製。雖然這些是要重現的基本設定，但sealed資料行是不具決定性的，而且每次都會變更值。目標是顯示與字節輸出相比的字節。範例pad_length值是有意選擇的。它們表明fixed填充結果與使用建議的最小pad_length設置max填充或需要其他填充時的填充相同的值。

共用密碼範例：wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

協同作業 ID 範例：a1b2c3d4-5678-90ab-cdef-EXAMPLE11111

主題

- 墊片類型 none

- 墊片類型 fixed (範例 1)
- 墊片類型 fixed (範例 2)
- 墊片類型 max (範例 1)
- 墊片類型 max (範例 2)

墊片類型 **none**

範例 1

輸入	null
preserveNulls	TRUE
輸出	null
確定性	Yes
輸入字節	0
輸出字節	0

範例 2

輸入	null
preserveNulls	FALSE
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSPbNIJfG3iXmu6cbCUrizuV
確定性	No
輸入字節	0
輸出字節	91

範例 3

輸入	empty string
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSPEM6qR8DWC2PB2GMlX41YK
確定性	No
輸入字節	0
輸出字節	91

範例 4

輸入	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9sGL5VLDQeHzh6DmPpyWNuI=
確定性	No
輸入字節	26
輸出字節	127

範例 5

輸入	abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqdP4/ QOQ3cXb/pbvPcnnohrHIGSX54ua+1/ JfcVjc=
確定性	No
輸入字節	62
輸出字節	175

墊片類型 **fixed** (範例 1)

在這個例子中，pad_length是 62，最大的輸入是 62 字節。

範例 1

輸入	null
preserveNulls	TRUE
輸出	null
確定性	Yes
輸入字節	0
輸出字節	0

範例 2

輸入	null
preserveNulls	FALSE
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=
確定性	No
輸入字節	0
輸出字節	175

範例 3

輸入	empty string
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=
確定性	No
輸入字節	0
輸出字節	175

範例 4

輸入	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=
確定性	No
輸入字節	26
輸出字節	175

範例 5

輸入	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6plwtH/8tRFnn2rF91bcB9G4+n8GiRfJNmqdP4/QOQ3cXb/pbvPcnnohrHIGSX54ua+1/JfcVjc=
確定性	No
輸入字節	62

輸出字節	175

墊片類型 **fixed** (範例 2)

在這個例子中，pad_length是 162，最大的輸入是 62 字節。

範例 1

輸入	null
preserveNulls	TRUE
輸出	null
確定性	Yes
輸入字節	0
輸出字節	0

範例 2

輸入	null
preserveNulls	FALSE
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb

確定性	No
輸入字節	0
輸出字節	307

範例 3

輸入	empty string
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT
確定性	No
輸入字節	0
輸出字節	307

範例 4

輸入	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY

	Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf
確定性	No
輸入字節	26
輸出字節	307

範例 5

輸入	abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/QOQ3cXb/pbvPcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i
確定性	No

輸入字節	62
輸出字節	307

墊片類型 **max** (範例 1)

在此範例中，pad_length為 0，最大輸入為 62 個位元組。

範例 1

輸入	null
preserveNulls	TRUE
輸出	null
確定性	Yes
輸入字節	0
輸出字節	0

範例 2

輸入	null
preserveNulls	FALSE
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfssGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoNpATs0GzbnLkor4L+/aSuA=
確定性	No
輸入字節	0

輸出字節	175

範例 3

輸入	empty string
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfstGSNWfMRp7nSb7SMX2s3JKLOhK1+7r75Tk+Mx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcoLB53l07VZpA6OwkuXu29CA=
確定性	No
輸入字節	0
輸出字節	175

範例 4

輸入	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5MG5vbmNlMDEyMzQ1Njc4OTBqfRYZ98t5KU6aWfsteEE1GKEPiRzyh0h7t6OmWMLTWCvO2ckr6pkx9jy48Fcg1yOPvBqRSZ7oqy1V3UKfYTLEZb/hCz7oaIneVsrcutBAcO+Mb9tuU2KIHH31AWg=
確定性	No

輸入字節	26
輸出字節	175

範例 5

輸入	abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqdP4/ QOQ3cXb/pbvPcnnohrHIGSX54ua+1/ JfcVjc=
確定性	No
輸入字節	62
輸出字節	175

墊片類型 **max** (範例 2)

在這個例子中，pad_length是 100，最大的輸入是 62 字節。

範例 1

輸入	null
preserveNulls	TRUE
輸出	null
確定性	Yes

輸入字節	0
輸出字節	0

範例 2

輸入	null
preserveNulls	FALSE
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfssGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv/xAySX+xcntotL703aBTBb
確定性	No
輸入字節	0
輸出字節	307

範例 3

輸入	empty string
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfstGSNWfMRp7nSb7S MX2s3JKLOhK1+7r75Tk+Mx9jy48

	Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwv84lVaT9Yd+6oQx65/+gdVT
確定性	No
輸入字節	0
輸出字節	307

範例 4

輸入	abcdefghijklmnopqrstuvwxyz
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6pkx9jy48 Fcg1yOPvBqRSZ7oqy1V3UKfYTLE Zb/hCz7oaIneVsrcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwtX5Hnl+WyfO6ks3QMaRDGSf
確定性	No
輸入字節	26
輸出字節	307

範例 5

輸入	abcdefghijklmnopqrstuvwxyzA BCDEFGHIJKLMNOPQRSTUVWXYZ01 23456789
preserveNulls	-
輸出	01:enc:bm9uY2UwMTIzNDU2Nzg5 MG5vbmNlMDEyMzQ1Njc4OTBqfRY Z98t5KU6aWfsteEE1GKEPiRzyh0 h7t6OmWMLTWCvO2ckr6plwtH/8t RFnn2rF91bcB9G4+n8GiRfJNmqd P4/QOQ3cXb/pbvPcnkB0xbLWD7z NdAqQGR0rXoSESdW0I0vpNoGcBf v4cJbG0A3h1DvtkSSVc2B80OOGp pzdDqhrUVN5wFNyn8vgfPMqDaeJk5bn +8o4WtG/ClipNcjDXvXVtK4vfCohcCA6 uwrmwjkJXQZOgPdeFX9Yr/8alV5i
確定性	No
輸入字節	62
輸出字節	307

疑難排解sealed欄

為什麼我的sealed列中的密文比進入cleartext它的大小大幾倍？

這取決於幾個因素。首先，Cleartext列中的密文總是至少為 91 字節的長度。如果您輸入的數據很小（例如，客戶的年齡），則規模將顯著增加。其次，如果設置preserveNulls為，false並且您的輸入數據包含大量的null值，那麼這些null值中的每一個都將被轉換為 91 字節的密文。最後，如果您使用填充，根據定義，字節被加密之前添加到cleartext數據中。

我在一sealed列中的大部分數據都非常小，我需要使用填充。我可以刪除大值並單獨處理它們以節省空間嗎？

我們不建議您移除較大的值並個別處理它們。這樣做會變更 C3R 加密用戶端所提供的隱私權保證。作為威脅模型，假設觀察者可以看到兩個加密的數據集。如果觀察者看到一個數據子集的列填充顯著大於或少於另一個子集，他們可以對每個子集中的數據的大小進行推論。例如，假設fullName資料行在一個檔案中填滿總共 40 個位元組，而且在另一個檔案中填補到 800 個位元組。觀察者可能會假設一個數據集包含世界上最長的 name747 字節）。

使用填充類型時是否需要提供額外的**max**填充？

沒有 使用max填補時，我們建議將 (也稱為超出欄中最大值的額外填充) 設定為 0。pad_length

我可以在使用**fixed**填充**pad_length**時選擇一個大號，以避免擔心最大值是否適合？

是的，但是較大的墊片長度效率低下，並且使用了比必要的更多存儲空間。我們建議您檢查以查看最大值的大小，並將其設定pad_length為該值。

我如何知道我是否需要由提供的加密保證？**preserveNulls**

不幸的是，答案是，這取決於。至少密碼編譯運算 Clean Rooms應檢閱preserveNulls設定如何保護您的資料。不過，我們建議您參考組織的資料處理要求，以及適用於個別協同合作的任何合約。

為什麼我必須承擔 base64 的開銷？

為了允許與表格文件格式（例如 CSV）的兼容性，需要 base64 編碼。雖然某些檔案格式 (例如) Parquet 可能支援資料的二進位表示，但協同合作中的所有參與者都必須以相同的方式表示資料，以確保正確的查詢結果。

疑難排解密文大小意外增加

假設您加密了數據，並且生成的數據的大小非常大。下列步驟可協助您識別大小增加的位置，以及您可以採取的動作 (如果有的話)。

確定大小增加發生的地方

在疑難排解加密資料大於資料的原因之前，您cleartext必須先確定大小增加的位置。 Cleartext列可以安全地被忽略，因為它們是不變的。查看剩餘的fingerprint和sealed列，然後選擇一個看起來很重要的列。

確定大小增加發生的原因

資fingerprint料行或sealed資料行可能會導致大小增加。

主題

- 大小增加是來自fingerprint列嗎？
- 大小增加是來自sealed列嗎？

大小增加是來自fingerprint列嗎？

如果最有助於增加儲存空間的資料行是一個資料fingerprint欄，這可能是因為cleartext資料很小 (例如，客戶年齡)。每個產生的fingerprint密文長度為 52 個位元組。不幸的是，沒有什麼可以做這個問題的 column-by-column 基礎上。如需詳細資訊，請參閱此fingerprint列的基本開銷資料行的詳細資訊，包括它如何影響儲存需求。

fingerprint欄中大小增加的另一個可能原因是協同作業設定`preserveNulls`。如果停用的協同作業設定 (預設設定)，fingerprint資料行中的所有`null`值都會變成 52 個位元組的加密文字。`preserveNulls`在目前的協同合作中，沒有任何事情可以做到這一點。建立協同作業時會`preserveNulls`設定此設定，且所有協同合作者都必須使用相同的設定，才能確保查詢結果正確無誤。有關`preserveNulls`設置以及啟用它如何影響數據的隱私保證的更多信息，請參閱。密碼計算

大小增加是來自sealed列嗎？

如果最有助於增加儲存空間的資料行是一個資料sealed欄，則有一些細節可能會導致大小增加。

如果數cleartext據很小（例如，客戶年齡），則每個產生的sealed密文長度至少為 91 個字節。不幸的是，對此問題無法做任何事情。如需詳細資訊，請參閱此sealed列的基本開銷資料行的詳細資訊，包括它如何影響儲存需求。

sealed列中存儲增加的第二個主要原因是填充。填充會在加密cleartext之前將額外的位元組加入，以隱藏資料集中個別值的大小。我們建議您將數據集的填充設置為最小可能的值。至少，`fixed`填充必須設置`pad_length`為包含列中的最大可能值。任何比這更高的設置都不會增加額外的隱私保證。例如，如果您知道資料行中的最大可能值可以是 50 個位元組，建議您將設定`pad_length`為 50 個位元組。不過，如果資sealed料行使用`max`填充，我們建議您將設定`pad_length`為 0 個位元組。這是因為`max`填充指的是超出列中最大值的附加填充。

sealed欄中大小增加的最後可能原因是協同合作設定`preserveNulls`。如果停用的協同作業設定 (預設設定)，sealed資料行中的所有`null`值都會變成 91 位元組的加密文字。`preserveNulls`在目前的協同合作中，沒有任何事情可以做到這一點。此`preserveNulls`設定是在建立協同合作時設定的，且所有協同合作者都必須使用相同的設定，才能確保查詢結果正確無誤。有關此設置的更多信息以及啟用它如何影響數據的隱私保證，請參閱。密碼計算

查詢登入 AWS Clean Rooms

查詢記錄是中的一項功能 AWS Clean Rooms。當您建立協作並開啟查詢記錄時，成員可以在 Amazon Logs 中存放與其相關的查詢 CloudWatch 日誌。

使用查詢記錄檔，成員可以判斷查詢是否符合分析規則，並符合協同合作合約。此外，查詢記錄還有助於支援稽核。

在 AWS Clean Rooms 主控台中開啟 [查詢記錄] 選項時，查詢記錄檔包括下列項目：

- `analysisRule`— 已配置表格的分析規則。
- `analysisTemplateArn`-已執行的分析範本 (根據分析規則顯示)。
- `collaborationId`— 執行查詢之協同作業的唯一識別元。
- `configuredTableID`— 查詢中參照之已配置資料表的唯一識別元。
- `directQueryAnalysisRulePolicy.custom.allowedAnalysis`— 允許在已配置表格上執行的分析範本 (視分析規則而定)。
- `directQueryAnalysisRulePolicy.v1.custom.allowedAnalysisProviders`— 允許建立查詢的查詢提供者 (根據分析規則顯示)。
- `eventID`— 查詢執行的唯一識別元。在 2023 年 8 月 31 日之後，唯一識別碼與. `protectedQueryID`
- `eventTimestamp`— 查詢執行時間。
- `parameters.parametervalue`— 參數值 (根據查詢文字顯示)。
- `queryText`— 執行查詢的 SQL 定義。如果有參數，則會標示為`:parametervalue`。
- `queryValidationErrors`— 查詢驗證時的查詢錯誤。
- `schemaName`— 查詢中參照的已配置資料表關聯名稱。

接收查詢記錄

您不需要在以外執行任何動作即可設 AWS Clean Rooms 定查詢記錄。 AWS Clean Rooms 在每個協同作業成員建立成員資格後，建立共同作業的記錄群組。

可以查詢的成員、可以接收結果的成員，以及在查詢中參照其組態資料表的成員，都會收到查詢記錄。

可以查詢的成員和可以接收結果的成員將會收到查詢中所參照之每個已設定資料表的查詢記錄。如果他們不擁有配置的表，他們將無法查看配置的表 ID（`configuredTableID`）。

如果成員在查詢中參照了多個已設定的資料表關聯，他們將會收到每個已設定資料表的查詢記錄檔。

系統會針對中包含不受支援和受支援 SQL 的查詢建立記錄 AWS Clean Rooms。如需詳細資訊，請參閱 AWS Clean Rooms SQL 參考。

當查詢參照與協同作業無關聯的已設定資料表時，也會建立記錄檔。

中不會針對不正確的 SQL 建立記錄檔 AWS Clean Rooms。

查詢記錄檔不會指出查詢已成功，而且查詢輸出已傳遞。他們確認查詢是由可以查詢的成員提交的。查詢記錄檔也會確認查詢中包含支援的 SQL，以 AWS Clean Rooms 及參考與協同作業相關聯的已設定資料表。

Example

例如，如果查詢在 AWS Clean Rooms 驗證其符合分析規則和查詢處理期間取消，則不會產生記錄檔。

如果您刪除記錄群組，您必須以相同的記錄群組名稱 (協同作業的協同作業 ID) 手動重新建立記錄群組。或者，您可以在會員資格中關閉和開啟登出功能。

如需如何開啟查詢記錄的詳細資訊，請參閱在中建立協同作業 AWS Clean Rooms。

如需 Amazon CloudWatch 日誌的詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。

使用查詢記錄

我們建議會員定期採取以下行動：

- 若要確認查詢是否符合共同作業所商定的使用案例或查詢，請檢閱在協同作業中執行的查詢。

  如需如何檢視最近查詢的詳細資訊，請參閱檢視最近的查詢。
- 若要確認已配置的表格資料欄是否符合協同合作的同意內容，請檢閱用於協同合作成員分析規則與查詢中的已配置表格資料欄。

  如需如何檢視已配置資料行的詳細資訊，請參閱檢視表格和分析規則。

設定 AWS Clean Rooms

下列主題說明如何設定 AWS Clean Rooms。

主題

註冊成為 AWS

在您可以使用任何 AWS 服務 AWS Clean Rooms, 包括, 你必須註冊 AWS.

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。
3. 當您註冊時 AWS 帳戶，系統會建立一個 AWS 帳戶 root 使用者。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行 需要根使用者存取權的任務。

設定下列項目的服務角色 AWS Clean Rooms

主題

建立管理員使用者

若要使用 AWS Clean Rooms，您必須為自己建立管理員使用者，並將管理員使用者新增至管理員群組。

若要建立管理員使用者，請選擇下列其中一個選項。

選擇一種管理管理員的方式	到	By	您也可以
在 IAM Identity Center (建議)	使用短期憑證存取 AWS。 這與安全性最佳實務一致。有關最佳實務的資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。	請遵循 AWS IAM Identity Center 使用者指南的入門中的說明。	AWS IAM Identity Center 在《使用AWS Command Line Interface 者指南》中設定 AWS CLI 要使用的，以設定程式設計方式存取。
在 IAM 中 (不建議使用)	使用長期憑證存取 AWS。	請遵循 IAM 使用者指南中建立您的第一個 IAM 管理員使用者和使用者群組的說明。	請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰，設定程式設計存取。

為協作成員建立 IAM 角色

成員是指身為協同作業參與者的 AWS 客戶。

若要為協作成員建立 IAM 角色

1. 遵循使用者指南中的建立角色，將許可委派給 IAM AWS Identity and Access Management 使用者程序。
2. 在 [建立原則] 步驟中，選取 [原則編輯器] 中的 [JSON] 索引標籤，然後根據授與協同作業成員的權能新增原則。

AWS Clean Rooms 根據一般使用案例提供下列受管理的策略：

如果您想要...	然後使用...
檢視資源和中繼資料	AWS 受管理的策略：AWSCleanRoomsReadOnlyAccess
Query	AWS 受管理的策略：AWSCleanRoomsFullAccess
查詢和接收結果	AWS 受管理的策略：AWSCleanRoomsFullAccess
管理協同合作資源，但不查詢	AWS 受管理的策略：AWSCleanRoomsFullAccessNoQuerying

如需有關由所提供之不同受管理策略的資訊 AWS Clean Rooms，請參閱 AWS 受管理的政策 AWS Clean Rooms

建立服務角色以讀取資料

AWS Clean Rooms 使用服務角色來讀取資料。

建立此服務角色的方法有兩種：

如果...	然後
您擁有建立服務角色所需的 IAM 許可	使用主 AWS Clean Rooms 控台建立服務角色。
您沒`iam:CreateRole` 有`iam:CreatePolicy` 權`iam:AttachRolePolicy` 限 或 您想要手動建立 IAM 角色	執行以下任意一項： • 請使用下列程序來建立服務角色。 • 請您的系統管理員使用下列程序建立服務角色。

若要建立服務角色以讀取資料

> **Note**
>
> 如果您沒有使用 AWS Clean Rooms 主控台建立服務角色的必要權限，您或您的 IAM 管理員才應遵循此程序。

1. 請遵循「使用AWS Identity and Access Management 者指南」中的「使用自訂信任原則 (主控台) 建立角色」程序。
2. 根據使用自訂信任原則 (主控台) 建立角色程序，使用下列自訂信任原則。

> **Note**
>
> 如果您要確保角色只能在特定協同合作成員資格的前後關聯中使用，則可以進一步縮小信任原則的範圍。如需詳細資訊，請參閱 預防跨服務混淆代理人。

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

3. 根據使用自訂信任原則 (主控台) 建立角色程序，使用下列權限原則。

> **Note**
>
> 下列範例政策支援讀取 AWS Glue 中繼資料及其對應 Amazon S3 資料所需的許可。但是，您可能需要修改此政策，具體取決於您設定 S3 資料的方式。例如，如果您已為 S3 資料設定自訂 KMS 金鑰，則可能需要使用其他 AWS KMS 許可修改此政策。

您的 AWS Glue 資源和基礎 Amazon S3 資源必須與協同 AWS Clean Rooms 合 AWS 區域 作相同。

```
{
    "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. 以您自己的資訊取代每個####。
5. 繼續遵循使用自訂信任原則建立角色 (主控台) 程序來建立角色。

建立服務角色以接收結果

> **Note**
>
> 如果您是只能收到結果的成員（在控制台中，您的會員能力僅為接收結果），請按照此步驟操作。

如果您是可以查詢和接收結果的成員（在控制台中，您的會員能力既是查詢和接收結果），則可以跳過此過程。

對於只能收到結果的協作成員，請 AWS Clean Rooms 使用服務角色將協作中查詢資料的結果寫入指定的 Amazon S3 儲存貯體。

建立此服務角色的方法有兩種：

如果...	然後
您擁有建立服務角色所需的 IAM 許可	使用主 AWS Clean Rooms 控台建立服務角色。
您沒`iam:CreateRole` 有`iam:CreatePolicy` 權`iam:AttachRolePolicy` 限 或 您想要手動建立 IAM 角色	執行以下任意一項： • 請使用下列程序來建立服務角色。 • 請您的系統管理員使用下列程序建立服務角色。

若要建立服務角色以接收結果

> **Note**
>
> 如果您沒有使用 AWS Clean Rooms 主控台建立服務角色的必要權限，您或您的 IAM 管理員才應遵循此程序。

1. 請遵循「使用AWS Identity and Access Management 者指南」中的「使用自訂信任原則 (主控台) 建立角色」程序。
2. 根據使用自訂信任原則 (主控台) 建立角色程序，使用下列自訂信任原則。

```
{
    "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. 根據使用自訂信任原則 (主控台) 建立角色程序，使用下列權限原則。

> **Note**
>
> 下列範例政策支援讀取 AWS Glue 中繼資料及其對應 Amazon S3 資料所需的許可。但是，您可能需要修改此政策，具體取決於您設定 S3 資料的方式。
> 您的 AWS Glue 資源和基礎 Amazon S3 資源必須與協同 AWS Clean Rooms 合 AWS 區域 作相同。

```
{
    "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. 用您自己的信息替換每個*###*：

   - *##* — 的名稱 AWS 區域。例如 **us-east-1**。
   - *A1b2C3D4-5678-90* AB-例子 — 可以查詢的成員的會員 ID。您可以在協同作業的 [詳細資料] 索引標籤上找到成員資格 ID。這樣 AWS Clean Rooms 可確保只有當此成員在此協同合作中執行分析時，才會擔任該角色。

- *ARN: AWS: ###:####-1:5555555555: ##/A1b2C3D4-5678-90B-#*子 — 可以查詢的成員的單一會員 ARN. 您可以在協同作業的 [詳細資料] 索引標籤上找到成員資格 ARN。這樣可以確保 AWS Clean Rooms 只有在此成員在此協同合作中執行分析時才會擔任該角色。
- *## – S3* 儲存貯體的 Amazon 資源名稱 (ARN)。您可以在 Amazon S3 儲存貯體的「屬性」索引標籤上找到 Amazon 資源名稱 (ARN)。
- *accountId* — S3 儲存貯體所在的 AWS 帳戶 識別碼。

  *##/##_key_### – S3 ###### **Amazon #### (ARN***)。您可以在 Amazon S3 儲存貯體的「屬性」索引標籤上找到 Amazon 資源名稱 (ARN)。

5. 繼續遵循使用自訂信任原則建立角色 (主控台) 程序來建立角色。

設定 AWS Clean Rooms ML 的服務角色

主題

- 建立服務角色以讀取訓練資料
- 建立服務角色以撰寫相似區段
- 建立服務角色以讀取種子資料

建立服務角色以讀取訓練資料

AWS Clean Rooms 使用服務角色來讀取訓練資料。如果您擁有必要的 IAM 許可，則可以使用主控台建立此角色。如果您沒有`CreateRole`權限，請要求管理員建立服務角色。

若要建立服務角色以訓練資料集

1. 使用您的管理員帳戶登入 IAM 主控台 (https://console.aws.amazon.com/iam/)。
2. 在 Access management (存取管理) 下，請選擇 Policies (政策)。
3. 選擇 Create policy (建立政策)。
4. 在 [原則編輯器] 中，選取 [JSON] 索引標籤，然後複製並貼上下列原則。

> **Note**
>
> 下列範例政策支援讀取 AWS Glue 中繼資料及其對應 Amazon S3 資料所需的許可。但是，您可能需要修改此政策，具體取決於您設定 S3 資料的方式。此原則不包含用於解密資料的 KMS 金鑰。

您的 AWS Glue 資源和基礎 Amazon S3 資源必須與協同 AWS Clean Rooms 合 AWS 區域 作相同。

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

如果您需要使用 KMS 金鑰來解密資料，請將此 AWS KMS 陳述式新增至先前的範本：

```
{
            "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. 選擇下一步。
6. 對於檢閱和建立，請輸入策略名稱和說明，然後檢閱摘要。
7. 選擇建立政策。

   您已針對建立策略 AWS Clean Rooms。
8. 在 Access management (存取管理) 下，請選擇 Roles (角色)。

   使用角色時，您可以建立短期認證，建議您提高安全性。您也可以選擇 [使用者] 建立長期認證。
9. 選擇建立角色。
10. 在 [建立角色] 精靈中，針對 [信任的實體類型] 選擇 [自訂信任原則]。
11. 將以下自訂信任原則複製並貼到 JSON 編輯器中。

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

```
}
```

永遠SourceAccount是您的 AWS 帳戶。SourceArn可以限制為特定的訓練資料集，但只能在建立該資料集之後。因為您無法預先知道訓練資料集 ARN，因此會在此指定萬用字元。

12. 選擇 [下一步]，然後在 [新增權限] 底下輸入您剛建立的原則名稱。（您可能需要重新加載頁面。）
13. 選取您建立之原則名稱旁的核取方塊，然後選擇 [下一步]。
14. 在名稱、檢閱和建立中，輸入角色名稱和說明。

> **Note**
>
> 角色名稱必須與授予可查詢和接收結果和成員角色的成員passRole權限中的模式相符。

    a. 檢閱選取信任的實體，並視需要進行編輯。
    b. 檢閱新增權限中的權限，並視需要進行編輯。
    c. 檢閱標籤，並視需要新增標籤。
    d. 選擇建立角色。
15. AWS Clean Rooms 已建立的服務角色。

建立服務角色以撰寫相似區段

AWS Clean Rooms 使用服務角色將相似區段寫入值區。如果您擁有必要的 IAM 許可，則可以使用主控台建立此角色。如果您沒有CreateRole權限，請要求管理員建立服務角色。

若要建立服務角色以撰寫相似區段

1. 使用您的管理員帳戶登入 IAM 主控台 (https://console.aws.amazon.com/iam/)。
2. 在 Access management (存取管理) 下，請選擇 Policies (政策)。
3. 選擇 Create policy (建立政策)。
4. 在 [原則編輯器] 中，選取 [JSON] 索引標籤，然後複製並貼上下列原則。

> **Note**
>
> 下列範例政策支援讀取 AWS Glue 中繼資料及其對應 Amazon S3 資料所需的許可。但是，您可能需要修改此政策，具體取決於您設定 S3 資料的方式。此原則不包含用於解密資料的 KMS 金鑰。

您的 AWS Glue 資源和基礎 Amazon S3 資源必須與協同 AWS Clean Rooms 合 AWS 區域 作相同。

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

如果您需要使用 KMS 金鑰來加密資料，請將此 AWS KMS 陳述式新增至範本：

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

如果您需要使用 KMS 金鑰來解密資料，請將此 AWS KMS 陳述式新增至範本：

```
{
            "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. 選擇下一步。
6. 對於檢閱和建立，請輸入策略名稱和說明，然後檢閱摘要。
7. 選擇建立政策。

   您已針對建立策略 AWS Clean Rooms。
8. 在 Access management (存取管理) 下，請選擇 Roles (角色)。

   使用角色時，您可以建立短期認證，建議您提高安全性。您也可以選擇 [使用者] 建立長期認證。
9. 選擇建立角色。
10. 在 [建立角色] 精靈中，針對 [信任的實體類型] 選擇 [自訂信任原則]。
11. 將以下自訂信任原則複製並貼到 JSON 編輯器中。

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

永遠SourceAccount是您的 AWS 帳戶。SourceArn可以限制為特定的訓練資料集，但只能在建立該資料集之後。因為您無法預先知道訓練資料集 ARN，因此會在此指定萬用字元。

12. 選擇下一步。
13. 選取您建立之原則名稱旁的核取方塊，然後選擇 [下一步]。
14. 在名稱、檢閱和建立中，輸入角色名稱和說明。

> **Note**
>
> 角色名稱必須與授予可查詢和接收結果和成員角色的成員`passRole`權限中的模式相符。

    a. 檢閱選取信任的實體，並視需要進行編輯。
    b. 檢閱新增權限中的權限，並視需要進行編輯。
    c. 檢閱標籤，並視需要新增標籤。
    d. 選擇建立角色。
15. AWS Clean Rooms 已建立的服務角色。

建立服務角色以讀取種子資料

AWS Clean Rooms 使用服務角色來讀取種子資料。如果您擁有必要的 IAM 許可，則可以使用主控台建立此角色。如果您沒有`CreateRole`權限，請要求管理員建立服務角色。

若要建立服務角色以讀取種子資料

1. 使用您的管理員帳戶登入 IAM 主控台 (https://console.aws.amazon.com/iam/)。
2. 在 Access management (存取管理) 下，請選擇 Policies (政策)。
3. 選擇 Create policy (建立政策)。
4. 在 [原則編輯器] 中，選取 [JSON] 索引標籤，然後複製並貼上下列原則。

> **Note**
>
> 下列範例政策支援讀取 AWS Glue 中繼資料及其對應 Amazon S3 資料所需的許可。但是，您可能需要修改此政策，具體取決於您設定 S3 資料的方式。此原則不包含用於解密資料的 KMS 金鑰。
> 您的 AWS Glue 資源和基礎 Amazon S3 資源必須與協同 AWS Clean Rooms 合 AWS 區域 作相同。

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

如果您需要使用 KMS 金鑰來解密資料，請將此 AWS KMS 陳述式新增至範本：

```
{
```

```
            "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. 選擇下一步。
6. 對於檢閱和建立，請輸入策略名稱和說明，然後檢閱摘要。
7. 選擇建立政策。

   您已針對建立策略 AWS Clean Rooms。
8. 在 Access management (存取管理) 下，請選擇 Roles (角色)。

   使用角色時，您可以建立短期認證，建議您提高安全性。您也可以選擇 [使用者] 建立長期認證。
9. 選擇建立角色。
10. 在 [建立角色] 精靈中，針對 [信任的實體類型] 選擇 [自訂信任原則]。
11. 將以下自訂信任原則複製並貼到 JSON 編輯器中。

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

永遠SourceAccount是您的 AWS 帳戶。SourceArn可以限制為特定的訓練資料集，但只能在建立該資料集之後。因為您無法預先知道訓練資料集 ARN，因此會在此指定萬用字元。

12. 選擇下一步。
13. 選取您建立之原則名稱旁的核取方塊，然後選擇 [下一步]。
14. 在名稱、檢閱和建立中，輸入角色名稱和說明。

> **Note**
>
> 角色名稱必須與授予可查詢和接收結果和成員角色的成員passRole權限中的模式相符。

    a. 檢閱選取信任的實體，並視需要進行編輯。
    b. 檢閱新增權限中的權限，並視需要進行編輯。
    c. 檢閱標籤，並視需要新增標籤。
    d. 選擇建立角色。
15. AWS Clean Rooms 已建立的服務角色。

在中建立協同作業 AWS Clean Rooms

協同作業是一種安全的邏輯界限，其AWS Clean Rooms中成員可以在已設定的資料表上執行 SQL 查詢。

中的任何成員都AWS Clean Rooms可以建立協同合作。

協同合作建立者可以指定要查詢和接收結果的單一成員。不過，協同合作建立者可能想要防止可查詢的成員存取查詢結果。在這種情況下，協同合作建立者可以指定一位可以查詢的成員，以及指定另一個可以接收結果的成員。

在大多數情況下，可以查詢的成員也是支付查詢計算費用的成員。不過，共同作業建立者可以設定不同的成員，以負責支付查詢運算成本。

如需如何使用 AWS SDK 建立共同作業的相關資訊，請參閱 AWS Clean RoomsAPI 參考。

主題

- 建立協同合作
- 後續步驟

建立協同合作

開始之前，請確定您已完成下列先決條件：

- 您有想要邀請加入協同作業的每個成員的名稱和 AWS 帳戶 ID。
- 您有權與共同作業的所有成員共用每個成員的名稱和 AWS 帳戶 ID。

> **Note**
>
> 您無法在建立共同作業後新增更多成員。

若要使用AWS Clean Rooms主控台建立協同作業

1. 登入AWS Management Console並開啟AWS Clean Rooms主控台，其中會以協同作業建立者的身分運作。AWS 帳戶

2. 在左側導覽窗格中，選擇「合作」。
3. 選擇右上角的 [建立共同作業]。
4. 對於步驟 1：定義協同合作，請執行下列操作：

   a. 在「詳細資訊」中，輸入協同作業的「名稱」與「說明」

      受邀參與協同合作的協同合作成員可以看到此資訊。「名稱」和「描述」可協助他們瞭解協同合作所參照的內容。

   b. 對於會員：

      i. 針對「成員 1：您」，輸入您希望協同作業顯示的「成員」顯示名稱。

      > **Note**
      >
      > 會員AWS 帳戶編號會自動包含您的 AWS 帳戶 ID。

      ii. 在「會員 2」中，輸入您要邀請加入協同作業之成員的「會員顯示名稱」和「會員 AWS 帳戶ID」。

      受邀加入協同作業的每個人都可以看到「成員」顯示名稱和「成員 AWS 帳戶 ID」。在您輸入並儲存這些欄位的值之後，就無法編輯這些欄位。

      > **Note**
      >
      > 您必須通知協同合作成員，協同作業中所有受邀和使用中的共同作業人員都可以看到他們的「成員 AWS 帳戶ID」和「成員」顯示名稱。

      iii. 如果您要新增其他成員，請選擇 [新增其他成員]。然後輸入會員顯示名稱和會員 AWS 帳戶 ID，這些成員可以提供您要邀請加入協同作業的資料。

   c. 對於會員能力，請選擇以下其中一項，

如果您想要…	然後...
查詢協同作業中的資料並接收結果	1. 選擇您自己作為可以執行查詢的成員。 2. 保留可接收結果之成員的預設設定為與執行查詢的使用者相同。

如果您想要...	然後...
查詢協同作業中的資料，並指派不同的成員以接收結果	1. 選擇您自己作為可以執行查詢的成員。 2. 從下拉式清單中選取可接收結果的成員。
接收合作中的查詢結果，並指派不同的成員來查詢資料	1. 從下拉式清單中選取可執行查詢的成員。 2. 選擇您自己作為可以從下拉列表中接收結果的會員。
建立和管理協同作業、指派不同成員以查詢資料，以及指派不同的成員以接收結果	1. 從下拉式清單中選取可執行查詢的成員。 2. 從下拉式清單中選取可接收結果的成員。

d. 對於付款設定，請選擇下列其中一項：

如果您想要...	然後...
將可執行查詢的成員指派為支付查詢計算費用的成員	保留將支付查詢費用的成員的預設設定為與執行查詢的使用者相同。
指派不同成員以支付查詢計算費用	從下拉式清單中選取要支付查詢費用的成員。

e. 如果您要啟用查詢記錄，請選取此協同作業的 Support 查詢記錄] 核取方塊。

f. 如果您要啟用密碼編譯運算功能，請選取 [在此協同作業中 Support 密碼編譯運算] 核取方塊，然後選擇下列密碼編譯運算參數：

- 允許cleartext欄

  如果您不希望加密資料表中允許cleartext資料欄，請選擇 [否]。

  如果您希望加密資料表中允許cleartext資料欄，請選擇 [是]。

  若要執行SUM或AVG在某些欄上執行，欄必須位於中cleartext。

- 允許重複

  如果您不希望fingerprint欄中允許重複的項目，請選擇「否」。

  如果要在欄位中允許重複項目，請選擇「是fingerprint」。

- 允許具有不同名稱JOIN的列

  如果您不想聯結不同名稱的fingerprint欄，請選擇「否」。

  如果您要聯結具有不同名稱的fingerprint欄，請選擇 [是]。

- 保留NULL值

  如果您不想保留NULL值，請選擇「否」。 NULL值不會顯示NULL在加密資料表中。

  如果您要保留NULL值，請選擇「是」。 NULL值會顯示為NULL在加密資料表中。

如需密碼編譯運算參數的詳細資訊，請參閱密碼計算參數。

如需如何加密資料以供中使用的詳細資訊AWS Clean Rooms，請參閱使用密碼編譯運算準備加密資料表 Clean Rooms。

> **Note**
>
> 在完成下一個步驟之前，請仔細驗證這些組態。建立協作後，您只能編輯協作名稱、說明，以及查詢日誌是否存放在 Amazon CloudWatch Logs 中。

g. 如果您要為協同作業資源啟用「標籤」，請選擇「新增標籤」，然後輸入「金鑰」與「值」配對。

h. 選擇 下一步。

5. 對於步驟 2：設定成員資格，請執行下列動作：

   a. 選擇一個選項：

如果選擇...	然後...
是的，立即建立會員即加入	共同作業和您的會員資格都會建立。 您在協同作業中的狀態為作用中。

如果選擇…	然後...
不會，我稍後會建立會員資格	只會建立協同合作。 您在合作中的狀態為「非活動」狀態。

b. 如果您是可以接收結果的成員，請在查詢結果設定預設值下選擇一個選項：

如果你...	然後...
保持選取 [立即設定預設設定] 核取方塊。(依預設會選取此選項。)	1. 對於 Amazon S3 中的結果目的地，請輸入 Amazon S3 目的地。 2. 對於查詢結果格式，請選擇 [CSV] 或 [實木複合地板]。
清除「立即設定預設設定」 核取方塊	只會建立協同合作。 您在合作中的狀態為「非活動」狀態。

c. 如果您在步驟 4.e 中選擇啟用查詢記錄，請在 Amazon Logs 中選擇下列其中一個 CloudWatch 日誌儲存選項：

如果選擇…	然後...
開啟	與您相關的查詢日誌會儲存在 Amazon CloudWatch 日誌中。 每個成員只能接收他們起始的查詢或包含其資料的記錄。 可接收結果的成員也會收到以協同合作方式執行的所有查詢記錄，即使查詢中未存取其資料也是如此。
關閉	與您相關的查詢日誌不會存放在您的 Amazon CloudWatch 日誌帳戶中。

> **Note**
>
> 開啟查詢記錄後，可能需要幾分鐘的時間才能設定日誌儲存，並開始在 Amazon Logs 中接收 CloudWatch 日誌。在這短暫的期間內，可以查詢的成員可能會執行實際上並未傳送記錄檔的查詢。

d. 如果您想要啟用成員資格資源的標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。

e. 如果您是支付查詢費用的成員，請選取 [我同意支付此共同作業中的查詢計算成本] 核取方塊，以表示您接受。

> **Note**
>
> 您必須選取此核取方塊才能繼續。
> 如需如何計算定價的詳細資訊，請參閱定價 AWS Clean Rooms。

如果您是支付查詢運算成本的成員，但不支付可查詢的成員，建議您在達到預算上限時使用AWS Budgets設定預算AWS Clean Rooms並接收通知。如需有關設定預算的詳細資訊，請參閱AWS Cost Management使用者指南AWS Budgets中的使用管理成本。如需有關設定通知的詳細資訊，請參閱AWS Cost Management使用者指南中的針對預算通知建立 Amazon SNS 主題。如果已達到預算上限，您可以聯絡可以執行查詢或離開協同合作的成員。如果您離開共同作業，將不再允許執行查詢，因此您將不再需要支付查詢計算費用的費用。

f. 選擇 下一步。

6. 對於步驟 3：檢閱和建立，請執行下列操作：

a. 檢閱您為先前步驟所做的選取，並視需要進行編輯。

b. 選擇下列其中一項：

如果您選擇...	然後選擇...
透過協同合作建立會員資格 (是的，立即建立會員資格即可加入)	建立協同合作與成員
建立共同作業，目前不要建立成員資格 (否，我稍後會建立成員資格)	建立合作

成功建立協同合作之後，您可以在「協同作業」下看到協同合作詳細資訊頁面。

後續步驟

您現在已準備好：

- 準備要查詢的資料表。AWS Clean Rooms（如果要查詢自己的數據，則為可選。）
- 將配置的表格與您的協同合作相關聯。（如果要查詢自己的數據，則為可選。）
- 為配置的表格配置分析規則。（如果要查詢自己的數據，則為可選。）
- 建立成員資格並加入協同合作。
- 管理您的協同合作。

建立會員資格並加入協同合作

成員資格是當成員加入中的協同合作時所建立的資源 AWS Clean Rooms。

您可以以查詢資料的成員、可以接收查詢結果的成員或兩者的身分加入協同合作。您也可以以成員身分加入協同合作，支付查詢運算費用。所有成員都可以貢獻數據。

如需如何使用 AWS SDK 建立成員資格和加入共同作業的詳細資訊，請參閱 AWS Clean Rooms API 參考。

主題

建立會員資格並加入協同合作

若要建立成員資格並加入協同合作

1. 登入 AWS Management Console 並與您的成員一起開啟AWS Clean Rooms 主機 AWS 帳戶。
2. 在左側導覽窗格中，選擇「合作」。
3. 在 [可加入] 索引標籤上，對於可加入的共同作業，選擇共同作業的名稱。
4. 在協同作業詳細資訊頁面上，檢視協同合作詳細資料，包括您的成員詳細資訊和其他成員的清單。

   確認共同作業中每個成員的 AWS 帳戶 ID 都是您要與其進行共同作業的 ID。
5. 選擇建立會員資格。
6. 在 [建立成員資格] 頁面的 [概觀] 中，檢視 [協同作業] 名稱、[協同合作] 說明、[協同合作] 建立者的 AWS 帳戶 ID、您的成員權能，以及將支付查詢費用的成員 ID。 AWS 帳戶
7. 如果協作建立者選擇啟用查詢記錄，請在 Amazon Logs 中選擇下列其中一個 CloudWatch 日誌儲存選項：

如果選擇...	然後...
開啟	與您相關的查詢日誌會儲存在 Amazon CloudWatch 日誌中。

如果選擇...	然後...
	每個成員只能接收其起始查詢或包含其資料的記錄。 可以接收結果的成員也會收到以協同合作方式執行的所有查詢記錄，即使查詢中未存取他們的資料也是如此。
關閉	與您相關的查詢日誌不會存放在您的 Amazon CloudWatch 日誌帳戶中。

> **Note**
>
> 開啟查詢記錄後，可能需要幾分鐘的時間才能設定日誌儲存，並開始在 Amazon Logs 中接收 CloudWatch 日誌。在這短暫的期間內，可以查詢的成員可能會執行實際上並未傳送記錄檔的查詢。

8. 如果您的會員能力包含「接收結果」：

   a. 對於「查詢結果」設定，

      i. 輸入 S3 目的地以指定 Amazon S3 中的結果目的地，或選擇瀏覽 S3 從可用 S3 儲存貯體清單中選取。

         Example

         例如：**`s3://bucket/prefix`**

      ii. 選擇結果格式（CSV 或實木複合地板）。

   b. 對於服務存取，請選擇 [建立和使用新的服務角色] 或 [使用現有的服務角色]。

> **Note**
>
> 您必須選取現有的服務角色或擁有建立新服務角色的權限。如需詳細資訊，請參閱 建立服務角色以接收結果。

9. 如果您想要啟用成員資格資源的標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。

10. 如果共同作業建立者已將您指定為將要支付查詢費用的成員，請選取 [我同意支付此共同作業中的查詢計算成本] 核取方塊，以表示您接受。

> **Note**
>
> 您必須選取此核取方塊才能繼續。
> 如需如何計算定價的詳細資訊，請參閱定價 AWS Clean Rooms。

如果您是支付查詢運算成本的成員，但不支付可查詢的成員，建議您在達到預算上限時使用 AWS Budgets 設定預算 AWS Clean Rooms 並接收通知。如需有關設定預算的詳細資訊，請參閱AWS Cost Management 使用者指南 AWS Budgets中的使用管理成本。如需有關設定通知的詳細資訊，請參閱AWS Cost Management 使用者指南中的針對預算通知建立 Amazon SNS 主題。如果已達到預算上限，您可以聯絡可以執行查詢或離開協同合作的成員。如果您離開共同作業，將不再允許執行查詢，因此您將不再需要支付查詢計算費用。

11. 如果您確定要建立成員資格並加入協同合作，請選擇 [建立成員資格]。

您將獲得協同作業中繼資料的讀取權限。除了其他成員的所有名稱和 AWS 帳戶 ID 之外，還包括協同作業的顯示名稱和說明等資訊。

如需如何離開協同合作的詳細資訊，請參閱離開合作。

後續步驟

您現在已準備好：

- 準備要查詢的資料表。 AWS Clean Rooms（如果要查詢自己的數據，則為可選。）
- 將配置的表格與您的協同合作相關聯。
- 為配置的表格配置分析規則。

準備查詢的資料表 AWS Clean Rooms

> **Note**
>
> 您可以在加入協同合作之前或之後準備資料表。準備好表格後，只要您對該表格的隱私需求相同，就可以在多個協作中重複使用它。

身為協同合作的成員，您必須先準備資料表，才能 AWS Clean Rooms 由可查詢的協同合作成員查詢資料表。

如果您的使用案例不需要您攜帶自己的資料，則可以略過此程序。

如果您的資料表已在中分類 AWS Glue，請跳至在中建立已配置的資料表 AWS Clean Rooms。

準備資料表包含下列步驟：

- 步驟 1：完成先決條件
- 步驟 2：(選擇性) 準備資料以進行密碼編譯運算
- 步驟 3：將您的資料表上傳到 Amazon S3
- 步驟 4：建立 AWS Glue 資料表
- 後續步驟

若要取得有關可用於查詢之資料格式的更多資訊，請參閱〈〉資料格式 AWS Clean Rooms。

步驟 1：完成先決條件

若要準備要搭配使用的資料表 AWS Clean Rooms，您必須完成下列先決條件：

- 您的資料集必須儲存為的其中一種支援的資料格式 AWS Clean Rooms。
- 您的資料表必須已分類， AWS Glue 並使用的支援資料類型。 AWS Clean Rooms
- 您的所有資料表都必須以建立協同作業的相同 AWS 區域 方式存放在 Amazon 簡單儲存服務 (Amazon S3) 中。
- AWS Glue Data Catalog 必須位於建立協同合作的相同區域中。
- 必 AWS Glue Data Catalog 須與會員資格 AWS 帳戶 相同。
- Amazon S3 存儲桶無法註冊 AWS Lake Formation。

- 協同合作建立者已在中設定協同合作 AWS Clean Rooms。如需詳細資訊，請參閱 在中建立協同作業 AWS Clean Rooms。
- 協同合作建立者已將協同合作 ID 以參與者的身分傳送給您。

步驟 2：(選擇性) 準備資料以進行密碼編譯運算

(選擇性) 如果您使用加密運算，且資料表包含您要加密的敏感資訊，則必須使用 C3R 加密用戶端來加密資料表。

若要準備資料以進行密碼編譯運算，請遵循中使用密碼編譯運算準備加密資料表 Clean Rooms的程序。

步驟 3：將您的資料表上傳到 Amazon S3

> **Note**
>
> 如果您打算在協同合作中使用加密資料表，則必須先加密資料以進行加密運算，然後再將資料表上傳到 Amazon S3。如需詳細資訊，請參閱 使用密碼編譯運算準備加密資料表 Clean Rooms。

將您的資料表上傳到 Amazon S3

1. 登入 AWS Management Console 並開啟 Amazon S3 主控台，網址為 https://console.aws.amazon.com/s3/。
2. 選擇「值區」，然後選擇要儲存資料表格的值區。
3. 選擇 [上傳]，然後依照提示進行。
4. 選擇 [物件] 索引標籤以檢視儲存資料的首碼。記下資料夾的名稱。

   您可以選取要檢視資料的資料夾。

步驟 4：建立 AWS Glue 資料表

如果您已經有一個 AWS Glue 數據表，則可以跳過此步驟。

在此步驟中，您可以在其中設定爬網程式， AWS Glue 以檢索 S3 儲存貯體中的所有檔案並建立 AWS Glue 資料表。如需詳細資訊，請參閱《AWS Glue 使用指南》AWS Glue中的〈定義爬行程式〉。

如需有關支援資 AWS Glue Data Catalog 料類型的詳細資訊，請參閱支援的資料類型。

> **Note**
>
> AWS Clean Rooms 目前不支援使用註冊的 S3 儲存貯體 AWS Lake Formation。

下列程序說明如何建立資 AWS Glue 料表。如果您想要使用具有 AWS Key Management Service (AWS KMS) 金鑰的加密 AWS Glue Data Catalog 物件，則需要設定 KMS 金鑰權限原則，以允許存取該加密資料表。如需詳細資訊，請參閱AWS Glue 開發人員指南中的 AWS Glue 中的設定加密。

建立 AWS Glue 表格的步驟

1. 請遵循「使用者指南」中的「在 AWS Glue 主控台上AWS Glue 使用檢索器」程序。
2. 記下 AWS Glue 數據庫名稱和 AWS Glue 表名。

後續步驟

現在您已準備好資料表，您可以：

- 建立已設定的資料表
- 建立 ML 模型

資料格式 AWS Clean Rooms

您用於查詢的資料集通 AWS Clean Rooms 常與您用於其他應用程式的資料集類型相同。例如，與 Amazon 雅典娜，Amazon EMR，Amazon Redshift Spectrum 和亞馬遜一起使用相同類型的數據集。QuickSight您可以直接從亞馬遜簡單儲存服務 (Amazon S3) 以原始格式查詢資料。

若要查詢資料，資料集必須採用 AWS Clean Rooms 支援的格式。包含資料集和 AWS Clean Rooms 叢集的 Amazon S3 儲存貯體必須位於同一個儲存貯體中 AWS 區域。

支援的資料格式

AWS Clean Rooms 支援下列結構化格式：

- 阿帕奇冰山表
- Parquet

- RCFile
- TextFile
- SequenceFile
- RegexSerde
- OpenCSV
- AVRO
- JSON

> **Note**
>
> 文字檔案中的timestamp值必須是格式yyyy-MM-dd HH:mm:ss.SSSSSS。例如：2017-05-01 11:30:59.000000.

我們建議使用單欄式儲存檔案格式，例如。Apache Parquet使用單欄式儲存檔案格式，您只需選擇所需的資料欄，即可最大幅度地減少 Amazon S3 中的資料傳輸。為了獲得最佳效能，大型物件應該分割成 100mb—1gb 物件。

支援的資料類型

為了獲得最佳體驗 AWS Clean Rooms，您必須將所有資料分類在中 AWS Glue。如需詳細資訊，請參閱開AWS Glue 發人員指南 AWS Glue Data Catalog中標題為開始使用的一節。

AWS Clean Rooms 支援下列 AWS Glue Data Catalog 資料類型：

- bigint
- boolean
- char
- date
- decimal
- double
- float
- int
- 嵌套數據類型，例如：

  - array
  - map
  - struct
- smallint
- string
- timestamp
- varchar

AWS Clean Rooms 不支援：

- binary
- 間隔

的檔案壓縮類型 AWS Clean Rooms

為了減少儲存空間、改善效能並將成本降至最低，我們強烈建議您壓縮資料集。

AWS Clean Rooms 根據檔案副檔名辨識檔案壓縮類型，並支援下表所示的壓縮類型和副檔名。

壓縮演算法	副檔名
GZIP	.gz
Bzip2	.bz2
Snappy	.snappy

您可以套用不同層級的壓縮。最常見的是，您可以壓縮整個檔案或壓縮檔案中的個別區塊。在檔案層級壓縮單欄格式並不會產生效能優勢。

伺服器端加密 AWS Clean Rooms

> **Note**
>
> 伺服器端加密不會取代需要它的使用案例的密碼編譯運算。

AWS Clean Rooms 透明地解密使用下列加密選項加密的資料集：

- SSE-S3 — 使用由 Amazon S3 管理的 AES-256 加密金鑰進行伺服器端加密
- SSE-KMS — 使用由管理的金鑰進行伺服器端加密 AWS Key Management Service

若要使用 SSE-S3，用來將已設定的資料表與協同作業相關聯的 AWS Clean Rooms 服務角色必須具有 KMS-解密權限。若要使用 SSE-KMS，KMS 金鑰原則也必須允許 AWS Clean Rooms 服務角色解密。

AWS Clean Rooms 不支援 Amazon S3 用戶端加密。如需伺服器端加密的詳細資訊，請參閱 Amazon 簡單儲存服務使用者指南中的使用伺服器端加密保護資料。

在中使用Apache Iceberg表格 AWS Clean Rooms

Apache Iceberg是資料湖的開放原始碼表格格式。 AWS Clean Rooms 可以使用儲存在中Apache Iceberg繼資料中的統計資料來最佳化查詢計畫，並減少無塵室查詢處理期間的檔案掃描 如需詳細資訊，請參閱 Apache 冰山文件。

AWS Clean Rooms 與冰山桌一起使用時，請考慮以下事項：

- AWS Glue Data Catalog 唯一的資料Apache Iceberg表 — 資料表必須 AWS Glue Data Catalog 根據開放原始碼膠合目錄實作來定義。
- 實木複合地板檔案格式 — AWS Clean Rooms 僅支援鑲木地板資料檔案格式的冰山表格。
- GZIP 和活潑的壓縮- AWS Clean Rooms 支持具有 GZIP 和壓縮的鑲木地板。Snappy
- 冰山版本- AWS Clean Rooms 支持對版本 1 和版本 2 冰山表運行查詢。
- 分割區 — 您不需要在中為Apache Iceberg表格手動新增分割區 AWS Glue。 AWS Clean Rooms 會自動偵測Apache Iceberg資料表中的新分割區，而且不需要手動操作即可更新資料表定義中的分割區。Iceberg 資料分割會在資料 AWS Clean Rooms 表結構定義中顯示為一般資料行，而不是分別顯示為已設定資料表結構定義中的資料分
- 限制
  - 僅限新冰山餐桌

    Apache Iceberg不支援從Apache Parquet表格轉換的表格。
  - 時間歷程查詢

    AWS Clean Rooms 不支援使用表格進行時間旅行查Apache Iceberg詢。
  - Athena 引擎版本 2

Iceberg不支援使用 Athena 引擎第 2 版建立的表格。

- 檔案格式

  Avro和「最佳化資料列」欄 (ORC) 檔案格式不受支援。

- 壓縮

  Zstandard不支援的 Parquet (Zstd) 壓縮。

冰山表格支援的資料類型

AWS Clean Rooms 可以查Iceberg詢包含下列資料類型的表格：

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

如需 Iceberg 資料類型的相關資訊，請參閱 Apache Iceberg 文件中的 Iceberg 結構描述。

使用密碼編譯運算準備加密資料表 Clean Rooms

Clean Rooms(C3R) 的密碼編譯運算是中的一項功能。 AWS Clean Rooms您可以使用 C3R 來限制任何一方和協同合作中可以學到的密碼編譯 AWS 內容。 AWS Clean Rooms

您可以先使用 C3R 加密用戶端 (一種用戶端加密工具) 加密資料表，然後再將資料表上傳到 Amazon Simple Storage Service (Amazon S3)。

如需詳細資訊，請參閱 密碼編譯運算 Clean Rooms。

使用 C3R 準備加密的資料表包含下列步驟：

步驟

步驟 1：完成先決條件

若要準備資料表以與 C3R 搭配使用，您必須完成下列先決條件：

- 您可以在 GitHub以下位置存取Clean Rooms儲存庫的密碼編譯運算：

  https://github.com/aws/c3r
- 您已設定使用 C3R 加密用戶端的 AWS 認證。C3R 加密用戶端會使用這些認證來進行唯讀 API 呼叫，以擷取協同作業中 AWS Clean Rooms 繼資料。如需詳細資訊，請參閱《第 2 版AWS Command Line Interface 使用者指南》 AWS CLI中的〈配置〉。
- 您的電腦上已安裝 Java Runtime Environment (JRE) 11 或更新版本。

  - 推薦的Java Runtime Environment，Amazon Corretto 11 或更高版本，可以從以下網址下載 https://aws.amazon.com/corretto。
  - 的Java Development Kit（JDK）包括相同版本JRE的相應的。不過，執行 Clean Rooms (C3R) 加密用戶端的「密碼編譯運算」不需要的其他功能。JDK
- 您的表格式資料檔案 (.csv) 或Parquet檔案 (. parquet) 會儲存在本機。
- 您或協同合作中的其他成員可以建立共用密鑰。如需詳細資訊，請參閱 步驟 5：建立共用密鑰。
- 協同作業建立者已在啟用密碼編譯運算 AWS Clean Rooms 的協同作業中建立協同作業。如需詳細資訊，請參閱 在中建立協同作業 AWS Clean Rooms。
- 協同合作建立者已將協同合作 ID 以參與者的身分傳送給您。合作 Amazon 資源名稱 (ARN) 包含在傳送的邀請中，其中包含協作 ID。

步驟 2：下載 C3R 加密用戶端

若要從下載 C3R 加密用戶端 GitHub

1. 前往Clean RoomsAWSGitHub儲存庫的密碼編譯運算：https://github.com/aws/c3r
2. 選擇並下載文件。

   源代碼，許可證和相關材料可以克隆或下載為. zip來自儲GitHub存庫登陸頁面的檔案。（請參閱存儲庫內容列表右上角的「代碼」按鈕）。

   最新簽署的 C3R 加密用戶端 Java Executable File (也就是指令行介面應用程式) 位於儲存庫的 [發行] 頁面上GitHub。

   對於 Apache 星火 C3R 加密客戶端包（`c3r-cli-spark`）是必須作為作業提交給正在運行的 Apache 星火服務器的 c3r-cli 的版本。如需詳細資訊，請參閱在阿帕奇星火上執行 C3R。

(選擇性) 步驟 3：檢視 C3R 加密用戶端中可用的命令

使用此程序來熟悉 C3R 加密用戶端中可用的命令。

檢視 C3R 加密用戶端中所有可用的命令

1. 從命令列介面 (CLI) 導覽至包含下載c3r-cli.jar檔案的資料夾。
2. 執行下列命令：`java -jar c3r-cli.jar`
3. 檢視可用命令和選項的清單。

步驟 4：為表格檔案產生加密結構描述

若要加密資料，需要描述資料使用方式的加密結構描述。本節說明 C3R 加密用戶端如何協助為含標題列或檔案的 CSV 檔案產生加密結構描述。Parquet

您只需要在每個文件中執行一次此操作。結構描述存在之後，就可以重複使用它來加密相同的檔案 (或任何具有相同資料行名稱的檔案)。如果資料行名稱或所需的加密結構描述變更，您必須更新結構描述檔案。如需詳細資訊，請參閱 (選擇性) 建立結構描述 (進階使用者)。

> **Important**
>
> 至關重要的是，所有合作方都使用相同的共享密鑰。如果合作方將JOIN被編輯或以其他方式比較查詢中的相等性，則合作方還應協調列名以匹配。否則，SQL 查詢可能會產生意外或不正確的結果。但是，如果協同合作建立者在協同合作建立期間啟用了`allowJoinsOnColumnsWithDifferentNames`加密設定，則不需要這樣做。如需加密相關設定的詳細資訊，請參閱。密碼計算參數

在結構描述模式下執行時，C3R 加密用戶端會逐欄瀏覽輸入檔案，提示您是否應該以及如何處理該資料行。如果檔案包含許多不需要加密輸出的資料行，互動式結構描述產生可能會變得繁瑣，因為您必須略過每個不需要的資料行。為了避免這種情況，您可以手動編寫結構描述，或創建僅包含所需列的輸入文件的簡化版本。然後，交互式架構生成器可以在該縮小的文件上運行。C3R 加密用戶端會輸出結構描述檔案的相關資訊，並詢問您應如何在目標輸出中包含或加密來源資料行 (如果有的話)。

對於輸入檔案中的每個來源欄，系統會提示您輸入：

1. 應該產生多少個目標資料行
2. 每個目標資料欄應如何加密 (如果有的話)
3. 每個目標資料欄的名稱
4. 如果資料行以資料行的形式加密，則在加密之前應如何填充資sealed料

> **Note**
>
> 當您針對已加密為資料行的資料行加密資sealed料時，必須判斷哪些資料需要填補。C3R 加密用戶端會在結構描述產生期間建議使用預設填補，將資料行中的所有項目填補至相同長度。在確定的長度時`fixed`，請注意填充是以字節為單位，而不是位。

以下是建立結構描述的決策表。

結構定義決策表

決策	來源資料欄中的目標資料行數 <' name-of-column '>?	目標資料欄類型：[c] cleartext fingerprint、[f] 或 [s]sealed？	目標資料欄標題名稱 <default 'name-of-column'>	將後綴添加 <suffix>到標題以指示它是如何加密的，[y] yes 或 [n] 否 <default 'yes'>	<' name-of-column _ 密封 '> 填補類型：[n] 一個，[f] 固定，或 [m] 最大值 <default 'max'>
保持未加密的資料欄。	1	c	不適用	不適用	不適用
將資料行加密為fingerprint資料行。	1	f	選擇預設值或輸入新的表頭名稱。	輸入y以選擇預設值 (`_fingerprint`) 或輸入n。	不適用
將資料行加密為sealed資料行。	1	s	選擇預設值或輸入新的表頭名稱。	輸入y以選擇預設值 (`_sealed`) 或輸入n。	選擇填充類型。 如需詳細資訊，請參閱(選擇性) 建立結構描述 (進階使用者)。
將資料行加密為fingerprint和sealed。	2	輸入第一個目標欄：f。 輸入第二個目標欄：s。	選擇每個目標欄的目標標題。	輸入y以選擇預設值或輸入n.	選擇填補類型 (僅適用於sealed欄)。 如需詳細資訊，請參閱(選擇性) 建立

決策	來源資料欄中的目標資料行數 <' name-of-column '>?	目標資料欄類型：[c] cleartext fingerprint、[f] 或 [s]sealed ?	目標資料欄標題名稱 <default 'name-of-column'>	將後綴添加 <suffix>到標題以指示它是如何加密的，[y] yes 或 [n] 否 <default 'yes'>	<' name-of-column _ 密封 '> 填補類型：[n] 一個，[f] 固定，或 [m] 最大值 <default 'max'>
					結構描述 (進階使用者)。

以下是如何建立加密結構描述的兩個範例。互動的確切內容取決於輸入檔案和您提供的回應。

範例

- 範例：產生資fingerprint料欄和資料欄的加密綱要 cleartext
- 範例：使用sealed、fingerprint和cleartext欄產生加密綱要

範例：產生資fingerprint料欄和資料欄的加密綱要 cleartext

在此範例中`ads.csv`，對於，只有兩欄：`username`和`ad_variant`。對於這些列，我們需要以下內容：

- 針對要加密為`username`資料`fingerprint`行的資料行
- 對於該`ad_variant`列是一`cleartext`列

若要產生資fingerprint料欄和資料行的加密結構描述 cleartext

1. (選擇性) 若要確保c3r-cli.jar要加密的檔案和檔案存在：

   a. 導航到所需的目錄並運行`ls`（如果使用Mac或Unix/Linux）或者`dir`如果使用Windows）。

   b. 檢視表格式資料檔案清單 (例如 .csv)，然後選擇要加密的檔案。

      在這個例子中，`ads.csv`是我們要加密的文件。

2. 從 CLI 執行下列命令，以互動方式建立結構描述。

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

> **Note**
>
> - 你可以`java --jar PATH/TO/c3r-cli.jar`跑 或者，如果您已`PATH/TO/c3r-cli.jar`將 CLASSPATH 環境變數加入，也可以執行類別名稱。C3R 加密客戶端將在 CLASSPATH 中查找以查找它（例如，）。`java com.amazon.psion.cli.Main`
> - 該`--interactive`標誌選擇用於開發模式的交互模式。這會引導使用者完成建立結構描述的精靈。具備進階技能的使用者可以建立自己的結構描述 JSON，而無需使用精靈。如需詳細資訊，請參閱 (選擇性) 建立結構描述 (進階使用者)。
> - 該`--output`標誌設置一個輸出名稱。如果您未包含該`--output`標誌，則 C3R 加密用戶端會嘗試挑選預設輸出名稱 (例如`<input>.out.csv`或結構描述)。`<input>.json`

3. 對於`Number of target columns from source column 'username'?`，請輸入，**1**然後按 Enter。
4. 對於`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`，請輸入，**f**然後按 Enter。
5. 對於`Target column headername <default 'username'>`，請按 Enter 鍵。

   使用預設名稱 `username` "。
6. 對於`Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`，請輸入，**y**然後按 Enter。

> **Note**
>
> 互動模式會建議新增至加密資料行標題的尾碼 (`_fingerprint`適用於fingerprint資料行和資料`_sealed`行sealed)。當您執行諸如上傳資料 AWS 服務 或建立 AWS Clean Rooms 共同作業等工作時，字尾可能會有所幫助。這些後綴有助於指示每個列中的加密數據可以做什麼。例如，如果您將列加密為 sealed column (`_sealed`) 並嘗試對其進行操作或嘗試反向操作，那麼事情將無法正常工作。JOIN

7. 對於`Number of target columns from source column 'ad_variant'?`，請輸入，**1**然後按 Enter。
8. 對於`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`，請輸入，**c**然後按 Enter。

9. 對於Target column headername <default 'username'>，請按 Enter 鍵。

   使用預設名稱 ad_variant "。

   結構描述會寫入名為的新檔案ads.json。

   > **Note**
   >
   > 您可以透過在任何文字編輯器中開啟資料架構來檢視資料架構，例如Notepad打開Windows或TextEdit打開macOS。

10. 您現在已準備好加密資料。

範例：使用sealed、fingerprint和cleartext欄產生加密綱要

在此範例中sales.csv，對於，有三欄：usernamepurchased、和product。對於這些列，我們需要以下內容：

- 對於該product列是一sealed列
- 針對要加密為username資料fingerprint行的資料行
- 對於該purchased列是一cleartext列

若要使用sealed、fingerprint和cleartext欄產生加密綱要

1. (選擇性) 若要確保c3r-cli.jar要加密的檔案和檔案存在：

   a. 導航到所需的目錄並運行ls（如果使用Mac或Unix/Linux）或者dir如果使用Windows）。

   b. 檢視表格式資料檔案 (.csv) 清單，然後選擇要加密的檔案。

      在這個例子中，sales.csv是我們要加密的文件。

2. 從 CLI 執行下列命令，以互動方式建立結構描述。

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

> **Note**
>
> - 該`--interactive`標誌選擇用於開發模式的交互模式。這會引導使用者完成建立結構描述的引導式工作流程。
> - 如果您是進階使用者，則無需使用引導式工作流程，即可建立自己的結構定義 JSON。如需詳細資訊，請參閱 (選擇性) 建立結構描述 (進階使用者)。
> - 對於沒有欄標題的 .csv 檔案，請參閱 CLI 中可用的結構描述命令的`--noHeaders`旗標。
> - 該`--output`標誌設置一個輸出名稱。如果您未包含該`--output`標誌，則 C3R 加密用戶端會嘗試挑選預設輸出名稱 (例如`<input>.out`或結構描述)。`<input>.json`

3. 對於`Number of target columns from source column ‘username’?`，請輸入，**1**然後按 Enter。
4. 對於`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`，請輸入，**f**然後按 Enter。
5. 對於`Target column headername <default 'username'>`，請按 Enter 鍵。

   使用預設名稱 `username`"。
6. 對於`Add suffix '_fingerprint' to header to indicate how it was encrypted, [y]es or [n]o <default 'yes'>`，請輸入，**y**然後按 Enter。
7. 對於`Number of target columns from source column ‘purchased’?`，請輸入，**1**然後按 Enter。
8. 對於`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`，請輸入，**c**然後按 Enter。
9. 對於`Target column headername <default 'purchased'>`，請按 Enter 鍵。

   使用預設名稱 `purchased`"。
10. 對於`Number of target columns from source column ‘product’?`，請輸入，**1**然後按 Enter。
11. 對於`Target column type: [c]leartext, [f]ingerprint, or [s]ealed?`，請輸入，**s**然後按 Enter。
12. 對於`Target column headername <default 'product'>`，請按 Enter 鍵。

    使用預設名稱 `product`"。

13. 對於‘product_sealed’ padding type: [n]one, [f]ixed, or [m]ax <default ’max’?>，按 Enter 選擇預設值。
14. 若要選擇預設值，請**Byte-length beyond max length to pad cleartext to in ‘product_sealed’ <default ‘0’>?**按 Enter 鍵。

    結構描述會寫入名為的新檔案sales.json。
15. 您現在已準備好加密資料。

步驟 5：建立共用密鑰

若要加密資料表，協同作業參與者必須同意並安全地共用共用密鑰。

共用密碼金鑰必須至少為 256 位元組 (32 位元組)。您可以指定較大的金鑰，但不會為您提供任何額外的安全性。

> **Important**
>
> 請記住，用於加密和解密的金鑰和協同作業 ID 對於所有協同作業參與者都必須相同。

以下各節提供了用於生成保存在各個終端機當前工作目錄secret.key中的共享密鑰的控制台命令的示例。

主題

- 範例：使用金鑰產生 OpenSSL
- 範例：Windows使用時產生金鑰 PowerShell

範例：使用金鑰產生 OpenSSL

對於一般用途密碼編譯程式庫，請執行下列命令來建立共用密碼金鑰。

```
openssl rand 32 > secret.key
```

如果您正在使用Windows且尚未OpenSSL安裝，則可以使用範例：在使用時產生金鑰中描述的範例Windows來產生金鑰PowerShell。

範例：Windows使用時產生金鑰 PowerShell

對於PowerShell上可用的終端機應用程式Windows，請執行下列命令以建立共用密鑰。

```
$bs = New-Object Byte[](32);
[Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($bs); Set-Content 'secret.key' -Encoding Byte -Value $bs
```

步驟 6：將共用密鑰存儲在環境變量中

環境變數是一種方便且可擴充的方式，可讓使用者從各種金鑰存放區提供私密金鑰， AWS Secrets Manager 並將其傳遞至 C3R 加密用戶端。

如果您使用 AWS CLI 將這些金鑰儲存在相關環境變數中， AWS 服務 則 C3R 加密用戶端可以使用儲存在中的金鑰。例如，C3R 加密用戶端可以使用來自的金鑰。 AWS Secrets Manager如需詳細資訊，請參閱AWS Secrets Manager 使用指南 AWS Secrets Manager中的使用建立和管理密碼。

> **Note**
>
> 但是，在使用 AWS 服務 諸如 AWS Secrets Manager 保存 C3R 密鑰之前，請確認您的用例是否允許它。某些用例可能需要保留密鑰。 AWS這是為了確保加密的數據和密鑰永遠不會被同一第三方持有。

共用密碼金鑰的唯一需求是共用密碼金鑰會經過base64編碼並儲存在環境變數`C3R_SHARED_SECRET`中。

以下各節說明將`secret.key`檔案轉換為base64並將其儲存為環境變數的主控台指令。`secret.key`檔案可能是從中列出的任何指令產生的，步驟 5：建立共用密鑰而且只是範例來源。

在Windows使用時將密鑰存儲在環境變量中 PowerShell

若要在使用時轉換為base64並設定環境變Windows數PowerShell，請執行下列命令。

```
$Bytes=[IO.File]::ReadAllBytes((Get-Location).ToString()+'\secret.key');
 $env:C3R_SHARED_SECRET=[Convert]::ToBase64String($Bytes)
```

將密鑰存儲在Linux或上的環境變量 macOS

若要在Linux或上轉換base64並設定環境變數macOS，請執行下列命令。

```
export C3R_SHARED_SECRET="$(cat secret.key | base64)"
```

步驟 7：加密資料

若要執行此步驟，您必須取得 AWS Clean Rooms 協同作業 ID 和共用密碼金鑰。如需詳細資訊，請參閱必要條件。

在下面的例子中，我們運行加密ads.csv，使用我們創建的模式稱為ads.json。

若要加密資料

1. 將共同作業的共用密碼金鑰儲存在中步驟 6：將共用密鑰存儲在環境變量中。
2. 在指令行中，輸入下列命令。

   ```
   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. 在中<name of input .csv file>，輸入輸入 .csv 檔案的名稱。
4. 在中schema=，輸入 .json 加密結構描述檔案的名稱。
5. 在中id=，輸入協同作業 ID。
6. 對於output=，輸入輸出檔案的名稱 (例如，ads-output.csv)。
7. 包括密碼計算參數和中所述的任何命令行標誌加密計算中的可選標誌 Clean Rooms。
8. 執行 命令。

在示例中ads.csv，我們運行以下命令。

java -jar c3r-cli.jar encrypt ***ads.csv*** --schema=***ads.json*** --id=***123e4567-e89b-42d3-a456-556642440000*** --output=***ads-output.csv***

在示例中sales.csv，我們運行以下命令。

java -jar c3r-cli.jar encrypt ***sales.csv*** --schema=***sales.json*** --id=***123e4567-e89b-42d3-a456-556642440000***

> **Note**
>
> 在此範例中，我們不指定輸出檔案名稱 (`--output=sales-output.csv`)。因此，產生了預設的輸出檔案`name-of-file.out.csv`名稱。

您現在已準備好驗證加密的資料。

步驟 8：驗證資料加密

驗證資料是否已加密

1. 檢視加密的資料檔案 (例如，`sales-output.csv`)。
2. 確認下列資料欄：
   a. 欄 1 — 已加密 (例如，`username_fingerprint`)。

      對於資fingerprint料行 (HMAC)，在版本和類型前置詞 (例如`01:hmac:`) 之後，有 44 個字元的 base64 編碼資料。

   b. 欄 2 — 未加密 (例如`purchased`)。
   c. 欄 3 — 已加密 (例如，`product_sealed`)。

      對於已加密 (SELECT) 資料行，加cleartext上版本和類型前置詞之後的任何填補長度 (例如，`01:enc:`) 與加密的長度成cleartext正比。也就是說，長度是輸入的大小加上大約 33% 的開銷，因為編碼。

您現在已準備好：

1. 將加密的資料上傳到 S3。
2. 創建一個 AWS Glue 表。
3. 在中建立已配置的表格 AWS Clean Rooms。

C3R 加密客戶端將創建不包含未加密數據的臨時文件（除非該數據在最終輸出中也將未加密）。但是，某些加密值可能無法正確填充。即使協同作業設定`allowRepeatedFingerprintValue`為，指紋資料行也可能包含重複的值`false`。之所以發生這個問題，是因為在檢查適當的填補長度和重複移除屬性之前寫入暫存檔案。

如果 C3R 加密用戶端失敗或在加密期間中斷，它可能會在寫入暫存檔之後，但在檢查這些內容並刪除暫存檔之前停止。因此，這些暫存檔案可能仍在磁碟上。如果是這種情況，這些檔案中的內容不會將純文字資料保護到與輸出相同的層級。特別是，這些臨時文件可能會向統計分析顯示純文本數據，這些數據不會對最終輸出起作用。用戶應刪除這些文件（尤其是SQLite數據庫），以防止這些文件落入未經授權的手中。

(選擇性) 建立結構描述 (進階使用者)

手動建立結構描述適用於進階使用者。

以下是包含或不含欄標題之輸入檔案之 JSON 結構定義檔案格式的說明。如果需要，高級用戶可以直接編寫或修改模式。

> **Note**
>
> C3R 加密客戶端可以幫助您通過中描述的互動過程範例：使用sealed、fingerprint和cleartext欄產生加密綱要或通過創建存根模板來創建模式。

對映和位置表格資料架構

以下段落說明兩種資料表結構定義：

- 對應資料表結構描述 — 此結構描述用於使用標題列和Apache Parquet檔案加密 .csv 檔案。
- 位置資料表結構描述 — 此結構描述用於加密沒有標題列的 .csv 檔案。

C3R 加密客戶端可以加密表格文件以進行協作。要做到這一點，它必須有一個對應的結構描述文件，該文件指定如何從輸入導出加密的輸出。

C3R 加密用戶端可以在命令列上執行 C3R 加密用戶端結構描述命令，協助產生INPUT檔案的結構描述。命令的一個例子是`java -jar c3r-cli.jar schema --interactive INPUT`。

結構描述會指定下列資訊：

1. 來源欄對映至哪些來源欄，透過其標頭名稱 (對映的結構描述) 或位置 (位置資料架構) 轉換輸出檔案中的欄
2. 要保留哪些目標資料欄 cleartext

3. 要針對SELECT查詢加密的目標資料欄

4. 要針對JOIN查詢加密的目標資料欄

此資訊會以資料表特定的 JSON 結構描述檔案編碼，該檔案由headerRow欄位為布林值的單一物件組成。該值必須true適用於Parquet具有標題列的檔案和 .csv 檔案，false否則。

對映資料表結構

對映的結構描述具有以下形狀。

```
{
  "headerRow": true,
  "columns": [
    {
      "sourceHeader": STRING,
      "targetHeader": STRING,
      "type": TYPE,
      "pad": PAD
    },
    ...
  ]
}
```

如果headerRow是true，則物件中的下一個欄位是columns，其中包含將來源標頭對應至目標標頭的資料行結構定義陣列 (也就是說明輸出資料行應包含的 JSON 物件)。

- sourceHeader— 資料衍生自之來源資料行的STRING標頭名稱。

> **Note**
>
> 相同的來源資料欄可用於多個目標資料欄。
> 輸出檔案中未列為結構定義中sourceHeader任何位置的輸入檔案中的資料行不會顯示在輸出檔案中。

- targetHeader— 輸出檔案中對應欄的STRING標頭名稱。

> **Note**
>
> 對於對應的綱要，此欄位是選擇性的。如果省略此欄位，sourceHeader則會重新用於輸出中的標頭名稱。如果輸出資料行分別為欄或fingerprintsealed欄，則會附加或。_fingerprint _sealed

- type— 輸TYPE出檔案中目標欄的。也就是說，其中之一 cleartextsealed，或fingerprint取決於在協同作業中使用欄的方式。
- pad— 資料行結構描述物件的欄位，只有在是時才會TYPE出現sealed。的對應值PAD是描述資料在加密之前應如何填充資料的物件。

```
{
  "type": PAD_TYPE,
  "length": INT
}
```

要指定預加密填充，type並length使用如下：

- PAD_TYPEas none-不填充將應用於列的數據，並且該length字段不適用（也就是省略）。
- PAD_TYPEas fixed — 資料行的資料會填補至指定length的位元組。
- PAD_TYPEas max — 資料行的資料會填補至最長值的位元組長度加上一個額外length位元組的大小。

以下是對應結構描述的範例，其中包含每種類型的資料行。

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

以下是一個更複雜的範例，以下是包含標題的 .csv 檔案範例。

```
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
```

在下列對應的結構描述範例中，資料`LastName`行`FirstName`和`cleartext`欄。資`State`料行會加密為`fingerprint`資料行，以及填補為的`sealed`欄`none`。其餘的列被省略。

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

以下是由對應結構描述產生的 .csv 檔案。

```
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=
```

位置資料表資料架構

位置資料架構具有以下造型。

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      },
      {
        "targetHeader": STRING,
        "type": TYPE,
        "pad": PAD
      }
    ],
    [],
    ...
  ]
}
```

如果headerRow是false，則物件中的下一個欄位是columns，其中包含一組項目。每個項目本身就是零個或多個位置資料行結構描述 (無sourceHeader欄位) 的陣列，這些結構描述了輸出應包含的 JSON 物件。

- sourceHeader— 資料衍生自之來源資料行的STRING標頭名稱。

  > **Note**
  >
  > 在位置結構描述中必須省略此欄位。在位置結構定義中，來源資料行是由結構描述檔案中資料行對應的索引推斷出來的。

- targetHeader— 輸出檔案中對應欄的STRING標頭名稱。

  > **Note**
  >
  > 位置資料架構需要此欄位。

- type— 輸TYPE出檔案中目標欄的。也就是說，其中之一 cleartextsealed，或fingerprint取決於在協同作業中使用欄的方式。

- pad— 資料行結構描述物件的欄位，只有在是時才會TYPE出現sealed。的對應值PAD是描述資料在加密之前應如何填充資料的物件。

```
{
  "type": PAD_TYPE,
  "length": INT
}
```

要指定預加密填充，type並length使用如下：

- PAD_TYPEas none-不填充將應用於列的數據，並且該length字段不適用（也就是省略）。
- PAD_TYPEas fixed — 資料行的資料會填補至指定length的位元組。
- PAD_TYPEas max — 資料行的資料會填補至最長值的位元組長度加上一個額外length位元組的大小。

> **Note**
>
> fixed如果您提前知道列數據的字節大小的上限，則非常有用。如果該資料行中的任何資料超過指定的資料，就會引發錯誤length。
> max當輸入數據的確切大小未知時很方便，因為無論數據大小如何，它都可以工作。不過，max需要額外的處理時間，因為它會加密資料兩次。 max在讀入暫存檔案時加密資料一次，並在已知資料行中最長的資料項目之後加密一次。
> 此外，最長值的長度不會在客戶端的調用之間保存。如果您計劃批次加密資料，或定期加密新資料，請注意產生的密碼文字長度可能會因批次而異。

以下是位置資料架構的範例。

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

作為一個複雜的例子，如果 .csv 文件沒有帶標題的第一行，則以下是一個示例。

```
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
```

位置結構描述具有以下形式。

```
{
  "headerRow": false,
  "columns": [
    [
      {
        "targetHeader": "GivenName",
```

```
        "type": "cleartext"
      }
    ],
    [
      {
        "targetHeader": "Surname",
        "type": "cleartext"
      }
    ],
    [],
    [],
    [
      {
        "targetHeader": "State_Join",
        "type": "fingerprint"
      },
      {
        "targetHeader": "State",
        "type": "sealed",
        "pad": {
          "type": "none"
        }
      }
    ],
    [],
    [],
    [],
    []
  ]
}
```

上述結構描述會產生下列輸出檔案，其中包含指定目標標頭的標頭資料列。

```
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=
```

在中建立已配置的資料表 AWS Clean Rooms

配置的表格是中現有表格的參照 AWS Glue Data Catalog。它包含決定如何查詢資料的分析規則。AWS Clean Rooms已配置的表格可以與一或多個協同作業相關聯。如需詳細資訊 AWS Glue，請參閱 AWS Glue 開發人員指南。

使用提供的統計資料產生，計算表格 AWS Glue 的資料行層次統計資料。 AWS Glue Data Catalog 一旦針對資料目錄中的表 AWS Glue 產生統計資料，Amazon Redshift Spectrum 就會自動使用這些統計資料來優化查詢計劃。如需使用計算資料行層級統計資料的詳細資訊 AWS Glue，請參閱使用資料行統計資料指南。

建立已設定的資料表

在此步驟中，您可以在中建立已配置的表格， AWS Clean Rooms 以便在協同合作中使用。

若要在中建立已配置的表格 AWS Clean Rooms

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇右上角的 [設定新資料表]。
4. 對於「配置新表格」，對於 「選擇」 AWS Glue 表格：
   a. 從下拉列表中選擇要配置的數據庫。
   b. 從下拉列表中選擇要配置的表。

> **Note**
>
> 若要確認此表格是否正確，請執行下列任一項作業：
>
> - 選擇 [檢視於] AWS Glue。
> - 開啟 [檢視結構定義] 以檢視結構描述。

5. 在協同作業中允許的欄位中，選擇 [所有欄] 或 [自訂清單]。

如果選擇...	然後...
所有欄	允許在中使用所有欄 AWS Clean Rooms (視分析規則而定)。
自訂清單	從 [指定允許的資料欄] 下拉式清單中選擇一或多個要允許的資料欄。

6. 對於 「配置」表格的詳細

   a. 輸入已設定之表格的「名稱」。

      您可以使用預設名稱或重新命名此表格。

   b. 輸入表格的「摘要」。

      描述有助於區分具有相似名稱的其他已配置表格。

   c. 如果您要為已設定的表格資源啟用標籤，請選擇 [新增標籤]，然後輸入 [索引鍵] 和 [值] 配對。

7. 選擇「配置新表格」。

後續步驟

現在，您已經建立了配置的表格，您可以：

- 為配置的表格配置分析規則
- 將已配置的表格與協同合作相關聯

將分析規則配置為已配置的表格

以下各節說明如何為已配置的表格配置分析規則。透過取消設定分析規則，您可以授權可以查詢的成員執行符合支援的特定分析規則的查詢。AWS Clean Rooms

AWS Clean Rooms支援以下類型的分析規則：彙總、清單和自訂。

每個已設定的表格只能有一個分析規則。

> **Important**
>
> 如果您在協同作業中使用「密碼編譯運算」，Clean Rooms且已加密資料表，則您新增至已加密配置資料表的分析規則應該與資料的加密方式一致。例如，如果您為 SELECT (彙總分析規則) 加密資料，則不應新增 JOIN (清單分析規則) 的分析規則。

若要瞭解中可用的分析規則類型AWS Clean Rooms，請參閱分析規則 AWS Clean Rooms。

如需彙總分析規則的詳細資訊，請參閱彙總分析規則。

如需清單分析規則的更多資訊，請參閱清單分析規則。

如需自訂分析規則的更多資訊，請參閱自訂分析規則 AWS Clean Rooms。

檢閱並瞭解這些章節之後，您可以執行下列程序：

主題

- 設定資料表的彙總分析規則 (引導流程)
- 設定資料表的清單分析規則 (引導流程)
- 設定資料表的自訂分析規則 (引導流程)
- 設定資料表的分析規則 (JSON 編輯器)
- 後續步驟

設定資料表的彙總分析規則 (引導流程)

彙總分析規則允許使用、和AVG函數沿選用維度彙總統計資料的查詢 COUNTSUM，而不會揭露資料列層級資訊。

此程序說明使用AWS Clean Rooms主控台中的 [引導式流程] 選項，將彙總分析規則新增至已設定資料表的程序。

若要將彙總分析規則新增至資料表 (引導流程)

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇配置的表格。
4. 在已設定的表格詳細資料頁面上，選擇設定分析規則。
5. 在「步驟 1：選擇類型」下的「類型」下，保留「彙總」選項預設為選取狀態。
6. 在建立方法下，選取引導流程，然後選擇下一步。
7. 在「步驟 2：指定查詢控制項」下，對於「彙總函式」：
   a. 從下拉式清單中選擇彙總函式：
      - 伯爵
      - 不同計數
      - SUM
      - 不同總和
      - AVG
   b. 從「欄」下拉式清單中選擇可在「彙總」函數中使用的欄。
   c. (選擇性) 選擇「新增其他函數」以新增另一個彙總函數，並將一或多個欄關聯至該函數。

      > **Note**
      >
      > 至少需要一個彙總函數。

   d. (選擇性) 選擇「移除」以移除彙總函數。
8. 對於加入控制項，
   a. 選擇一個選項允許自行查詢表格：

如果選擇...	然後...
否，只能查詢重疊	只有在聯結至可查詢之成員所擁有的資料表時，才能查詢資料表。
是	該表可以通過本身或當連接到其他表進行查詢。

b. 在 [指定聯結資料行] 底下，選擇您要允許在INNERJOIN陳述式中使用的資料行。

如果您在上一個步驟中選取了 「是」，則此選項為選用性。

c. 在「指定允許的運算子進行比對」下，選擇可用於在多個聯結欄上進行比對的運算子 (如果有的話)。如果您選取兩個或多個JOIN欄，則需要其中一個運算子。

如果選擇...	然後...
和	您可以AND在INNER JOIN匹配條件中包括以將一列聯接到表之間的另一列。
或	您可以OR在INNER JOIN匹配條件中包括在表之間合併多個列匹配項。這個邏輯運算符對於獲得更高的匹配率很有用。

9. (選擇性) 對於維度控制項，請在「指定維度資料欄」下拉式清單中，選擇要允許在 SELECT 陳述式中使用哪些欄 WHERE GROUPBY，以及查詢的、和ORDERBY部分。

> **Note**
>
> 彙總函數或聯結資料行不能用作維度資料行。

10. 對於純量函數，請為您要允許哪些純量函數選擇一個選項？

如果選擇...	然後...
目前所有支援 AWS Clean Rooms	您允許目前支援的所有純量函數。AWS Clean Rooms

如果選擇...	然後...
	• 您可以選擇 [檢視清單] 來查看中AWS Clean Rooms支援的純量函數的完整清單。
自訂清單	您可以自訂允許的純量函數。 • 從「指定允許的純量函數」下拉式清單中選擇一或多個選項。
無	您不想允許任何標量函數。

如需詳細資訊，請參閱純量函數。

11. 選擇 下一步。
12. 在「步驟 3：指定查詢結果控制項」下，針對「彙總」限制：
    a. 選擇每個列名的下拉列表。
    b. 在套用COUNT DISTINCT函數之後，針對要傳回的每個輸出資料列必須符合的每個不同值的最小數目，選取下拉式清單。
    c. 選擇新增限制條件，新增更多聚總限制條件
    d. (選擇性) 選擇移除以移除聚總限制條件。
13. 選擇 下一步。
14. 在 [步驟 4：檢閱和設定] 底下，檢閱您為先前步驟所做的選擇，視需要進行編輯，然後選擇 [設定分析規則]。

您會看到一則確認訊息，指出您已成功設定表格的彙總分析規則。

設定資料表的清單分析規則 (引導流程)

清單分析規則允許查詢輸出關聯資料表與可查詢之成員資料表之間重疊的資料列層級清單。

此程序說明使用AWS Clean Rooms主控台中的 [引導式流程] 選項將清單分析規則新增至已設定資料表的程序。

若要將清單分析規則新增至資料表 (引導流程)

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇配置的表格。
4. 在已設定的表格詳細資料頁面上，選擇設定分析規則。
5. 在「步驟 1：選擇類型」下的「類型」下，選擇「清單」選項。
6. 在建立方法下，選取引導流程，然後選擇下一步。
7. 在「步驟 2：指定查詢控制項」下的「聯結」控制項：

   a. 在 [指定聯結資料行] 底下，選擇您要允許在INNERJOIN陳述式中使用的資料行。

   b. 在「指定允許的運算子進行比對」下，選擇可用於在多個聯結欄上進行比對的運算子 (如果有的話)。如果您選取兩個或多個JOIN欄，則需要其中一個運算子。

如果選擇...	然後...
和	您可以AND在INNER JOIN匹配條件中包括以將一列聯接到表之間的另一列。
或	您可以OR在INNER JOIN匹配條件中包括在表之間合併多個列匹配項。這個邏輯運算符對於獲得更高的匹配率很有用。

8. (選擇性) 對於 List 控制項，請在「指定清單欄」下拉式清單中，選擇要允許在查詢輸出中使用的欄 (亦即，在SELECT陳述式中使用)，或用來篩選結果 (亦即WHERE陳述式)。
9. 選擇 下一步。
10. 在 [步驟 3：檢閱和設定] 底下，檢閱您為先前步驟所做的選擇，視需要進行編輯，然後選擇 [設定分析規則]。

您會看到確認訊息，指出您已成功設定表格的清單分析規則。

設定資料表的自訂分析規則 (引導流程)

自訂分析規則會在已設定的資料表上啟用自訂 SQL 查詢。如果使用分析範本或差分隱私，則需要自訂分析規則。

此程序說明使用AWS Clean Rooms主控台中的 [引導式流程] 選項將自訂分析規則新增至已設定資料表的程序。

若要將自訂分析規則新增至表格 (引導流程)

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇配置的表格。
4. 在已設定的表格詳細資料頁面上，選擇設定分析規則。
5. 在「步驟 1：選擇類型」下的「類型」下，選擇「自訂」選項。
6. 在建立方法下，選取引導流程，然後選擇下一步。
7. 在「步驟 2：設定差分隱私」下方，確定您要開啟或關閉差分隱私。差分隱私是一種經過數學驗證的技術，可保護您的數據免受重新識別攻擊。

   a. 對於差分隱私：

如果你...	然後選擇...
擁有使用者層級資料，並希望防止重新識別嘗試	開啟
沒有使用者層級的資料，或不需要針對重新識別嘗試進行防護	關閉

   b. 如果您已選擇開啟差分隱私權，請選取 [使用者識別碼] 欄，其中包含您使用者的唯一識別碼，例如您要保護其隱私權的`user_id`欄。如果您想要在協同作業中為兩個或多個資料表開啟差異隱私權，您必須在這兩個分析規則中設定與「使用者識別碼」欄相同的欄，以維持跨資料表的使用者定義一致。如果設定錯誤，可以查詢的成員會收到錯誤訊息，指出有兩欄可供選擇，以計算執行查詢時使用者貢獻的數量 (例如，使用者所做的廣告曝光次數)。

   c. 選擇 下一步。

8. 在「步驟 3：指定查詢控制項」下，

   a. 對於控制類型：

如果您想要...	然後選擇...
檢閱每個新的分析範本，然後再在已設定的表格上執行	檢閱每個新分析，然後才允許在此表格上執行
讓任何分析範本或直接查詢都可以在您設定的資料表上執行	允許特定協同合作者建立的任何查詢在不檢閱此表格的情況下執行

b. 選擇下列其中一項：

如果您選擇...	然後...
檢閱每個新分析，然後才允許在此表格上執行	在「允許執行的分析範本」下，選擇「新增分析範本」，然後從下拉式清單中選擇適當的「協同作業」和「分析」範本。
允許特定協同合作者建立的任何查詢在不檢閱此表格的情況下執行	在「AWS 帳戶允許建立任何查詢」下，選擇「新增」AWS 帳戶，然後選擇適當的 AWS 帳戶ID。

9. 選擇 下一步。
10. 在 [步驟 4：檢閱和設定] 底下，檢閱您為先前步驟所做的選擇，視需要進行編輯，然後選擇 [設定分析規則]。

您會看到確認訊息，指出您已成功設定表格的自訂分析規則。

設定資料表的分析規則 (JSON 編輯器)

下列程序顯示如何使用AWS Clean Rooms主控台中的 JSON 編輯器選項將分析規則新增至資料表。

若要設定資料表的彙總、清單或自訂分析規則 (JSON 編輯器)

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇配置的表格。

4. 在已設定的表格詳細資料頁面上，選擇設定分析規則。
5. 在「步驟 1：選擇類型」下的「類型」下，選擇「彙總」、「清單」或「自訂」選項。
6. 在 [建立方法] 下，選取 [JSON 編輯器]，然後選擇 [下一步]
7. 在「步驟 2：指定控制項」下，您可以選擇插入查詢結構 (插入範本) 或插入檔案 (從檔案匯入)。

如果選擇...	然後...
插入範本	1. 在「分析」規則定義中指定所選分析規則的參數。 2. 您可以按 Ctrl + 空格鍵來啟用自動完成。 如需彙總分析規則參數的詳細資訊，請參閱彙總分析規則-查詢控制項。 如需清單分析規則參數的更多資訊，請參閱〈〉清單分析規則-查詢控制項。
從檔案匯入	1. 從本地驅動器中選擇 JSON 文件。 2. 選擇 Open (開啟)。 分析規則定義會顯示上載檔案中的分析規則。

8. 選擇 下一步。
9. 在 [步驟 3：檢閱和設定] 底下，檢閱您為先前步驟所做的選擇，視需要進行編輯，然後選擇 [設定分析規則]。

您會收到確認訊息，指出您已成功設定表格的分析規則。

後續步驟

現在，您已將分析規則配置為已配置的表格，您已準備好：

- 將已配置的表格與協同合作相關聯
- 查詢資料表 (以可查詢的成員身分)

將已配置的表格與協同合作產生關聯

建立已配置的表格並在其中新增分析規則之後，您可以將其與協同合作相關聯。

> **Important**
>
> 在將已設定的 AWS Glue 表格與協同作業建立關聯之前， AWS Glue 表格位置必須指向 Amazon Simple Storage Service (Amazon S3) 資料夾，而不是單一檔案。您可以檢視 AWS Glue 主控台中的表格，網址為 https://console.aws.amazon.com/glue/，以確認此位置。

> **Note**
>
> 如果您已在中設定加密 AWS Glue 並建立服務角色，則必須授與該角色存取權，才能用 AWS KMS keys 來解密 AWS Glue 資料表。
> 如果您關聯由 AWS KMS加密 Amazon S3 資料集支援的已設定資料表，則必須授予該角色存取權，才能使用 KMS 金鑰解密 Amazon S3 資料。
> 如需詳細資訊，請參閱AWS Glue 開發人員指南 AWS Glue中的設定加密。

下列主題說明如何使用主 AWS Clean Rooms 控台將已配置的表格與協同作業相關聯：

主題

如需如何使用 AWS SDK 將已設定的資料表與協同作業相關聯的詳細資訊，請參閱 AWS Clean Rooms API 參考。

從設定的表格詳細資訊頁面建立關聯已設定表格

若要從已配置的 AWS Glue 表格詳細資訊頁面將表格與協同作業相關

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。

2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇配置的表格。
4. 在已設定的表格詳細資訊頁面上，選擇關聯至協同合作。
5. 在「將表格與協同作業相關聯」對話方塊中，從下拉式清單中選擇「合作」。
6. 選擇 [選擇合作]。

   在「關聯表格」頁面上，您選擇之已設定之表格的名稱會顯示在「選擇已設定的表格」段落下。
7. 對於選擇已配置的表格，請執行下列操作：

如果您想要...	然後...
設定新表格	選擇設定表格，然後依照設定表格頁面上的提示進行操作。
檢視已設定之表格的結構描述和分析規則	開啟 [檢視結構描述和分析規則]。

8. 選取 [建立並使用新的服務角色] 或 [使用現有的服務角色]，以指定服務存取權限。

如果選擇...	然後...
建立並使用新的服務角色	• AWS Clean Rooms 建立具有此表格所需原則的服務角色。 • 預設的服務角色名稱為 `cleanrooms-<timestamp>` • 您必須具有建立角色和附加原則的權限。 • 如果您的輸入資料已加密，您可以選取 [此資料已使用 KMS 金鑰加密] AWS KMS key ，然後輸入將用於解密資料輸入的資料。
使用現有的服務角色	1. 從下拉式清單中選擇現有的服務角色名稱。 如果您有列出角色的權限，則會顯示角色清單。 如果您沒有列出角色的權限，則可以輸入要使用之角色的 Amazon 資源名稱 (ARN)。

如果選擇...	然後...
	2. 選擇在 IAM 中檢視外部連結來檢視服務角色。 如果沒有現有的服務角色，則無法使用 [使用現有服務角色] 選項。 根據預設， AWS Clean Rooms 不會嘗試更新現有的角色原則來新增必要的權限。 3. (選擇性) 選取 [將具有必要權限的預先設定原則新增至此角色] 核取方塊，以將附加必要的權限新增至角色。您必須具有修改角色和建立策略的權限。

> **Note**
>
> - AWS Clean Rooms 需要根據分析規則進行查詢的權限。如需有關權限的詳細資訊 AWS Clean Rooms，請參閱AWS 受管理的政策 AWS Clean Rooms。
> - 如果角色沒有足夠的權限 AWS Clean Rooms，您會收到錯誤訊息，指出該角色沒有足夠的權限 AWS Clean Rooms。在繼續之前，必須先新增角色原則。
> - 如果您無法修改角色原則，您會收到錯誤訊息，指出 AWS Clean Rooms 找不到服務角色的原則。

9. 如果您要為已設定的表格關聯資源啟用標籤，請選擇 [新增標記]，然後輸入 [索引鍵] 和 [值] 配對。
10. 選擇「關聯表」。

從協同合作詳細資訊頁面關聯已配置的表格

若要從協同合作詳細資訊頁面將 AWS Glue 表格與協同作業相關

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇「合作」。

3. 選擇合作。
4. 在「表格」標籤上，選擇「關聯表格」。
5. 對於選擇已配置的表格，請執行下列操作：

如果您想要...	然後...
選擇現有的已設定表格	從下拉式清單中選擇您要與協同合作產生關聯的「已設定」表格名稱。
設定新表格	選擇設定表格，然後依照設定表格頁面上的提示進行操作。
檢視已設定之表格的結構描述和分析規則	開啟 [檢視結構描述和分析規則]。

6. 對於表關聯的詳細信息，
   a. 輸入關聯表格的「名稱」。

      您可以使用預設名稱或重新命名此表格。

   b. (選擇性) 輸入表格的「說明」。

      描述有助於編寫查詢。
7. 選取 [建立並使用新的服務角色] 或 [使用現有的服務角色]，以指定服務存取權限。

如果選擇...	然後...
建立並使用新的服務角色	• AWS Clean Rooms 建立具有此表格所需原則的服務角色。 • 預設的服務角色名稱為`cleanrooms-<timestamp>` 。 • 您必須具有建立角色和附加原則的權限。 • 如果您的輸入資料已加密，您可以選取 [此資料已使用 KMS 金鑰加密] AWS KMS key ，然後輸入將用於解密資料輸入的資料。
使用現有的服務角色	1. 從下拉式清單中選擇現有的服務角色名稱。

如果選擇...	然後...
	如果您有列出角色的權限，則會顯示角色清單。 如果您沒有列出角色的權限，則可以輸入要使用之角色的 Amazon 資源名稱 (ARN)。 2. 選擇在 IAM 中檢視外部連結來檢視服務角色。 如果沒有現有的服務角色，則無法使用 [使用現有服務角色] 選項。 根據預設， AWS Clean Rooms 不會嘗試更新現有的角色原則來新增必要的權限。 3. (選擇性) 選取 [將具有必要權限的預先設定原則新增至此角色] 核取方塊，以將附加必要的權限新增至角色。您必須具有修改角色和建立策略的權限。

> **Note**
>
> - AWS Clean Rooms 需要根據分析規則進行查詢的權限。如需有關權限的詳細資訊 AWS Clean Rooms，請參閱AWS 受管理的政策 AWS Clean Rooms。
> - 如果角色沒有足夠的權限 AWS Clean Rooms，您會收到錯誤訊息，指出該角色沒有足夠的權限 AWS Clean Rooms。在繼續之前，必須先新增角色原則。
> - 如果您無法修改角色原則，您會收到錯誤訊息，指出 AWS Clean Rooms 找不到服務角色的原則。

8. 如果您要為已設定的表格關聯資源啟用標籤，請選擇 [新增標記]，然後輸入 [索引鍵] 和 [值] 配對。
9. 選擇「關聯表」。

後續步驟

現在，您已將已配置的資料表與協同作業相關聯，您就可以：

- 如果您是共同作業建立者，請編輯共同作業
- 查詢資料表 (以可查詢的成員身分)

設定差異隱私權政策

此程序說明使用 AWS Clean Rooms 主控台中的 [引導式流程] 選項在協同合作中設定差異隱私權政策的程序。對於具有差分隱私保護的所有表格，這是一次性步驟。

若要設定差異隱私設定 (引導流程)

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇「合作」。
3. 選擇合作。
4. 在協同作業頁面的 [表格] 索引標籤上，選擇 [設定差異隱私權原則]
5. 在 [設定差異隱私權原則] 頁面上，選擇下列屬性的值：

   - 隱私權預算
   - 每月更新隱私權預算
   - 每個查詢新增的雜訊

   您可以使用預設值或輸入支援特定使用案例的自訂值。在選擇「隱私權預算」和「每次查詢新增雜訊」的值之後，您可以根據所有資料查詢中可能的彙總數量來預覽產生的公用程式。
6. 選擇設定。

您會看到一則確認訊息，指出您已成功設定協同作業的差異隱私權政策。

後續步驟

現在您已設定差分隱私，您已準備好：

- 查詢資料表 (以可查詢的成員身分)
- 管理共同作業 (如果您是共同作業建立者)

使用分析範本

分析範本搭配使用自訂分析規則 AWS Clean Rooms. 使用分析範本，您可以定義參數以協助您重複使用相同的查詢。 AWS Clean Rooms 支援具有常值的參數化子集。

分析範本是協同合作特定的。對於每個協同合作，成員只能看到該共同作業中的查詢。如果您打算在協同合作中使用差分隱私，則應確保您的分析範本與 AWS Clean Rooms 差分隱私的一般用途查詢結構相容。

主題

- 建立分析範本
- 檢閱分析範本
- 使用分析範本查詢已設定的資料表

建立分析範本

如需如何使用 AWS SDK 建立分析範本的相關資訊，請參閱 AWS Clean Rooms API 參考。

若要使用 AWS Clean Rooms 主控台建立分析範本

1. 登入 AWS Management Console 並開啟主控台，並使用 AWS 帳戶 該AWS Clean Rooms 主控台做為協同作業建立者使用。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇協同合作。
4. 在 [範本] 索引標籤上，移至 [由您建立的分析範本] 區段。
5. 選擇 [建立分析範本]。
6. 在 [建立分析範本] 頁面上，對於 [詳細資訊]，輸入名稱和選用說明。
7. 針對「表格」，檢視與協同合作相關聯的已配置表格。
8. 對於定義，

    a. 輸入分析範本的定義。

    b. 選擇「匯入來源」以匯入定義。

    c. (選擇性) 在參數名稱前面輸入冒號 (:)，在 SQL 編輯器中指定參數。

    例如：

```
    WHERE table1.date + :date_period > table1.date
```

9. 如果您先前已新增參數，請在參數-選用之下，針對每個參數名稱選擇類型和預設值 (選用)。
10. 如果要為設定的表格資源啟用標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。
11. 選擇建立。

您現在已準備好：

- 通知您的協同合作成員，他們可以檢閱分析範本。（如果要查詢自己的數據，則為可選。）

檢閱分析範本

在協同合作成員建立分析範本之後，您可以檢閱並核准該範本。在分析模板和批准後，它可以在中查詢 AWS Clean Rooms。

使用 AWS Clean Rooms 主控台檢閱分析範本

1. 登入 AWS Management Console 並開啟主控台，並使用 AWS 帳戶 該AWS Clean Rooms 主控台做為協同作業建立者使用。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇協同合作。
4. 在「範本」標籤上，移至「由其他成員建立的分析範本」區段。
5. 選擇「可執行」狀態為「否」的分析樣版，需要您進行複查。
6. 選擇檢閱。
7. 複查分析規則「概觀」、「定義」和「參數」(如果有的話)。
8. 複查定義中參考的表格下列出的已設定表格。

   每個表格旁邊的「狀態」 都會顯示為「不允許範本」。
9. 選擇 表格。

如果您	然後選擇
核准分析範本	樣板, 上, 桌子。選擇以確認您的核准。
不核准分析範本	不允許

您現在可以使用分析範本來查詢資料表 (作為可查詢的成員)。

使用分析範本查詢已設定的資料表

此程序示範如何使用 AWS Clean Rooms 主控台中的分析範本，以自訂分析規則查詢已配置的資料表。

若要使用分析範本以自訂分析規則查詢已設定的資料表

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇「您的會員能力」狀態為「查詢」的合作。
4. 在「查詢」頁籤的「表格」下，檢視表格及其相關聯的分析規則類型 (自訂分析規則)。

> **Note**
>
> 如果您在清單中沒有看到預期的表格，可能是因為下列原因：
>
> - 表格尚未關聯。
> - 這些表沒有配置分析規則。

5. 在「分析」區段下，從下拉式清單中選取分析範本。
6. 輸入您要在查詢中使用的分析範本中的參數值。該值必須在參數的指定數據類型中。您可以在每次執行分析範本時使用不同的值。不支援空白或參數NULL值。也不支援在LIMIT子句中使用參數。
7. 選擇執行。

> **Note**
>
> 如果可以接收結果的成員尚未設定查詢結果設定，則無法執行查詢。

8. 繼續調整參數並再次執行查詢，或選擇「+」按鈕以在新標籤中開始新查詢。

在協同作業中查詢資料

身為可以查詢的成員，您可以執行下列其中一項作業：

- 使用 SQL 程式碼編輯器手動建置 SQL 查詢。
- 使用分析產生器使用者介面來建立查詢，而不需要撰寫 SQL 程式碼。
- 使用核准的分析範本。

當可以查詢的成員在協同作業中的資料表上執行 SQL 查詢時，會 AWS Clean Rooms 假設相關角色代表他們存取資料表。 AWS Clean Rooms 視需要將分析規則套用至輸入查詢及其輸出。

AWS Clean Rooms 支援可能與其他查詢引擎不同的 SQL 查詢。如需規格，請參閱 AWS Clean Rooms SQL 參考。如果您要對受差分隱私保護的資料表執行查詢，您應該確定您的查詢與 AWS Clean Rooms 差分隱私權的一般用途查詢結構相容。

> **Note**
>
> 使用的密碼編譯運算時Clean Rooms，並非所有 SQL 作業都會產生有效的結果。例如，您可以在加密的資料行COUNT上執行，但是執SUM行加密的數字會導致錯誤。此外，查詢也可能會產生不正確的結果。例如，SUM密封資料行的查詢會產生錯誤。但是，對密封列的GROUPBY查詢似乎成功，但產生的組與通過明文GROUPBY查詢生成的組不同。

下列主題說明如何使用主 AWS Clean Rooms 控台在協同作業中查詢資料。

主題

- 使用 SQL 程式碼編輯器
- 使用分析建置器
- 查詢具有差分隱私的資料
- 檢視近期查詢
- 檢視查詢詳細資訊

如需如何直接呼叫 AWS Clean Rooms `StartProtectedQuery` API 作業或使用 AWS SDK 來查詢資料或檢視查詢的相關資訊，請參閱 AWS Clean Rooms API 參考。

如需查詢記錄的相關資訊，請參閱查詢登入 AWS Clean Rooms。

> **Note**
>
> 如果您對加密的資料表執行查詢，則加密資料行的結果會加密。

如需有關接收查詢結果的資訊，請參閱接收查詢結果。

使用 SQL 程式碼編輯器

身為可以查詢的成員，您可以在 SQL 程式碼編輯器中撰寫 SQL 程式碼，以手動方式建立查詢。SQL 程式碼編輯器位於 AWS Clean Rooms 主控台的 [查詢] 索引標籤的 [分析] 區段中。

依預設，會顯示 SQL 程式碼編輯器。如果您要使用分析建置器來建立查詢，請參閱使用分析建置器。

> **Important**
>
> 如果您開始在程式碼編輯器中撰寫 SQL 查詢，然後開啟 Analysis 產生器 UI，則不會儲存您的查詢。

AWS Clean Rooms 支持許多 SQL 命令，函數和條件。如需詳細資訊，請參閱 AWS Clean Rooms SQL 參考。

> **Tip**
>
> 如果在查詢執行時發生排程的維護，查詢會終止並復原。您必須重新啟動查詢。

若要使用 SQL 程式碼編輯器手動建立查詢

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇「您的會員能力」狀態為「查詢」的合作。
4. 在「查詢」頁籤上，移至「分析」區段。

> **Note**
>
> 只有在可以接收結果的成員以及負責支付查詢計算成本的成員已加入協同作業為作用中成員時，才會顯示「分析」區段。

5. 在 [查詢] 索引標籤的 [資料表] 下，檢視表格清單及其相關聯的分析規則類型 (彙總分析規則、清單分析規則或自訂分析規則)。

> **Note**
>
> 如果您在清單中沒有看到預期的表格，可能是因為下列原因：
>
> - 表格尚未關聯。
> - 這些表沒有配置分析規則。

6. (選擇性) 若要檢視表格的結構定義和分析規則控制項，請選取加號圖示 (+) 以展開表格。
7. 透過在 SQL 程式碼編輯器中輸入查詢來建立查詢。

(選擇性) 如果您要使用範例查詢	(選擇性) 如果要插入欄名稱或函數
1. 選取表格旁邊的三個垂直點。 2. 在 [插入編輯器] 下，選擇 [範例查詢]。 **Note** 插入範例查詢會將查詢附加到編輯器中。 此時會顯示查詢範例。下面列出的所有表都包括在查詢中。 3. 編輯查詢中的預留位置值。	1. 選取欄旁邊的三個垂直點。 2. 在「在編輯器中插入」下，選擇「欄名稱」 3. 若要在欄中手動插入允許的函數，請選取欄旁邊的三個垂直點，選取 [在編輯器中插入]，然後選取允許函數的名稱 (例如INNER JOINSUMDISTINCT、SUM 或 COUNT)。 4. 按 Ctrl + 空格鍵可在程式碼編輯器中檢視資料表結構描述。 **Note** 可以查詢的成員可以檢視和使用每個已設定資料表

(選擇性) 如果您要使用範例查詢	(選擇性) 如果要插入欄名稱或函數
	關聯中的分割區資料欄。請確定資料分割資料行在已設定之資料 AWS Glue 表底層的資料表中標示為分割資料行。 5. 編輯查詢中的預留位置值。

8. 選擇執行。

> **Note**
>
> 如果可以接收結果的成員尚未設定查詢結果設定，則無法執行查詢。

9. 繼續調整參數並再次執行查詢，或選擇「+」按鈕以在新標籤中開始新查詢。

> **Note**
>
> AWS Clean Rooms 旨在提供清晰的錯誤消息。如果錯誤訊息沒有足夠的詳細資料可協助您進行疑難排解，請連絡客戶團隊。提供錯誤發生方式的描述以及錯誤訊息 (包括任何識別碼)。如需詳細資訊，請參閱 疑難排 AWS Clean Rooms。

使用分析建置器

您可以使用分析生成器來構建查詢，而無需編寫 SQL 代碼。使用分析建置器，您可以為具有下列條件的協同作業建立查詢：

- 使用彙總分析規則的單一表格，不需要 JOIN
- 兩個使用彙總分析規則的表格 (每個成員各一個)
- 兩個使用清單分析規則的表格 (每個成員各一個)
- 兩個使用彙總分析規則的表格 (每個成員各一個)，以及兩個使用清單分析規則的表格 (每個成員各一個)

如果您想要手動撰寫 SQL 查詢，請參閱使用 SQL 程式碼編輯器。

分析產生器會在 AWS Clean Rooms 主控台的 [查詢] 索引標籤的 [分析] 區段中顯示為 [分析建置器 UI] 選項。

> **Important**
>
> 如果您打開 Analysis 生成器 UI，開始在分析生成器中構建查詢，然後關閉 Analysis 生成器 UI，則不會保存您的查詢。

> **Tip**
>
> 如果在查詢執行時發生排程的維護，查詢會終止並復原。您必須重新啟動查詢。

下列主題說明如何使用分析建置器。

主題

- 使用分析建置器查詢單一資料表 (彙總)
- 使用分析建置器查詢兩個資料表 (彙總或清單)

使用分析建置器查詢單一資料表 (彙總)

此程序示範如何在 AWS Clean Rooms 主控台中使用 Analysis 產生器 UI 來建立查詢。此查詢適用於具有使用彙總分析規則且不JOIN需要的單一資料表的共同作業。

若要使用分析建置器查詢單一資料表

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇「您的會員能力」狀態為「查詢」的合作。
4. 在「查詢」頁籤的「表格」下，檢視表格及其相關聯的分析規則類型。(分析規則類型應為彙總分析規則。)

   > **Note**
   >
   > 如果您沒有看到預期的表格，可能是由於以下原因：

- 該表尚未關聯。
- 表格未設定分析規則。

5. 在「分析」部分下，打開「分析生成器 UI」。
6. 建立查詢。

   如果要查看所有彙總量度，請跳至步驟 9。

   a. 在「選擇測量結果」中，複查預設已預先選取的彙總量度，並視需要移除任何量度。

   b. (選擇性) 對於「新增區段」— 選用，請選擇一或多個參數。

   > **Note**
   >
   > 新增區段 — 只有在為表格指定維度時才會顯示選用區段。

   c. (選擇性) 對於 [新增篩選器] — 選用，請選擇 [新增篩選器]，然後選擇 [參數]、[運算子] 和 [值]。

   若要新增更多篩選器，請選擇 [新增其他篩選器

   若要移除篩選器，請選擇 [移除]。

   > **Note**
   >
   > ORDER BY不支援彙總查詢。
   > 篩選器僅支援AND運算子。

   d. (選擇性) 對於 [新增說明] — 選用，輸入說明以協助識別查詢清單中的查詢。
7. 展開「預覽 SQL 程式碼」。

   a. 檢視從分析建置器產生的 SQL 程式碼。

   b. 若要複製 SQL 程式碼，請選擇「複製」。

   c. 若要編輯 SQL 程式碼，請選擇 「在 SQL 程式碼編輯器中編輯」。
8. 選擇執行。

> **Note**
>
> 如果可以接收結果的成員尚未設定查詢結果設定，則無法執行查詢。

9. 繼續調整參數並再次執行查詢，或選擇「+」按鈕以在新標籤中開始新查詢。

> **Note**
>
> AWS Clean Rooms 旨在提供清晰的錯誤消息。如果錯誤訊息沒有足夠的詳細資料可協助您進行疑難排解，請連絡客戶團隊。提供錯誤發生方式的描述以及錯誤訊息 (包括任何識別碼)。如需詳細資訊，請參閱 疑難排 AWS Clean Rooms。

使用分析建置器查詢兩個資料表 (彙總或清單)

此程序說明如何使用 AWS Clean Rooms 主控台中的分析產生器，為具有下列條件的協同作業建立查詢：

- 兩個使用彙總分析規則的表格 (每個成員各一個)
- 兩個使用清單分析規則的表格 (每個成員各一個)
- 兩個使用彙總分析規則的表格 (每個成員各一個)，以及兩個使用清單分析規則的表格 (每個成員各一個)

使用分析建置器查詢兩個資料表的步驟

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇「您的會員能力」狀態為「查詢」的合作。
4. 在 [查詢] 索引標籤的 [資料表] 下，檢視兩個資料表及其相關聯的分析規則類型 (彙總分析規則或清單分析規則)。

> **Note**
>
> 如果您在清單中沒有看到預期的表格，可能是因為下列原因：

- 表格尚未關聯。
- 這些表沒有配置分析規則。

5. 在「分析」部分下，打開「分析生成器 UI」。
6. 建立查詢。

如果協同合作包含兩個使用「彙總」分析規則的表格和兩個使用「清單」分析規則的表格，請先選擇「彙總」或「清單」，然後根據選取的分析規則依照提示進行操作。

如果兩個表使用彙總分析規則	如果兩個表使用列表分析規則
1. 在「選擇測量結果」中，複查預設已預先選取的彙總量度，並視需要移除任何量度。 2. 在「比對」記錄中，選擇一或多個記錄。 **Note** 使用分析產生器時，您只能在單對欄上進行比對。 3. (選擇性) 對於「新增區段」— 選用，請選擇一或多個參數。 **Note** 新增區段 — 只有在為表格指定維度時才會顯示選用區段。 4. (選擇性) 對於 [新增篩選器] — 選用，請選擇 [新增篩選器]，然後選擇參數、運算子和值。	1. 針對 「選擇屬性」，複查預設已預先選取的清單屬性，並視需要移除任何測量結果。 2. 在「比對」記錄中，選擇一或多個記錄。 **Note** 使用分析產生器時，您只能在單對欄上進行比對。 3. (選擇性) 對於 [新增篩選器] — 選用，請選擇 [新增篩選器]，然後選擇參數、運算子和值。 若要新增更多篩選器，請選擇 [新增其他篩選器 若要移除篩選器，請選擇 [移除]。 **Note** LIMIT不支援清單查詢。

如果兩個表使用彙總分析規則	如果兩個表使用列表分析規則
若要新增更多篩選器，請選擇 [新增其他篩選器 若要移除篩選器，請選擇 [移除]。 Note ORDER BY不支援彙總查詢。 篩選器僅支援AND運算子。 5. (選擇性) 對於 [新增描述] — 選用，輸入說明以協助識別最近查詢清單中的查詢。	篩選器僅支援AND運算子。 4. (選擇性) 對於 [新增描述] — 選用，輸入說明以協助識別最近查詢清單中的查詢。

7. 展開「預覽 SQL 程式碼」。
   a. 檢視從分析建置器產生的 SQL 程式碼。
   b. 若要複製 SQL 程式碼，請選擇「複製」。
   c. 若要編輯 SQL 程式碼，請選擇 「在 SQL 程式碼編輯器中編輯」。
8. 選擇執行。

> **Note**
> 如果可以接收結果的成員尚未設定查詢結果設定，則無法執行查詢

9. 繼續調整參數並再次執行查詢，或選擇「+」按鈕以在新標籤中開始新查詢。

> **Note**
> AWS Clean Rooms 旨在提供清晰的錯誤消息。如果錯誤訊息沒有足夠的詳細資料可協助您進行疑難排解，請連絡客戶團隊。提供錯誤發生方式的描述以及錯誤訊息 (包括任何識別碼)。如需詳細資訊，請參閱 疑難排 AWS Clean Rooms。

查詢具有差分隱私的資料

一般而言，在開啟差分隱私時，撰寫和執行查詢不會變更。不過，如果沒有足夠的隱私權預算剩餘，您就無法執行查詢。當您執行查詢並使用隱私權預算時，您可以看到大約可以執行多少彙總，以及可能對 future 查詢造成什麼影響。

若要檢視協同合作中差異隱私的影響

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇「您的成員詳細資料」狀態為「執行查詢」的協同作業。
4. 在 [查詢] 索引標籤的 [表格] 下方，檢視剩餘的隱私權預算。這會顯示為剩餘彙總函數的估計數目和使用的公用程式 (以百分比顯示)。

   > **Note**
   >
   > 預估的剩餘彙總函數和使用的公用程式百分比只會顯示可以查詢的成員。

5. 選擇 [檢視影響] 以檢視在結果中注入多少雜訊，以及您可以執行的彙總函數大約數目。

檢視近期查詢

您可以在 [最近的查詢] 索引標籤上檢視過去 90 天內執行的查詢。

> **Note**
>
> 如果您唯一的會員能力是 Con tribute 資料，而您並非支付查詢計算費用的成員，則主控台上不會顯示 [查詢] 索引標籤。

檢視最近查詢的步驟

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇合作。

4. 在 [查詢] 索引標籤的 [查詢] 下，檢視過去 90 天內執行的查詢。
5. 要按狀態對最近的查詢進行排序，請從 「所有狀態」 下拉列表中選擇某個狀態。

   狀態為：「已提交」、「已啟動」、「已取消」、「成功」、「失敗」和「逾時」。

檢視查詢詳細資訊

您可以以執行查詢的成員或可以接收結果的成員身分檢視查詢詳細資訊。

若要檢視查詢的詳細資訊

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇合作。
4. 在「查詢」頁籤上，執行下列其中一項作業：

   - 選擇您要檢視之特定查詢的選項按鈕，然後選擇「檢視明細」。
   - 選擇「受保護的查詢 ID」。
5. 在「查詢詳細資訊」頁面上，

   - 如果您是可以執行查詢的成員，請檢視查詢詳細資訊、SQL 文字和結果。

     您會看到一則訊息，確認查詢結果已傳遞給可接收結果的成員。
   - 如果您是可以接收結果的成員，請檢視查詢詳細資料和結果。

接收查詢結果

作為可以收到結果的會員，您可以從中接收查詢輸出AWS Clean Rooms進入您加入協同作業時指定的 Amazon S3 儲存貯體中。

下列主題說明如何使用AWS Clean Rooms控制台。

主題

如需有關如何查詢資料或檢視查詢的資訊，請呼叫AWS Clean RoomsAPI 直接或使用AWS開發套件，請參閱AWS Clean RoomsAPI 參考資訊。

如需有關查詢記錄的資訊，請參閱查詢登入 AWS Clean Rooms。

> **Note**
>
> 如果您對加密的資料表執行查詢，則加密資料行的結果會加密。

接收查詢結果

查詢結果位於查詢結果設定預設值部分和查詢的部分查詢「」中的標籤AWS Clean Rooms控制台。

若要接收查詢結果

1. 登錄到AWS Management Console並打開AWS Clean Rooms安慰與您的AWS 帳戶（如果您尚未這樣做）。
2. 在左側導覽窗格中選擇合作。
3. 選擇具有以下功能的協作您的會員能力的狀態接收結果。
4. 若要直接從中接收查詢結果AWS Clean Rooms，在「」查詢標籤下查詢，下受保護的查詢 ID欄中，選取查詢。
5. 在「」查詢詳情頁面，下方結果中，執行下列其中一項作業：

如果你想...	然後選擇...
複製結果。	Copy (複製)
下載結果。	下載 **Note** 默認情況下，下載的網站名稱是相應的`Query id`這是在運行查詢時顯示的AWS Clean Rooms。
在 Amazon S3 中看到結果。	在 Amazon S3 中看到 Amazon S3 主控台在單獨的索引標籤中開啟。

6. 如果您使用加密資料，您現在可以使用解密數據表。

   如需詳細資訊，請參閱使用 C3R 加密用戶端解密資料表。

編輯查詢結果設定的預設值

身為可以接收結果的成員，您可以在AWS Clean Rooms控制台。

編輯查詢結果設定的預設值的步驟

1. 登錄到AWS Management Console並打開AWS Clean Rooms安慰與您的AWS 帳戶（如果您尚未這樣做）。
2. 在左側導覽窗格中選擇合作。
3. 選擇具有以下功能的協作您的會員能力的狀態接收結果。
4. 在「」查詢標籤下查詢結果設定，選擇編輯。
5. 在「」編輯查詢結果設定預設值頁面上，視需要修改下列任一項目：

   a. 下查詢結果設定，修改Amazon S3 中的結果目的地或結果格式。

b. 下服務存取，修改授權方法AWS Clean Rooms寫入您所指定的 Amazon S3 儲存貯體中。

已更新查詢結果設定顯示在協同合作詳細資訊頁面上。

在其他中使用查詢輸出AWS 服務

查詢輸出AWS Clean Rooms可在主控台上使用 (如果主控台用於執行查詢)，並在指定的 Amazon S3 儲存貯體中下載。從那裡，您可以在其他中使用查詢輸出AWS 服務，如亞馬遜 QuickSight 和亞馬遜 SageMaker，取決於這些服務使用 Amazon S3 儲存的資料的方式。

有關亞馬遜的更多資訊 QuickSight，請參閱亞馬遜 QuickSight文件。

有關亞馬遜的更多資訊 SageMaker，請參閱亞馬遜 SageMaker文件。

使用 C3R 加密用戶端解密資料表

針對使用「密碼編譯運算」的協同作業，請遵循此程序Clean Rooms和 C3R 加密客戶端來加密數據表。在您擁有之後，請使用此程序在協同作業中查詢的資料。

此程序需要共用密鑰和協同合作 ID。

可以接收結果的成員會使用用於加密協同作業資料的相同共用密鑰和協同作業 ID 來解密資料。

> **Note**
>
> AWS Clean Rooms共同作業已限制可執行及檢視查詢結果的人員。若要執行解密，任何有權存取這些結果的人，都需要用來加密資料的相同共用密鑰和共同作業 ID。

解密加密的資料表

1. (選擇性)檢視 C3R 加密用戶端中可用的命令。
2. (選擇性) 瀏覽至所需的目錄並執行`ls`(macOS) 或`dir`(Windows).
   - 驗證c3r-cli.jar文件和加密的查詢結果數據文件位於所需的目錄中。

     > **Note**
     >
     > 如果查詢結果是從AWS Clean Rooms控制台界面，他們很可能在下載資料夾為您的使用者帳戶。(例如，下載使用者目錄中的資料夾Windows和macOS。) 建議您將查詢結果檔案移至與c3r-cli.jar。
3. 將共用密鑰存儲在`C3R_SHARED_SECRET`環境變數。如需詳細資訊，請參閱步驟 6：將共用密鑰存儲在環境變量中。
4. 從AWS Command Line Interface(AWS CLI)，執行下列命令。

   java -jar c3r-cli.jar decrypt ***<name of input .csv file>*** --id=***<collaboration id>*** --output=***<output file name>***
5. 替換每個`#######`使用您自己的信息：
   a. 對於`id=`」下方，輸入協同作業 ID。
   b. 對於`output=`，輸入輸出檔名稱 (例如，`results-decrypted.csv`).

如果未指定輸出名稱，將在終端機中顯示預設名稱。

c. 使用您偏好的 CSV 或在指定的輸出文件中查看解密的數據Parquet檢視應用程式 (例如 Microsoft Excel、文字編輯器或其他應用程式)。

管理 AWS Clean Rooms

下列主題說明如何 AWS Clean Rooms 使用主 AWS Clean Rooms 控台管理中的協同作業、成員和已配置的表格。

如需如何 AWS Clean Rooms 使用 AWS SDK 進行管理的相關資訊，請參閱 AWS Clean Rooms API 參考。

主題

- 管理協同合作 AWS Clean Rooms
- 管理已配置的資料表 AWS Clean Rooms

管理協同合作 AWS Clean Rooms

下列主題說明協同作業建立者如何AWS Clean Rooms使用主AWS Clean Rooms控台來管理中的協同作業。

如需如何使用 AWS SDK 管理共同作業的相關資訊，請參閱 AWS Clean RoomsAPI 參考。

主題

- 編輯協同合作
- 刪除協同合作
- 檢視協同合作
- 檢視表格和分析規則
- 查看差異隱私使用記錄
- 監控會員狀態
- 從協同作業中移除成員
- 離開合作
- 編輯配置的表格關聯
- 取消已配置表格的關聯
- 編輯微分隱私權政策
- 刪除差異隱私權政策
- 檢視計算出的差異隱私參數

編輯協同合作

瞭解如何編輯共同作業的不同部分。

主題

編輯協同合作名稱和說明

建立協同作業之後，您只能編輯協同作業名稱和說明。

> **Note**
>
> 如果您已啟用查詢記錄，則可以編輯查詢日誌是否存放在 Amazon Lo CloudWatch gs 帳戶中。

若要編輯協同合作名稱和說明

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇您建立的協同合作。
4. 在協同合作詳細資訊頁面上，選擇 [動作]，然後選擇 [編輯協同合作
5. 對於「詳細資訊」，請編輯協同作業的「名稱」和「說明
6. 選擇儲存變更。

編輯協作標籤

身為共同作業建立者，您可以在建立協同合作資源之後管理標籤。

若要編輯協同作業標籤

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇您建立的協同合作。
4. 選擇下列其中一項：

如果您是...	然後...
合作的成員	選擇詳細資訊索引標籤。
協同合作建立者，但不是協同合作的成員	向下捲動頁面至「標籤」區段。

5. 如需協作詳細資料，請選擇管理標籤。
6. 在 Manage tags (管理標籤) 頁面上，可以執行下列操作：
   - 若要移除標籤，請選擇 Remove (移除)。
   - 若要新增標籤，請選擇 Add new tag (新增新標籤)。
   - 若要儲存變更，請選擇 [儲存變更]

編輯會員標籤

身為共同作業建立者，您可以在建立協同合作之後管理成員資格資源上的標籤。

若要編輯成員資格標籤

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇您建立的協同合作。
4. 選擇詳細資訊索引標籤。
5. 如需會員詳細資料，請選擇管理標籤。
6. 在「管理成員資格標記」頁面上，您可以執行下列動作：
   - 若要移除標籤，請選擇 Remove (移除)。

- 若要新增標籤，請選擇 Add new tag (新增新標籤)。
- 若要儲存您所做的變更，請選擇 Save changes (儲存變更)。

編輯關聯的表格標籤

身為協同合作建立者，您可以在將表格與協同合作產生關聯之後，管理關聯表格資源上的標籤。

編輯關聯表格標籤的步驟

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇您建立的協同合作。
4. 選擇 Tables (資料表) 索引標籤。
5. 針對您關聯的表格，選擇一個表格。
6. 在已設定的表格詳細資料頁面上，針對標籤，選擇管理標記。

   在 Manage tags (管理標籤) 頁面上，可以執行下列操作：

   - 若要移除標籤，請選擇 Remove (移除)。
   - 若要新增標籤，請選擇 Add new tag (新增新標籤)。
   - 若要儲存您所做的變更，請選擇 Save changes (儲存變更)。

編輯分析範本標籤

身為共同作業建立者，您可以在建立協同合作之後管理分析範本資源上的標籤。

若要編輯成員資格標籤

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇您建立的協同合作。
4. 選擇 Templates (範本) 標籤。
5. 在「您建立的分析範本」區段中，選擇分析範本。

6. 在分析範本表格詳細資料頁面上，向下捲動至「標籤」區段。
7. 選擇 Manage tags (管理標籤)。
8. 在 Manage tags (管理標籤) 頁面上，可以執行下列操作：
   - 若要移除標籤，請選擇 Remove (移除)。
   - 若要新增標籤，請選擇 Add new tag (新增新標籤)。
   - 若要儲存您所做的變更，請選擇 Save changes (儲存變更)。

編輯差異隱私政策標籤

身為共同作業建立者，您可以在建立協同合作之後管理分析範本資源上的標籤。

若要編輯成員資格標籤

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇包含您要編輯的差異隱私權政策的共同作業。
4. 選擇 Tables (資料表) 索引標籤。
5. 在 [表格] 索引標籤上，選擇 [管理標籤]。
6. 在 Manage tags (管理標籤) 頁面上，可以執行下列操作：
   - 若要移除標籤，請選擇 Remove (移除)。
   - 若要新增標籤，請選擇 Add new tag (新增新標籤)。
   - 若要儲存您所做的變更，請選擇 Save changes (儲存變更)。

刪除協同合作

身為共同作業建立者，您可以刪除您所建立的協同合作。

> **Note**
>
> 刪除共同作業時，您和所有成員都無法執行查詢、接收結果或提供資料。每個協同作業成員都可以繼續存取自己的資料，作為其成員資格的一部分。

若要刪除協同合作

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇您要刪除的協同作業。
4. 在「操作」 下，選擇「刪除協作」
5. 確認刪除，然後選擇 [刪除]。

檢視協同合作

身為共同作業建立者，您可以檢視您所建立的所有共同作業。

若要檢視協同合作

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 在「共同作業」頁面的「上次使用」下，檢視最近使用的 5 個協同作業。
4. 在使用中成員資格標籤上，檢視具有作用中成員資格的共同作業清單。

   您可以按名稱，會員資格創建日期和您的會員詳細信息進行排序。

   您可以使用搜尋列來搜尋協同合作。
5. 在 [可加入] 索引標籤上，檢視可加入的共同作業清單。
6. 在 [不再可用] 索引標籤上，檢視已刪除的共同作業清單，以及不再可用之共同作業的成員資格 (已移除的成員資格)。

檢視表格和分析規則

若要檢視與協同合作和分析規則相關聯的表格

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇合作。

4. 選擇 Tables (資料表) 索引標籤。
5. 選擇下列其中一項：
   a. 若要檢視協同合作中相關聯的表格，請針對您關聯的表格選擇一個表格 (藍色文字)。
   b. 若要檢視共同作業中相關聯的其他表格，請針對共同作業人員關聯的表格選擇表格 (藍色文字)。
6. 在表格詳細資訊頁面上檢視表格詳細資訊和分析規則。

查看差異隱私使用記錄

作為以差分隱私保護數據的協作成員，在您創建具有差異隱私的協作之後，您可以監控隱私預算的使用情況。

若要檢視執行了多少彙總，以及使用了多少隱私權預算

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇合作。
4. 選擇 Tables (資料表) 索引標籤。
5. 選擇 [檢視使用記錄檔 (藍色文字)]。
6. 檢視使用情況詳細資料，包括隱私權預算以及提供的公用程式。

監控會員狀態

身為協同合作建立者，您可以在建立協同作業之後，在「成員」(Members) 標籤上監視所有成員的狀態。

若要檢查成員的狀態

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇您建立的協同合作。
4. 選擇「成員」頁標。

5. 檢視每個成員的「會員」狀態。

從協同作業中移除成員

> **Note**
>
> 移除成員也會從共同作業中移除其所有相關聯的資料集。

若要從協同作業中移除成員

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇您建立的協同合作。
4. 選擇「成員」頁標。
5. 選取要移除之成員旁邊的選項按鈕。

> **Note**
>
> 共同作業建立者無法選擇自己的帳戶 ID。

6. 選擇移除。
7. 在對話方塊中，輸入文字輸入欄位來確認移除成員的決定。**`confirm`**

> **Note**
>
> 如果您移除支付查詢計算費用的成員，則不允許在共同作業中執行其他查詢。

離開合作

身為共同作業成員，您可以刪除您的成員資格以離開協同合作。如果您是協同合作建立者，您只能透過刪除協同合作來離開協同合作。

> **Note**
>
> 刪除會員資格後，即表示您離開共同作業，無法重新加入。如果您是支付查詢計算費用的會員，而您刪除了會員資格，則不允許再執行任何查詢。

若要離開協同合作

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 在使用有效成員資格中，選擇您所屬的協同合作。
4. 選擇動作。
5. 選擇刪除會員資格。
6. 在對話方塊中，輸入文字輸入欄位，然後選擇 [清空並刪除成員資格]，以確定要離開協同合作的決定。**`confirm`**

   您會在主控台上看到訊息，指出成員資格已刪除。

   協同合作建立者會將「成員」狀態視為「左」。

編輯配置的表格關聯

身為協同合作成員，您可以編輯已建立的已配置表格關聯。

編輯已配置的表格關聯

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇合作。
4. 選擇「表格」頁標。
5. 針對您關聯的表格，選擇一個表格。
6. 在表格詳細資訊頁面上，向下捲動以檢視「表格」關聯詳細資訊。
7. 選擇編輯 。
8. 在 「編輯已配置的表格關聯」頁面上，更新「說明」或「服務」存取資訊。

9. 選擇儲存變更。

取消已配置表格的關聯

身為協同合作成員，您可以取消已配置表格與協同作業的關聯。此動作可防止可查詢的成員查詢資料表。

取消已規劃表格的關聯的步驟

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇合作。
4. 選擇「表格」頁標。
5. 針對您關聯的表格，選取您要取消關聯之表格旁邊的選項按鈕。
6. 選擇 Disassociate (取消關聯)。
7. 在對話方塊中，選擇「取消關聯」，以確認取消已配置表格的關聯性的決定，並防止可查詢的成員查詢表格。

編輯微分隱私權政策

在配置差異隱私政策後，您可以隨時更新它以更好地反映您的隱私需求。

若要編輯差異隱私權政策

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇合作。
4. 在協同作業頁面的「表格」標籤上，選擇「您關聯的表格」下方的「編輯」。
5. 在 「編輯差異隱私」頁面上，為下列屬性選擇新值：

    - 隱私權預算 — 移動滑桿以在協同作業期間隨時增加或減少預算。可以查詢的成員開始查詢您的資料後，您就無法減少預算。如果隱私權預算增加，在使用新增的隱私權預算之前，AWS Clean Rooms將繼續使用現有預算，直到完全消耗為止。

- 每個查詢新增的雜訊 — 移動滑桿，以在協同作業期間隨時增加或減少每個查詢新增的雜訊。

> **Note**
>
> 您可以選擇「互動式」範例，探索「隱私權預算」和「每次查詢新增的雜訊」的不同值如何影響您可執行的彙總函式數目。

您無法變更隱私權預算重新整理的值。若要變更您的選擇，您必須刪除差異隱私權政策並建立新的隱私權政策。

6. 選擇儲存變更。

您會看到確認訊息，指出您已成功編輯差異隱私權政策。

刪除差異隱私權政策

您可以從協同作業的 [表格] 索引標籤中刪除差異隱私權政策。

若要刪除差異隱私權政策

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇合作。
4. 在協同作業頁面的 [表格] 索引標籤上，選取 [差異隱私權政策] 旁邊的 [刪除]。
5. 如果您確定要刪除差分隱私權政策，請選擇 [刪除]。

刪除差異隱私權政策後，您將無法存取該政策中的隱私權預算使用記錄。如果刪除差分隱私政策，則無法查詢開啟差分隱私權的表格。

檢視計算出的差異隱私參數

對於具有差分隱私專業知識的使用者，您可以從協同作業的「查詢」索引標籤中檢視計算出的差分隱私參數。

檢視計算出的差分隱私參數的步驟

1. 登入AWS Management Console並使用您的AWS Clean Rooms主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [協同作業]。
3. 選擇合作。
4. 在「查詢」頁籤的「結果」區段中，選取「檢視計算的差分隱私參數」。

在「計算的差異隱私權參數」表格中，您可以看到彙總函式的敏感度值，其定義為新增、移除或修改單一使用者記錄時，函數結果可以變更的最大量。此清單包含下列差異隱私參數：

- 使用者貢獻限制 (UCL) 是 SQL 查詢中使用者貢獻的最大資料列數。舉例來說，如果您想要計算指定廣告活動中每位使用者可以有多次曝光次數的符合曝光次數，AWS Clean Rooms差異隱私就必須限制單一使用者的曝光次數，以確保差異隱私權計算的準確性。換句話說，如果任何使用者的曝光次數多於繫結，則AWS Clean Rooms會根據計算出的 UCL 值，自動取得該使用者曝光次數的統一隨機抽樣，並在執行查詢時排除該使用者的剩餘曝光次數。如果您要計算唯一使用者的數目，UCL 值等於 1。這是因為新增、移除或修改單一使用者最多只能變更 1 個不同使用者的計數。
- 最小值是在聚合函數中使用的運算式的下限，例如`sum()`。例如，如果運算式是稱為的資料行`purchase_value`，則最小值是資料行的下限。
- 最大值是在聚合函數中使用的運算式的上限，例如`sum()`。例如，如果表示式是稱為的欄`purchase_value`，則最大值是資料行的上限。

在「計算的差異隱私參數」表格中，您可以使用這些參數來更好地瞭解查詢結果中的雜訊總量。例如，當每個查詢新增的已設定「雜訊」為 30 位使用者且執行`COUNT DISTINCT (user_id)`查詢時，「AWS Clean Rooms差分隱私」會新增介於 -30 到 30 之間的隨機雜訊，且機率很高，因為敏感度`COUNT DISTINCT`為 1。在具有相同組態的`COUNT`查詢的情況下，「AWS Clean Rooms差分隱私」會新增由使用者貢獻限制縮放的統計雜訊，因為單一使用者可能會對查詢結果提供多個資料列。在像`SUM`查詢的情況下，`SUM (purchase_value)`其中所有的列值是正的，總噪聲是由用戶貢獻限制乘以最大值縮放。 AWS Clean Rooms差分隱私會自動計算敏感度參數，以便在查詢執行階段執行雜訊新增，並耗盡隱私權預算。隱私預算的耗盡是必要的，因為敏感性參數是依賴於數據的。

管理已配置的資料表 AWS Clean Rooms

下列主題說明如何使用主 AWS Clean Rooms 控台管理中已設 AWS Clean Rooms 定的表格。

如需如何使用 AWS SDK 管理已設定資料表的詳細資訊，請參閱 AWS Clean Rooms API 參考。

主題

編輯配置的表格詳細

身為協同合作成員，您可以編輯已配置的表格詳細資訊。

若要編輯配置的表格詳細

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇您建立的已配置表格。
4. 在已設定的表格詳細資訊頁面上，向下捲動至「已設定的表格詳細
5. 選擇編輯。
6. 更新已配置表格的「名稱」或「說明」。
7. 選擇儲存變更。

編輯配置的表格標籤

身為協同合作成員，在您建立已配置的表格之後，您可以在「已配置的表格」標籤上管理已配置表格資源上的標籤。

若要編輯已配置的表格標籤

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇您建立的已配置表格。
4. 在已設定的表格詳細資訊頁面上，向下捲動至「標記」區段。
5. 選擇管理標籤。

6. 在 Manage tags (管理標籤) 頁面上，可以執行下列操作：
   - 若要移除標籤，請選擇 Remove (移除)。
   - 若要新增標籤，請選擇 Add new tag (新增新標籤)。
   - 若要儲存您所做的變更，請選擇 Save changes (儲存變更)。

編輯配置的表格分析規則

編輯已配置的表格分析規則

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇您建立的已配置表格。
4. 在已設定的表格詳細資料頁面上，向下捲動至彙總分析規則、清單分析規則或自訂分析規則區段。（您的選擇取決於您為配置的表格選擇的分析規則類型。）
5. 選擇編輯。
6. 您可以在「編輯分析規則」頁面執行下列作業：
   - 透過下列方式修改分析規則定義：
     - 修改 JSON 編輯器。
     - 選擇從檔案匯入以上傳新的分析規則定義。
   - 從下列選項中選取，即可預覽成員在協同合作中可看到的內容：
     - 表格檢視
     - JSON
     - 查詢範例
7. 選擇儲存變更，以儲存您所做的變更。

刪除配置的表格分析規則

> **Warning**
>
> 此動作無法復原，並會影響所有相關資源。

若要刪除已設定的表格分析規則

1. 登入 AWS Management Console 並使用您的AWS Clean Rooms 主機 AWS 帳戶 (如果您尚未這麼做) 開啟主機。
2. 在左側導覽窗格中，選擇 [已設定的表格]。
3. 選擇您建立的已配置表格。
4. 在已設定的表格詳細資料頁面上，向下捲動至彙總分析規則、清單分析規則或自訂分析規則區段。（您的選擇取決於您為配置的表格選擇的分析規則類型。）
5. 選擇刪除。
6. 如果您確定要刪除分析規則，請選擇 [刪除]。

疑難排 AWS Clean Rooms

本節介紹使用時可能出現的一些常見問題以 AWS Clean Rooms 及如何解決這些問題。

問題

- 查詢所參考的一或多個資料表無法由其關聯的服務角色存取。資料表/角色擁有者必須授與表格的服務角色存取權。
- 其中一個基礎資料集具有不支援的檔案格式。
- 使用的Clean Rooms密碼編譯運算時，查詢結果不如預期。

查詢所參考的一或多個資料表無法由其關聯的服務角色存取。資料表/角色擁有者必須授與表格的服務角色存取權。

- 確認已視需要設定服務角色的權限。如需詳細資訊，請參閱設定 AWS Clean Rooms。

其中一個基礎資料集具有不支援的檔案格式。

- 請確定您的資料集採用其中一種支援的檔案格式：
  - Parquet
  - RCFile
  - TextFile
  - SequenceFile
  - RegexSerde
  - OpenCSV
  - AVRO
  - JSON

  如需詳細資訊，請參閱 資料格式 AWS Clean Rooms。

使用的Clean Rooms密碼編譯運算時，查詢結果不如預期。

如果您使用的是 Clean Rooms (C3R) 的「密碼編譯運算」，請確認您的查詢是否正確使用加密資料行：

- 這些sealed欄僅用於SELECT子句中。
- 這些fingerprint欄僅用於JOIN子句 (和特定條件下的GROUP BY子句)。
- 如果協同作業設定需要，您只是具有相同名稱的JOINingfingerprint欄。

如需更多詳細資訊，請參閱 密碼計算 及 the section called “列類型”。

中的安全性 AWS Clean Rooms

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。要了解適用的合規計劃 AWS Clean Rooms，請參閱合規計劃的 AWS 服務範圍合規計劃。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Clean Rooms。它會說明如何設定 AWS Clean Rooms 以符合安全性和合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的 AWS Clean Rooms 資源。

目錄

資料保護 AWS Clean Rooms

AWS 共用責任模型適用於中的資料保護 AWS Clean Rooms。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API AWS Clean Rooms 或 AWS SDK 時 AWS 服務 使用或其他使用時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

靜態加密

AWS Clean Rooms 永遠加密靜態的所有服務中繼資料，而不需要任何額外的設定。當您使用時，此加密是自動的 AWS Clean Rooms。

無塵室 ML 會加密儲存在靜態服務中的所有資料。 AWS KMS如果您選擇提供自己的 KMS 金鑰，您的相似模型和相似區段產生任務的內容會使用 KMS 金鑰進行靜態加密。

> **Note**
>
> 您可以使用 Amazon S3 中的加密選項來保護靜態資料。
> 如需詳細資訊，請參閱 Amazon S3 使用者指南中的指定 Amazon S3 加密。

傳輸中加密

AWS Clean Rooms 使用傳輸層安全性 (TLS) 和用戶端加密來進行傳輸中的加密。與通信始終 AWS Clean Rooms 通過 HTTPS 完成，因此您的數據在傳輸過程中始終是加密的。這包括使用無塵室 ML 時傳輸中的所有資料。

加密基礎資料

如需如何加密基礎資料的詳細資訊，請參閱密碼編譯運算 Clean Rooms。

資料保留 AWS Clean Rooms

當您建立相似的模型時，Clean Rooms ML 會讀取您的訓練資料，將其轉換為適合我們 ML 模型的格式，並將訓練過的模型參數儲存在 Clean Rooms ML 中。無塵室 ML 不會保留訓練資料的副本。 AWS Clean Rooms 查詢執行後，SQL 查詢不會保留任何資料。然後，無塵室 ML 會使用訓練有素的模型來總結所有使用者的行為。只要相似模型處於作用中狀態，Clean Rooms ML 就會為資料中的每個使用者儲存使用者層級的資料集。

當您啟動相似區段產生工作時，Clean Rooms ML 會讀取種子資料、從關聯的相似模型讀取行為摘要，並建立儲存在服務中的相似區段。 AWS Clean Rooms 無塵室 ML 不會保留種子資料的副本。只要工作處於作用中狀態，無塵室 ML 就會儲存工作的使用者層級輸出。

如果您想要移除相似模型或相似區段產生工作資料，請使用 API 將其刪除。清理室 ML 會以非同步方式刪除與模型或工作相關聯的所有資料。完成此程序後，Clean Rooms ML 會刪除模型或工作的中繼資料，且該中繼資料將不再顯示在 API 中。無塵室 ML 會保留已刪除的資料 3 天，以防止災難復原。一旦工作或模型在 API 中不再顯示，且已經過去 3 天，與該模型或工作相關聯的所有資料都會被永久刪除。

資料協同合作的最佳做法 AWS Clean Rooms

本主題說明在 AWS Clean Rooms中執行資料協同合作的最佳作法。

AWS Clean Rooms 遵循AWS 共同責任模式。 AWS Clean Rooms 提供分析規則，您可以設定這些規則，以加強在協同合作中保護敏感資料的能力。您在中設定的分析規則 AWS Clean Rooms 會強制執行您已設定的限制 (查詢控制項和查詢輸出控制項)。您負責確定限制並相應地配置分析規則。

數據協作可能涉及的 AWS Clean Rooms不僅僅是您使用. 為了協助您充分發揮資料協同合作的優勢，建議您在使用分析規則時，執行下列最佳作法， AWS Clean Rooms 並特別是搭配使用分析規則。

主題

- 最佳做法 AWS Clean Rooms
- 在中使用分析規則的最佳作法 AWS Clean Rooms

最佳做法 AWS Clean Rooms

您有責任評估每次數據協作的風險，並將其與您的隱私要求（例如外部和內部合規計劃和政策）進行比較。我們建議您在使用時採取其他行動 AWS Clean Rooms。這些動作可能有助於進一步管理風險，並協助防範第三方嘗試重新識別您的資料 (例如差異攻擊或旁通道攻擊)。

例如，在進行合作之前，請考慮對其他合作者進行盡職調查，並與他們簽訂法律協議。若要監控您資料的使用情況，請考慮在使用時採用其他稽核機制 AWS Clean Rooms。

在中使用分析規則的最佳作法 AWS Clean Rooms

中的分析規則可 AWS Clean Rooms 讓您透過在已配置的資料表上設定查詢控制項來限制可執行的查詢。例如，您可以設定查詢控制項，說明如何聯結已配置的資料表，以及可以選取哪些資料行。您也可以透過設定查詢結果控制項 (例如輸出資料列上的彙總臨界值) 來限制查詢輸出。服務會拒絕任何查詢，並移除不符合成員在查詢中設定資料表上設定的分析規則的資料列。

我們建議您在已配置的表格上使用分析規則時採用以下 10 種最佳作法：

- 針對個別的查詢使用案例 (例如，受眾規劃或歸因) 建立個別設定的資料表。您可以使用相同的基礎資料表建立多個已設定的資料 AWS Glue 表。
- 在分析規則中指定合作查詢所需的欄 (例如維度欄、清單欄、聯結欄)。這可能有助於降低差異攻擊的風險，或讓其他成員對您的資料進行逆向工程。使用允許清單資料欄功能來記下您 future 可能想要查詢的其他資料欄。若要自訂可用於特定協同合作的資料欄，請使用相同的基礎資料表建立其他已設定的資料 AWS Glue 表。
- 在分析規則中指定協同合作中進行分析所需的函數。這有助於降低可能在個別資料點上呈現資訊的罕見功能錯誤所帶來的風險。若要自訂可用於特定協同合作的函數，請使用相同的基礎資料表建立其他已設定的資料 AWS Glue 表。
- 在資料列層級值敏感的任何資料行上新增彙總條件約束。這包括已配置表格中的欄，這些欄也存在於其他協同作業成員資料表和分析規則中，做為彙總條件約束。這也包括已設定資料表中無法查詢的資料欄，也就是已設定資料表中但不在分析規則中的資料行。彙總限制可協助降低因為查詢結果與協同合作以外的資料建立關聯而產生的風險
- 建立測試協同作業和分析規則，以測試使用指定分析規則建立的限制。
- 檢閱已配置資料表上的共同作業人員設定的資料表和成員的分析規則，以檢查它們是否符合協同合作所同意的內容。這有助於降低其他成員自行設計資料以執行未同意的查詢所造成的風險。
- 在設定分析規則之後，檢閱已設定資料表上所提供的查詢範例 (僅限主控台)。

> **Note**
>
> 除了提供的範例查詢之外，還可以根據分析規則和其他協同合作成員表格和分析規則進行其他查詢。

- 您可以在協同合作中新增或更新已配置表格的分析規則。當您執行此操作時，請檢閱與已配置表格相關聯的所有協同作業及其產生的影響。這有助於確保沒有協同合作使用過時的分析規則。
- 檢閱共同作業中執行的查詢，以檢查查詢是否符合使用案例或協同合作商定的查詢。當查詢記錄功能開啟時，查詢記錄檔中可用。) 這有助於降低成員執行未同意的分析以及潛在攻擊 (例如側通道攻擊) 的風險。
- 檢閱協同作業成員分析規則和查詢中使用的已配置表格欄，以檢查它們是否符合協同合作中同意的內容。開啟該功能時，查詢記錄檔中即可使用這些查詢。) 這有助於降低其他成員自行設計資料以執行未同意的查詢所造成的風險。

的 Identity and Access Management AWS Clean Rooms

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有權限) 來使用 AWS Clean Rooms 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在進行的工作 AWS Clean Rooms。

服務使用者 — 如果您使用 AWS Clean Rooms 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AWS Clean Rooms 功能來完成工作時，您可能需要其他權限。了解存取的管理方式可協助您向管理員請求正確的許可。若您無法存取 AWS Clean Rooms中的某項功能，請參閱 疑難排解 AWS Clean Rooms 身分和存取。

服務管理員 — 如果您負責公司的 AWS Clean Rooms 資源，您可能擁有完整的存取權 AWS Clean Rooms。決定您的服務使用者應該存取哪些 AWS Clean Rooms 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步瞭解貴公司如何搭配使用 IAM AWS Clean Rooms，請參閱如何與 IAM AWS Clean Rooms 搭配使用。

IAM 管理員：如果您是 IAM 管理員，建議您掌握如何撰寫政策以管理 AWS Clean Rooms存取權的詳細資訊。若要檢視可在 IAM 中使用的 AWS Clean Rooms 基於身分的政策範例，請參閱。以身分識別為基礎的原則範例 AWS Clean Rooms

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者或貴公司的單一登入驗證是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 使用者指南中的如何登入您 AWS 帳戶的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以便使用您的認證加密簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議方法來自行簽署請求的詳細資訊，請參閱 AWS 一般參考 中的第 4 版簽署程序。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 根使用者，使用建立帳戶時所使用的電子郵件地址和密碼即可登入並存取。強烈建議您不要以根使用者處理日常作業。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱中的登入AWS 帳戶根使用者 資料和 IAM 身分AWS 一般參考。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI

或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

每個 IAM 實體 (使用者或角色) 在開始時都沒有許可。根據預設，使用者無法執行任何作業，甚至也無法變更他們自己的密碼。若要授予使用者執行動作的許可，管理員必須將許可政策附加到使用者。或者，管理員可以將使用者新增到具備預定許可的群組。管理員將許可給予群組時，該群組中的所有使用者都會獲得那些許可。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策則是獨立的政策，您可以將這些政策附加到 AWS 帳戶中的多個使用者、群組和角色。受管政策包括 AWS 受管政策和客戶管理的策略。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源

的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需 Organizations 和 SCP 的詳細資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

如何與 IAM AWS Clean Rooms 搭配使用

在您使用 IAM 管理存取權限之前 AWS Clean Rooms，請先了解哪些 IAM 功能可搭配使用 AWS Clean Rooms。

您可以搭配使用的 IAM 功能 AWS Clean Rooms

IAM 功能	AWS Clean Rooms 支持
身分型政策	是
資源型政策	部分
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	部分
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	是
服務連結角色	否

若要深入瞭解如何以 AWS Clean Rooms 及其他如何 AWS 服務 使用大多數 IAM 功能 AWS 服務 ，請參閱 IAM 使用者指南中的 IAM。

以身分識別為基礎的原則 AWS Clean Rooms

支援身分型政策	是

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

以身分識別為基礎的原則範例 AWS Clean Rooms

若要檢視以 AWS Clean Rooms 身分為基礎的原則範例，請參閱。以身分識別為基礎的原則範例 AWS Clean Rooms

以資源為基礎的政策 AWS Clean Rooms

支援以資源基礎的政策	部分

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

此 AWS Clean Rooms 服務僅支援一種以資源為基礎的原則，稱為已設定的相似模型受管理資源原則，該原則會附加至已設定的相似模型。此原則定義哪些主參與者可以在已設定的相似模型上執行動作。

要了解如何將以資源為基礎的策略附加到已設定的相似模型，請參閱。適用於 AWS Clean Rooms ML 的 IAM 行為

的政策動作 AWS Clean Rooms

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS Clean Rooms 動作清單，請參閱服務授權參考 AWS Clean Rooms中所定義的動作。

中的策略動作在動作之前 AWS Clean Rooms 使用下列前置詞。

```
cleanrooms
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "cleanrooms:action1",
      "cleanrooms:action2"
         ]
```

若要檢視以 AWS Clean Rooms 身分為基礎的原則範例，請參閱。以身分識別為基礎的原則範例 AWS Clean Rooms

的政策資源 AWS Clean Rooms

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 AWS Clean Rooms 資源類型及其 ARN 的清單，請參閱服務授權參考 AWS Clean Rooms中的定義資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Clean Rooms定義的動作。

若要檢視以 AWS Clean Rooms 身分為基礎的原則範例，請參閱。以身分識別為基礎的原則範例 AWS Clean Rooms

的政策條件索引鍵 AWS Clean Rooms

支援服務特定政策條件金鑰	部分

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要瞭解 AWS Clean Rooms ML 如何使用原則條件金鑰，請參閱適用於 AWS Clean Rooms ML 的 IAM 行為。

ACL 在 AWS Clean Rooms

支援 ACL	否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

阿巴克與 AWS Clean Rooms

支援 ABAC (政策中的標籤)	是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱 IAM 使用者指南中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的使用屬性型存取控制 (ABAC)。

使用臨時登入資料 AWS Clean Rooms

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

轉寄存取工作階段 AWS Clean Rooms

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

AWS Clean Rooms的服務角色

支援服務角色	是

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 AWS Clean Rooms 功能。只有在 AWS Clean Rooms 提供指引時才編輯服務角色。

服務連結角色 AWS Clean Rooms

支援服務連結角色。	否

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

以身分識別為基礎的原則範例 AWS Clean Rooms

根據預設，使用者和角色不具備建立或修改 AWS Clean Rooms 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需有關由定義的動作和資源類型的詳細資訊 AWS Clean Rooms，包括每個資源類型的 ARN 格式，請參閱服務授權參考 AWS Clean Rooms中的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 使用 AWS Clean Rooms 主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 AWS Clean Rooms 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access

Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 AWS Clean Rooms 主控台

若要存取 AWS Clean Rooms 主控台，您必須擁有最少一組權限。這些權限必須允許您列出和檢視有關 AWS 帳戶. AWS Clean Rooms 如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色仍可使用 AWS Clean Rooms 主控台，請同時將 AWS Clean Rooms *FullAccess*或受*ReadOnly* AWS 管理的原則附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "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 受管理的政策 AWS Clean Rooms

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理的策略：**AWSCleanRoomsReadOnlyAccess**

您可以附加AWSCleanRoomsReadOnlyAccess至 IAM 主體。

此原則會將唯讀權限授與AWSCleanRoomsReadOnlyAccess協同作業中的資源和中繼資料。

許可詳細資訊

此政策包含以下許可：

- CleanRoomsRead— 允許主參與者對服務的唯讀存取權。
- ConsoleDisplayTables— 允許主參與者唯讀存取所需的中 AWS Glue 繼資料，以便在主控台上顯示基礎資料 AWS Glue 表的相關資料。
- ConsoleLogSummaryQueryLogs— 允許主參與者查看查詢記錄檔。
- ConsoleLogSummaryObtainLogs-允許主參與者擷取記錄結果。

```
{
 "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 受管理的策略：**AWSCleanRoomsFullAccess**

您可以附加AWSCleanRoomsFullAccess至 IAM 主體。

此原則授與管理權限，允許在 AWS Clean Rooms 協同作業中對資源和中繼資料的完整存取 (讀取、寫入和更新)。此原則包括執行查詢的存取權。

許可詳細資訊

此政策包含以下許可：

- CleanRoomsAccess— 授予對所有資源的所有動作的完整存取權 AWS Clean Rooms。
- PassServiceRole— 授與僅將服務角色傳遞給其名稱中具有 "cleanrooms" 的服務 (PassedToService條件) 的存取權。
- ListRolesToPickServiceRole— 可讓主參與者列出其所有角色，以便在使用 AWS Clean Rooms時選擇服務角色。
- GetRoleAndListRolePoliciesToInspectServiceRole— 允許主體在 IAM 中查看服務角色和對應的政策。
- ListPoliciesToInspectServiceRolePolicy— 允許主體在 IAM 中查看服務角色和對應的政策。
- GetPolicyToInspectServiceRolePolicy— 允許主體在 IAM 中查看服務角色和對應的政策。
- ConsoleDisplayTables— 允許主參與者唯讀存取所需的中 AWS Glue 繼資料，以便在主控台上顯示基礎資料 AWS Glue 表的相關資料。
- ConsolePickQueryResultsBucketListAll— 允許主體從寫入查詢結果的所有可用 S3 儲存貯體清單中選擇 Amazon S3 儲存貯體。
- SetQueryResultsBucket— 允許主體選擇要寫入其查詢結果的 S3 儲存貯體。

- ConsoleDisplayQueryResults— 允許主體向客戶顯示查詢結果，並從 S3 儲存貯體讀取。
- WriteQueryResults— 允許主體將查詢結果寫入客戶擁有的 S3 儲存貯體。
- EstablishLogDeliveries— 允許主體將查詢日誌傳遞到客戶的 Amazon CloudWatch 日誌日誌群組。
- SetupLogGroupsDescribe— 允許主體使用 Amazon CloudWatch 日誌記錄群組建立程序。
- SetupLogGroupsCreate— 允許主體建立 Amazon CloudWatch 日誌日誌群組。
- SetupLogGroupsResourcePolicy— 允許主體在 Amazon CloudWatch 日誌日誌群組上設定資源政策。
- ConsoleLogSummaryQueryLogs— 允許主參與者查看查詢記錄檔。
- ConsoleLogSummaryObtainLogs-允許主參與者擷取記錄結果。

```
{
 "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 受管理的策略：**AWSCleanRoomsFullAccessNoQuerying**

您可以附加AWSCleanRoomsFullAccessNoQuerying到您的IAM principals.

此原則授與管理權限，允許在 AWS Clean Rooms 協同作業中對資源和中繼資料的完整存取 (讀取、寫入和更新)。此原則會排除執行查詢的存取權。

許可詳細資訊

此政策包含以下許可：

- CleanRoomsAccess— 授予對所有資源上所有動作的完整存取權 AWS Clean Rooms，但在協同作業中查詢除外。

- CleanRoomsNoQuerying— 明確拒絕StartProtectedQuery並防UpdateProtectedQuery止查詢。
- PassServiceRole— 授與僅將服務角色傳遞給其名稱中具有 "cleanrooms" 的服務 (PassedToService條件) 的存取權。
- ListRolesToPickServiceRole— 可讓主參與者列出其所有角色，以便在使用 AWS Clean Rooms時選擇服務角色。
- GetRoleAndListRolePoliciesToInspectServiceRole— 允許主體在 IAM 中查看服務角色和對應的政策。
- ListPoliciesToInspectServiceRolePolicy— 允許主體在 IAM 中查看服務角色和對應的政策。
- GetPolicyToInspectServiceRolePolicy— 允許主體在 IAM 中查看服務角色和對應的政策。
- ConsoleDisplayTables— 允許主參與者唯讀存取所需的中 AWS Glue 繼資料，以便在主控台上顯示基礎資料 AWS Glue 表的相關資料。
- EstablishLogDeliveries— 允許主體將查詢日誌傳遞到客戶的 Amazon CloudWatch 日誌日誌群組。
- SetupLogGroupsDescribe— 允許主體使用 Amazon CloudWatch 日誌記錄群組建立程序。
- SetupLogGroupsCreate— 允許主體建立 Amazon CloudWatch 日誌日誌群組。
- SetupLogGroupsResourcePolicy— 允許主體在 Amazon CloudWatch 日誌日誌群組上設定資源政策。
- ConsoleLogSummaryQueryLogs— 允許主參與者查看查詢記錄檔。
- ConsoleLogSummaryObtainLogs-允許主參與者擷取記錄結果。
- cleanrooms— 管理服務內的協作、分析範本、已配置的表格、成員資格和相關資源。 AWS Clean Rooms 執行各種作業，例如建立、更新、刪除、列出和擷取這些資源的相關資訊。
- iam— 將名稱包含 "cleanrooms" 的服務角色傳遞給 AWS Clean Rooms 服務。列出角色、原則，並檢查與服務相關的 AWS Clean Rooms 服務角色和原則。
- glue— 擷取有關資料庫、表格、分割區和結構描述的資訊 AWS Glue。這是 AWS Clean Rooms 服務顯示和與基礎資料來源互動所必需的。
- logs— 管理日誌的日誌傳遞， CloudWatch 日誌組和資源策略。查詢和擷取與 AWS Clean Rooms 服務相關的記錄。這些權限對於服務內的監視、稽核和疑難排解是必要的。

此原則也明確拒絕這些動
作，cleanrooms:StartProtectedQuery並cleanrooms:UpdateProtectedQuery防止使用者直接執行或更新受保護的查詢，而這些查詢應透過受 AWS Clean Rooms 控制的機制來完成。

```
{
 "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 受管理的策略：**AWSCleanRoomsMLReadOnlyAccess**

您可以附加AWSCleanRoomsMLReadOnlyAccess至 IAM 主體。

此原則會將唯讀權限授與AWSCleanRoomsMLReadOnlyAccess協同作業中的資源和中繼資料。

此政策包含以下許可：

- CleanRoomsConsoleNavigation— 授予檢視 AWS Clean Rooms 主控台畫面的存取權。
- CleanRoomsMLRead— 允許主體以唯讀方式存取「清潔室 ML」服務。

```
{
    "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 受管理的策略：**AWSCleanRoomsMLFullAccess**

您可以附加AWSCleanRoomsMLFullAcces至 IAM 主體。此原則授與允許 Clean Rooms ML 所需資源和中繼資料的完整存取權 (讀取、寫入和更新) 的管理權限。

許可詳細資訊

此政策包含以下許可：

- CleanRoomsMLFullAccess— 授予對所有潔淨室 ML 動作的存取權。

- PassServiceRole— 授與僅將服務角色傳遞給其名稱中具有 "cleanrooms-ml" 的服務 (PassedToService條件) 的存取權。
- CleanRoomsConsoleNavigation— 授予檢視 AWS Clean Rooms 主控台畫面的存取權。
- CollaborationMembershipCheck— 當您在協同作業中啟動對象產生 (相似區段) 工作時，Clean Rooms ML 服務會呼叫ListMembers以檢查共同作業是否有效、呼叫者是作用中成員，以及設定的對象模型擁有者是作用中成員。一律需要此權限；只有主控台使用者才需要主控台瀏覽 SID。
- AssociateModels— 允許主參與者將「潔淨室」ML 模型與您的協同合作產生關聯。
- TagAssociations— 允許主參與者將標籤新增至相似模型與協同合作之間的關聯。
- ListRolesToPickServiceRole— 可讓主參與者列出其所有角色，以便在使用 AWS Clean Rooms時選擇服務角色。
- GetRoleAndListRolePoliciesToInspectServiceRole— 允許主體在 IAM 中查看服務角色和對應的政策。
- ListPoliciesToInspectServiceRolePolicy— 允許主體在 IAM 中查看服務角色和對應的政策。
- GetPolicyToInspectServiceRolePolicy— 允許主體在 IAM 中查看服務角色和對應的政策。
- ConsoleDisplayTables— 允許主參與者唯讀存取所需的中 AWS Glue 繼資料，以便在主控台上顯示基礎資料 AWS Glue 表的相關資料。
- ConsolePickOutputBucket— 允許主體為已設定的受眾模型輸出選取 Amazon S3 儲存貯體。
- ConsolePickS3Location— 可讓主參與者選取值區內的位置，以進行已配置的受眾模型輸出。

```
{
    "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 RoomsAWS 受管理策略的更新

檢視 AWS Clean Rooms 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「 AWS Clean Rooms 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AWSCleanRoomsFullAccessNoQuerying – 更新現有政策	已新增 cleanrooms:BatchGetSchemaAnalysisRule 到 CleanRoomsAccess。	2024年5月13日
AWSCleanRoomsFullAccess – 更新現有政策	已ConsolePickQueryResultsBucket將此原則中的 [陳述式 ID] AWSCleanRoomsFullAccess 從SetQueryResultsBucket中更新至，以更好地表示權限，因為在使用和不使用主控台的情況下都需要使用權限來設定查詢結果值區。	2024年3月21日
AWSCleanRoomsMLReadOnlyAccess – 新政策 AWSCleanRoomsMLFullAccess – 新政策	添加AWSCleanRoomsMLReadOnlyAccessAWSCleanRoomsMLFullAccess並支持 AWS Clean Rooms ML。	2023 年 11 月 29 日
AWSCleanRoomsFullAccessNoQuerying – 更新現有政策	已新增cleanrooms:CreateAnalysisTemplatecleanrooms:GetAnalysisTemplate、cleanrooms:UpdateAnalysisTemplate、 cleanrooms:DeleteAnalysisTemplate、cleanrooms:ListAnalysisTemplates、cleanrooms:GetCollaborationAnalysisTemplate、cleanrooms:BatchGetCollaborationAnalysisTemplate、和cleanrooms:ListCollaborationAnalysisTemplates以啟	2023 年 7 月 31 日

變更	描述	日期
	CleanRoomsAccess用新的分析範本功能。	
AWSCleanRoomsFullAccessNoQuerying – 更新現有政策	已新增cleanrooms:ListTagsForResourcecleanrooms:UntagResource、和cleanrooms:TagResource以啟CleanRoomsAccess用資源標記。	2023 年 3 月 21 日
AWS Clean Rooms 開始追蹤變更	AWS Clean Rooms 開始追蹤其 AWS 受管理策略的變更。	2023 年 1 月 12 日

疑難排解 AWS Clean Rooms 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能會遇到的 AWS Clean Rooms 常見問題。

主題

- 我沒有執行操作的授權 AWS Clean Rooms
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪 AWS 帳戶 問我的 AWS Clean Rooms 資源

我沒有執行操作的授權 AWS Clean Rooms

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 cleanrooms:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cleanrooms:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 Mateo 政策，允許他使用 cleanrooms:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到錯誤，告知您未獲授權執行 `iam:PassRole` 動作，您的政策必須更新，允許您將角色傳遞給 AWS Clean Rooms。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

名為 `marymajor` 的 IAM 使用者嘗試使用主控台在 AWS Clean Rooms中執行動作時，發生下列範例錯誤。但是，動作要求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 AWS Clean Rooms 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 AWS Clean Rooms 支援這些功能，請參閱如何與 IAM AWS Clean Rooms 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策的差異。

預防跨服務混淆代理人

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

建議您在資源策略中使用aws:SourceArn全域條件內容索引鍵，以限制將其他服務 AWSClean Rooms提供給資源的權限。如果您想要僅允許一個資源與跨服務存取相關聯，則請使用 aws:SourceArn。

防範混淆代理人問題的最有效方法是使用 aws:SourceArn 全域條件內容索引鍵，以及資源的完整 ARN。在中 AWSClean Rooms，您還必須與sts:ExternalId條件索引鍵進行比較。

的值aws:SourceArn必須設定為假定角色之成員資格的 ARN。

下列範例顯示如何使用aws:SourceArn全域條件前後關聯鍵入 AWSClean Rooms來避免混淆的副問題。

> **Note**
>
> 範例原則適用於 AWSClean Rooms用來存取客戶資料之服務角色的信任原則。
> 會*# ID* 的值是您在協同合作中的 AWSClean Rooms會員 ID。

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

適用於 AWS Clean Rooms ML 的 IAM 行為

跨帳戶工作

無塵室 ML 允許一個人創建的某些資源被另一個 AWS 帳戶 人在他們的帳戶中安全地訪問 AWS 帳戶。當 AWS 帳戶 A 中的用戶端呼叫 StartAudienceGenerationJob AWS 帳戶 B 擁有的ConfiguredAudienceModel資源時，無塵室 ML 會為該工作建立兩個 ARN。A 中的一個 ARN 和 AWS 帳戶 B 中的另一個 AWS 帳戶 。ARN 除了它 AWS 帳戶們之外是相同的。

Clean Rooms ML 會為任務建立兩個 ARN，以確保兩個帳戶都可以將自己的 IAM 政策套用至任務。例如，兩個帳戶都可以使用以標籤為基礎的存取控制，並套用其 AWS 組織的策略。工作會處理來自兩個帳戶的資料，因此兩個帳戶都可以刪除工作及其相關資料。兩個帳戶都不能阻止其他帳戶刪除工作。

只有一個作業執行，而且兩個帳戶在呼叫時都可以看到工作ListAudienceGenerationJobs。這兩個帳戶都可以使用具有自己的 AWS 帳戶 ID 的 ARN 在工作上呼叫Delete、和 Export API。Get

使 AWS 帳戶 用帶有其他 AWS 帳戶 ID 的 ARN 時，兩者都無法訪問作業。

工作的名稱在中必須是唯一的 AWS 帳戶。在 AWS 帳戶 B 中的名稱是 *$ ## $* 名稱。在 B 中 AWS 帳戶 檢視工作時， AWS 帳戶 A 選擇的名稱會以 AWS 帳戶 A 為前綴。

為了讓跨帳戶StartAudienceGenerationJob成功， AWS 帳戶 B 必須使用類似下列範例的資源策略，對 AWS 帳戶 B 中的新工作和 AWS 帳戶 B ConfiguredAudienceModel 中的新工作都允許該動作：

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

如果您使用 AWS Clean Rooms ML API 建立`manageResourcePolicies`設定為 true 的相似模型，請為您 AWS Clean Rooms 建立此原則。

此外，AWS 帳戶 A 中呼叫者的身份政策需要`StartAudienceGenerationJob`權限`arn:aws:cleanrooms-ml:us-west-1:AccountA:audience-generation-job/*`。因此，有三個 IAM 資源的行動`StartAudienceGenerationJob`：AWS 帳戶 A 工作，AWS 帳戶 B 工作和 AWS 帳戶 B `ConfiguredAudienceModel`。

> **Warning**
>
> 開始工作的會收到有關 AWS 帳戶 該工作的 AWS CloudTrail 稽核記錄事件。擁有 AWS 帳戶的`ConfiguredAudienceModel`不會收到 AWS CloudTrail 稽核記錄事件。

標記工作

當您設定childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE參數時CreateConfiguredAudienceModel，帳戶內所有從設定的相似模型建立的相似節段產生工作，預設為具有與已設定的相似相似模型相同的標記。設定的相似模型是父項，相似區段產生工作是子項。

如果您要在自己的帳戶中建立工作，則工作的要求標籤會覆寫父標籤。由其他帳戶建立的工作絕不會在您的帳戶中建立標籤。如果您設置childResourceTagOnCreatePolicy=FROM_PARENT_RESOURCE了另一個帳戶創建了一個作業，則該作業有兩個副本。您帳戶中的副本具有父資源標籤，而工作提交者帳戶中的副本具有來自請求的標籤。

驗證協同合作者

將權限授與 AWS Clean Rooms 協同作業的其他成員時，資源策略應包含條件索引鍵cleanrooms-ml:CollaborationId。這會強制要StartAudienceGenerationJob求中包含collaborationId參數。當collaborationId參數包含在請求中時，Clean Rooms ML 會驗證協同合作是否存在、工作提交者是共同作業的作用中成員，而設定的相似模型擁有者是共同作業的作用中成員。

當 AWS Clean Rooms 管理設定的相似模型資源策略（manageResourcePolicies參數TRUE在CreateConfiguredAudienceModelAssociation 請求中）時，將在資源策略中設置此條件鍵。因此，您必須指定collaborationId中的StartAudienceGenerationJob。

跨帳戶存取權

只StartAudienceGenerationJob能跨帳戶呼叫。所有其他無塵室 ML API 只能與您自己帳戶中的資源搭配使用。這可確保您的訓練資料、相似模型組態和其他資訊保持私密。

無塵室 ML 永遠不會透露 Amazon S3 或跨帳戶的 AWS Glue 位置。訓練資料位置、設定的相似模型輸出位置，以及相似區段產生工作植入位置，在帳戶之間永遠不會顯示。如果您Get是另一個帳戶提交的受眾產生工作，則服務不會顯示種子位置。

符合性驗證 AWS Clean Rooms

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，如 PCI DSS 等各種合規性需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

韌性 AWS Clean Rooms

AWS 全球基礎架構是圍繞區 AWS 域和可用區域建立的。區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

基礎結構安全 AWS Clean Rooms

作為託管服務， AWS Clean Rooms 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫透 AWS Clean Rooms 過網路進行存取。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

網路安全

在查詢執行期間從 S3 儲存貯體 AWS Clean Rooms 讀取時， AWS Clean Rooms 和 Amazon S3 之間的流量會透過 AWS 私有網路安全路由。傳輸中的流量是使用 Amazon Signature 第 4 版通訊協定 (SIGv4) 來簽署，並使用 HTTPS 來加密。此流量會根據您為設定的表格設定的 IAM 服務角色進行授權。

您可以透 AWS Clean Rooms 過端點以程式設計方式連線到。如需服務端點的清單，請參閱AWS Clean Rooms AWS 一般參考.

所有服務端點均僅限 HTTPS。如果您想要從 VPC 連接到並且不想具有網際網路連線， AWS Clean Rooms 則可以使用 Amazon 虛擬私有雲 (VPC) 端點。如需詳細資訊，請參閱AWS PrivateLink 指南 AWS PrivateLink中的透過存取 AWS 服務。

您可以將 IAM 政策指派給 IAM 主體，這些主體會使用 aws: SourceVpce 內容金鑰來限制 IAM 主體只能透過 VPC 端點撥打電話，而不能 AWS Clean Rooms 透過網際網路撥打電話。

使用介面端點存取 AWS Clean Rooms 或 AWS Clean Rooms ML (AWS PrivateLink)

您可以使 AWS PrivateLink 用在虛擬私有雲 (VPC) 和 AWS Clean Rooms / AWS Clean Rooms 或 ML 之間建立私人連線。您可以在不使用網際網路閘道、NAT 裝置、VPN 連線 AWS Clean Rooms 或連線

的情況下，就像在 VPC 中一樣存取或 AWS Clean Rooms AWS Direct Connect ML。VPC 中的執行個體不需要公用 IP 位址即可存取 AWS Clean Rooms。

您可以建立由 AWS PrivateLink提供支援的介面端點來建立此私有連線。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是請求者管理的網路介面，可作為目的地為 AWS Clean Rooms之流量的進入點。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的透過 AWS PrivateLink存取 AWS 服務。

的注意事項 AWS Clean Rooms

設定的介面端點之前 AWS Clean Rooms，請先檢閱AWS PrivateLink 指南中的考量事項。

AWS Clean Rooms 和 AWS Clean Rooms ML 支持通過接口端點對其所有 API 操作進行調用。

AWS Clean Rooms 或 AWS Clean Rooms ML 不支援 VPC 端點原則。預設情況下，允許透過介面端點完整存取 AWS Clean Rooms 和 AWS Clean Rooms ML。或者，您可以將安全群組與端點網路介面相關聯，以透過介面端點控制傳送至 AWS Clean Rooms 或 AWS Clean Rooms ML 的流量。

建立的介面端點 AWS Clean Rooms

您可以使用 Amazon VPC 主控台 AWS Clean Rooms 或 AWS Command Line Interface (AWS CLI) 為或 AWS Clean Rooms ML 建立介面端點。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的建立介面端點。

建立 AWS Clean Rooms 使用下列服務名稱的介面端點。

```
com.amazonaws.region.cleanrooms
```

使用下列服務名稱建立 AWS Clean Rooms ML 的介面端點。

```
com.amazonaws.region.cleanrooms-ml
```

如果您為介面端點啟用私有 DNS，您可以 AWS Clean Rooms 使用其預設的區域 DNS 名稱向 API 要求。例如 `cleanrooms-ml.us-east-1.amazonaws.com`。

監控 AWS Clean Rooms

監控是維持其他 AWS 解決方案的可靠性、可用性和效能的 AWS Clean Rooms 重要組成部分。 AWS 提供下列監控工具來監視 AWS Clean Rooms、在發生錯誤時回報，並在適當時自動採取行動：

- Amazon CloudWatch 日誌可讓您從 Amazon EC2 執行個體和其他來源監控 AWS CloudTrail、存放和存取日誌檔。Amazon CloudWatch Logs 可以監控日誌檔中的資訊，並在符合特定閾值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。

  無塵室 ML 允許跨帳戶工作執行特定 API 動作。啟動 AWS 帳戶 工作的會收到工作的 AWS CloudTrail 稽核記錄事件。如需更多資訊，請參閱適用於 AWS Clean Rooms ML 的 IAM 行為
- AWS CloudTrail擷取由您或代表您發出的 API 呼叫和相關事件， AWS 帳戶 並將日誌檔傳遞到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》。

使用 AWS CloudTrail 記錄 AWS Clean Rooms API 呼叫

AWS Clean Rooms整合了AWS CloudTrail，這是一種提供使用者、角色或AWS 服務中所採取之動作的記錄的服務AWS Clean Rooms。 CloudTrail 會將的所有 API 呼叫擷取AWS Clean Rooms為事件。擷取的呼叫包括從 AWS Clean Rooms 主控台進行的呼叫，以及針對 AWS Clean Rooms API 操作的程式碼呼叫。如果您建立追蹤，就可以將 CloudTrail事件持續交付至 Amazon S3 儲存貯體，包括的事件AWS Clean Rooms。即使未設定追蹤，您依然可以在事件歷史記錄中檢視最新的事件。 CloudTrail 使用由收集的資訊 CloudTrail，您就可以判斷傳送至的請求AWS Clean Rooms、提出請求的 IP 地址、提出請求的對象、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail用者指南。

AWS Clean Rooms中的資訊 CloudTrail

CloudTrail 當您建立帳戶AWS 帳戶時，系統即會在中啟用。此外AWS Clean Rooms，中發生活動時，系統便會將該活動記錄至 CloudTrail 事件，並將其他AWS 服務事件記錄至事件歷史記錄中。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

如需您 AWS 帳戶 帳戶中正在進行事件的記錄 (包含 AWS Clean Rooms 的事件)，請建立追蹤。線索能 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該

追蹤會套用至所有的 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還能設定其他服務，AWS 服務以進一步分析和處理 CloudTrail 日誌中收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定的 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌檔案
- 從多個帳戶接收 CloudTrail 日誌檔案

所有AWS Clean Rooms動作均由「API 參考」記錄 CloudTrail 並記錄在「AWS Clean RoomsAPI 參考」中。

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根使用者或 IAM 使用者憑證提出該請求。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 AWS Clean Rooms 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付至您指定的 Amazon S3 儲存貯體。 CloudTrail 日誌檔案包含一個或多個日誌項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。 CloudTrail 日誌檔案並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

範例AWS Clean Rooms CloudTrail 事件

下列範例會示範個別 CloudTrail 事件：

主題

- StartProtectedQuery (成功)
- StartProtectedQuery(失敗)

StartProtectedQuery (成功)


```
{
    "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(失敗)

```
{
    "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"
}
```

建立 AWS Clean Rooms 資源 AWS CloudFormation

AWS Clean Rooms 與 AWS CloudFormation整合的服務可協助您建立資源模型並設定資 AWS 源。藉由此整合，您可以花更少的時間來建立和管理資源和基礎架構。您可以建立描述您想要的所有 AWS 資源的範本，並為您 AWS CloudFormation 佈建和設定這些資源。資源的範例包括協同合作、已配置的表格、已配置的表格關聯以及成員資格。

使用時 AWS CloudFormation，您可以重複使用範本，以一致且重複地設定 AWS Clean Rooms 資源。描述您的資源一次，然後在多 AWS 帳戶 個和中一遍又一遍地佈建相同的資源 AWS 區域。

AWS Clean Rooms 和 AWS CloudFormation 範本

若要佈建和設定 AWS Clean Rooms 與相關服務的資源，您必須瞭解AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式化的文本檔案。這些範本說明您要在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，可以使用 AWS CloudFormation 設計工具來協助您開始 AWS CloudFormation 使用範本。如需更多詳細資訊，請參閱 AWS CloudFormation 使用者指南 中的 什麼是 AWS CloudFormation 設計器？。

AWS Clean Rooms 支援在中建立協同作業、已配置的表格、已配置的表格關聯和成員資格。 AWS CloudFormation如需詳細資訊，包括用於協同作業的 JSON 和 YAML 範本、已設定的資料表、已設定的資料表關聯和成員資格等範例，請參閱使用者指南中的AWS Clean Rooms 資源類型參考資料。AWS CloudFormation

可使用以下範本：

- 分析範本

  指定 AWS Clean Rooms 分析範本，包括名稱、描述、格式、來源、參數和標籤。

  如需詳細資訊，請參閱下列主題：

  AWS::CleanRooms::AnalysisTemplate《AWS Clean Rooms 使用者指南》中的

  AWS Clean Rooms API 參考中的 CreateAnalysisTemplate
- 協作

  指定 AWS Clean Rooms 協同合作，包括名稱、描述、類型、參數和標籤。

  如需詳細資訊，請參閱下列主題：

AWS::CleanRooms::Collaboration《AWS CloudFormation 使用者指南》中的

AWS Clean Rooms API 參考中的 CreateCollaboration

- 配置的表

  在中指定已設定的表格 AWS Clean Rooms，包括允許的欄、分析方法、說明、名稱、資料表參考、隱私權預算和標籤。已配置的表格代表中已配置為在中 AWS Glue Data Catalog 使用的現有表格的參考 AWS Clean Rooms。已配置的表格包含決定如何使用資料的分析規則。

  如需詳細資訊，請參閱下列主題：

  AWS::CleanRooms::ConfiguredTable《AWS CloudFormation 使用者指南》中的

  AWS Clean Rooms API 參考中的 CreateConfiguredTable

- 配置的表格關聯

  在中指定已設定的表格關聯 AWS Clean Rooms，包括 ID、說明、成員 ID、名稱、角色、Amazon 資源名稱 (ARN) 和標籤。已配置的表格關聯會將已配置的表格與協同合作連結。

  如需詳細資訊，請參閱下列主題：

  AWS::CleanRooms::ConfiguredTableAssociation《AWS CloudFormation 使用者指南》中的

  AWS Clean Rooms API 參考中的 CreateConfiguredTableAssociation

- 會員

  指定特定協同作業識別碼的成員資格，並加入中的共同作業 AWS Clean Rooms。

  如需詳細資訊，請參閱下列主題：

  AWS::CleanRooms::Membership《AWS CloudFormation 使用者指南》中的

  AWS Clean Rooms API 參考中的 CreateMembership

- 隱私預算範本

  指定 AWS Clean Rooms 隱私權預算範本，包括隱私權預算、每次查詢新增的雜訊，以及每月隱私權預算重新整理。

  如需詳細資訊，請參閱下列主題：

AWS::CleanRooms::PrivacyBudgetTemplate《AWS CloudFormation 使用者指南》中的

AWS Clean Rooms API 參考中的 CreatePrivacyBudgetTemplate

- 建立訓練資料集

  從資料 AWS Glue 表指定「潔淨室」ML 模型的訓練資料集。

  如需詳細資訊，請參閱下列主題：

  AWS::CleanRoomsML::TrainingDataset《AWS CloudFormation 使用者指南》中的

  CreateTrainingDataset潔淨室 ML API 參考

進一步了解 AWS CloudFormation

若要進一步了解 AWS CloudFormation，請參閱下列資源：

- AWS CloudFormation
- AWS CloudFormation 使用者指南
- AWS CloudFormation API 參考
- AWS CloudFormation 命令列介面使用者指南

的配額 AWS Clean Rooms

您的每個配額都 AWS 帳戶 有預設配額 (先前稱為限制) AWS 服務。除非另有說明，否則每個配額都特定於 AWS 區域. 您可以要求增加某些配額，而其他配額則無法增加。

若要檢視的配額 AWS Clean Rooms，請開啟「Service Quotas」主控台。在導覽窗格中，選擇 AWS 服務並選取AWS Clean Rooms。

若要請求提升配額，請參閱《Service Quotas 使用者指南》中的請求提升配額。如果「Service Quotas」中尚未提供配額，請使用「服務限制提高」表單。

您 AWS 帳戶 有下列相關配額 AWS Clean Rooms。

資源	預設	描述
每次合作邀請的成員	5	每次協同合作邀請的成員人數上限
每個帳戶的會員資格	100	一個帳戶的會員資格數目上限
每個帳戶建立的共同作業	10	每個帳戶建立的最大共同作業次數
每個帳戶設定的表格	60	帳戶可建立的已設定資料表數目上限
每個成員資格表關聯	25	每個有效成員資格的關聯表格數目上限
每個成員資格並行進行中	5	每個成員資格同時進行查詢的最大數量
每個已設定表格允許清單的欄	100	每個已設定的資料表可允許列出的最大資料欄數
每個受保護的查詢已設定	15	受保護查詢中已設定資料表的數目上限

資源	預設	描述
每個會籍的分析範本	25	每個成員資格的最大分析範本數
針對每個成員資格設定相似模型 (對象模型) 關聯	5	每個成員資格設定的相似模型關聯數目上限。

資源參數限制

資源	預設	描述
分析規則大小	100 KB	分析規則的 JSON 大小上限
查詢文字長度	90 KB (針對差異隱私權查詢為 8 KB)	SQL 查詢陳述式的最大文字長度
查詢執行時間	12 小時	在逾時前執行查詢的持續時間上限
查詢資料檔案輸出大小	6.2 GB	受保護查詢的輸出檔案大小上限

每個帳戶的每個端點配額 AWS 帳戶 有以下每秒 API 交易 (TPS)。

API 限流配額

資源	速率限制	描述
`BatchGetCollaborationAnalysisTemplate` 要求率	5 TPS	每秒最大 `BatchGetCollaborationAnalysisTemplate` API 呼叫數
`BatchGetSchema` 要求率	5 TPS	每秒最大 `BatchGetSchema` API 呼叫數

資源	速率限制	描述
CreateAnalysisTemplate 要求率	5 TPS	每秒最大 CreateAnalysisTemplate API 呼叫數
CreateCollaboration 要求率	5 TPS	每秒最大 CreateCollaboration API 呼叫數
CreateConfiguredAudienceModelAssociation 要求率	5 TPS	每秒的 CreateConfiguredAudienceModelAssociation 呼叫次數上限
CreateConfiguredTable 要求率	5 TPS	每秒的 CreateConfiguredTable 呼叫次數上限
CreateConfiguredTableAnalysisRule 要求率	5 TPS	每秒的 CreateConfiguredTableAnalysisRule 呼叫次數上限
CreateConfiguredTableAssociation 要求率	5 TPS	每秒的 CreateConfiguredTableAssociation 呼叫次數上限
CreateMembership 要求率	5 TPS	每秒的 CreateMembership 呼叫次數上限
CreatePrivacyBudgetTempate 要求率	5 TPS	每秒的 CreatePrivacyBudgetTemplate 呼叫次數上限
DeleteAnalysisTemplate 要求率	5 TPS	每秒的 DeleteAnalysisTemplate 呼叫次數上限
DeleteCollaboration 要求率	5 TPS	每秒的 DeleteCollaboration 呼叫次數上限

資源	速率限制	描述
DeleteConfiguredAudienceModelAssociation 要求率	5 TPS	每秒的 DeleteConfiguredAudienceModelAssociation 呼叫次數上限
DeleteConfiguredTable 要求率	5 TPS	每秒的 DeleteConfiguredTable 呼叫次數上限
DeleteConfiguredTableAnalysisRule 要求率	5 TPS	每秒的 DeleteConfiguredTableAnalysisRule 呼叫次數上限
DeleteConfiguredTableAssociation 要求率	5 TPS	每秒的 DeleteConfiguredTableAssociation 呼叫次數上限
DeleteMember 要求率	5 TPS	每秒的 DeleteMember 呼叫次數上限
DeleteMembership 要求率	5 TPS	每秒的 DeleteMembership 呼叫次數上限
DeletePrivacyBudgetTemplate 要求率	5 TPS	每秒的 DeletePrivacyBudgetTemplate 呼叫次數上限
GetAnalysisTemplate 要求率	5 TPS	每秒的 GetAnalysisTemplate 呼叫次數上限
GetCollaboration 要求率	5 TPS	每秒的 GetCollaboration 呼叫次數上限
GetCollaborationConfiguredAudienceModelAssociation 要求率	5 TPS	每秒的 GetCollaborationConfiguredAudienceModelAssociation 呼叫次數上限

資源	速率限制	描述
GetCollaborationPrivacyBudgetTemplate 要求率	5 TPS	每秒的 GetCollaborationPrivacyBudgetTemplate 呼叫次數上限
GetConfiguredAudienceModelAssociation 要求率	5 TPS	每秒的 GetConfiguredAudienceModelAssociation 呼叫次數上限
GetConfiguredTable 要求率	5 TPS	每秒的 GetConfiguredTable 呼叫次數上限
GetConfiguredTableAnalysisRule 要求率	5 TPS	每秒的 GetConfiguredTableAnalysisRule 呼叫次數上限
GetConfiguredTableAssociation 要求率	20 TPS	每秒的 GetConfiguredTableAssociation 呼叫次數上限
GetMembership 要求率	5 TPS	每秒的 GetMembership 呼叫次數上限
GetPrivacyBudgetTemplate 要求率	5 TPS	每秒的 GetPrivacyBudgetTemplate 呼叫次數上限
GetProtectedQuery 要求率	20 TPS	每秒的 GetProtectedQuery 呼叫次數上限
GetSchema 要求率	5 TPS	每秒的 GetSchema 呼叫次數上限
GetSchemaAnalysisRule 要求率	5 TPS	每秒的 GetSchemaAnalysisRule 呼叫次數上限

資源	速率限制	描述
ListAnalysisTemplates 要求率	5 TPS	每秒的 ListAnalysisTemplates 呼叫次數上限
ListCollaborationConfiguredAudienceModelAssociations 要求率	5 TPS	每秒的 ListCollaborationConfiguredAudienceModelAssociations 呼叫次數上限
ListCollaborationPrivacyBudgets 要求率	5 TPS	每秒的 ListCollaborationPrivacyBudgets 呼叫次數上限
ListCollaborationPrivacyBudgetTemplates 要求率	5 TPS	每秒的 ListCollaborationPrivacyBudgetTemplates 呼叫次數上限
ListCollaborations 要求率	5 TPS	每秒的 ListCollaborations 呼叫次數上限
ListConfiguredAudienceModelAssociations 要求率	5 TPS	每秒的 ListConfiguredAudienceModelAssociations 呼叫次數上限
ListConfiguredTableAssociations 要求率	5 TPS	每秒的 ListConfiguredTableAssociations 呼叫次數上限
ListConfiguredTables 要求率	5 TPS	每秒的 ListConfiguredTables 呼叫次數上限
ListMembers 要求率	5 TPS	每秒的 ListMembers 呼叫次數上限

資源	速率限制	描述
ListMemberships 要求率	5 TPS	每秒的 ListMemberships 呼叫次數上限
ListPrivacyBudgets 要求率	5 TPS	每秒的 ListPrivacyBudgets 呼叫次數上限
ListPrivacyBudgetTemplates 要求率	5 TPS	每秒的 ListPrivacyBudgetTemplates 呼叫次數上限
ListProtectedQueries 要求率	5 TPS	每秒的 ListProtectedQueries 呼叫次數上限
ListSchemas 要求率	5 TPS	每秒的 ListSchemas 呼叫次數上限
StartProtectedQuery 要求率	5 TPS	每秒的 StartProtectedQuery 呼叫次數上限
UpdateAnalysisTemplate 要求率	5 TPS	每秒的 UpdateAnalysisTemplate 呼叫次數上限
UpdateCollaboration 要求率	5 TPS	每秒的 UpdateCollaboration 呼叫次數上限
UpdateConfiguredAudienceModelAssociation 要求率	5 TPS	每秒的 UpdateConfiguredAudienceModelAssociation 呼叫次數上限
UpdateConfiguredTable 要求率	5 TPS	每秒的 UpdateConfiguredTable 呼叫次數上限

資源	速率限制	描述
UpdateConfiguredTableAnalysisRule 要求率	5 TPS	每秒的 UpdateConfiguredTableAnalysisRule 呼叫次數上限
UpdateConfiguredTableAssociation 要求率	5 TPS	每秒的 UpdateConfiguredTableAssociation 呼叫次數上限
UpdatePrivacyBudgetTemplate 要求率	5 TPS	每秒的 UpdatePrivacyBudgetTemplate 呼叫次數上限

AWS Clean Rooms ML API 節流配額

資源	速率限制	描述
CreateAudienceModel 要求率	1 TPS 速率，3 TPS 爆發	每秒最大 CreateAudienceModel API 呼叫數
CreateConfiguredAudienceModel 要求率	10 TPS	每秒最大 CreateConfiguredAudienceModel API 呼叫數
CreateTrainingDataset 要求率	10 TPS	每秒最大 CreateTrainingDataset API 呼叫數
DeleteAudienceGenerationJob 要求率	2 個 TPS 速率，10 TPS 爆發	每秒最大 DeleteAudienceGenerationJob API 呼叫數
DeleteAudienceModel 要求率	2 個 TPS 速率，10 TPS 爆發	每秒最大 DeleteAudienceModel API 呼叫數
DeleteConfiguredAudienceModel 要求率	10 TPS	每秒最大 DeleteConfiguredAudienceModel API 呼叫數

資源	速率限制	描述
DeleteConfiguredAudienceModelPolicy 要求率	25 TPS	每秒最大 DeleteConfiguredAudienceModelPolicy API 呼叫數
DeleteTrainingDataset 要求率	10 TPS	每秒最大 DeleteTrainingDataset API 呼叫數
GetAudienceGenerationJob 要求率	50 TPS	每秒最大 GetAudienceGenerationJob API 呼叫數
GetAudienceModel 要求率	50 TPS	每秒最大 GetAudienceModel API 呼叫數
GetConfiguredAudienceModel 要求率	50 TPS	每秒最大 GetConfiguredAudienceModel API 呼叫數
GetConfiguredAudienceModelPolicy 要求率	50 TPS	每秒最大 GetConfiguredAudienceModelPolicy API 呼叫數
GetTrainingDataset 要求率	50 TPS	每秒最大 GetTrainingDataset API 呼叫數
ListAudienceExportJobs 要求率	50 TPS	每秒最大 ListAudienceExportJobs API 呼叫數
ListAudienceGenerationJobs 要求率	50 TPS	每秒最大 ListAudienceGenerationJobs API 呼叫數
ListAudienceModels 要求率	50 TPS	每秒最大 ListAudienceModels API 呼叫數

資源	速率限制	描述
ListConfiguredAudienceModels 要求率	50 TPS	每秒最大 ListConfiguredAudienceModels API 呼叫數
ListTagsForResource 要求率	50 TPS	每秒最大 ListTagsForResource API 呼叫數
ListTrainingDatasets 要求率	50 TPS	每秒最大 ListTrainingDatasets API 呼叫數
PutConfiguredAudienceModelPolicy 要求率	25 TPS	每秒最大 PutConfiguredAudienceModelPolicy API 呼叫數
StartAudienceExportJob 要求率	1 TPS 速率，3 TPS 爆發	每秒最大 StartAudienceExportJob API 呼叫數
StartAudienceGenerationJob 要求率	1 TPS 速率，5 TPS 爆發	每秒最大 StartAudienceGenerationJob API 呼叫數
TagResource 要求率	10 TPS	每秒最大 TagResource API 呼叫數
UntagResource 要求率	50 TPS	每秒最大 UntagResource API 呼叫數
UpdateConfiguredAudienceModel 要求率	10 TPS	每秒最大 UpdateConfiguredAudienceModel API 呼叫數

名稱	預設	可調整	描述
每個受眾產生工作的活躍受眾匯出工作	每個受支援的區域：25	否	對象產生工作的作用中對象匯出工作數目上限
待中/進行中觀眾導出每個客戶的工作數量	每個受支援的區域：20	否	每個客戶的待置/進行中觀眾匯出工作的最大數量
每位客戶的待中/進行中受眾產生工作	每個受支援的區域：10	是	每個客戶的待置/進行中聽眾產成工作的最大數量
每個客戶的待中/進行中受眾模型	每個支持地區：2	是	每個客戶的待中/進行中受眾模型培訓工作的最大數量

潔淨室 ML 配額

資源	預設	描述
資料集	每個工作	
最大互動次數	二千億	訓練資料允許的最大互動次數。較大的輸入會向下取樣。
最小互動次數	100 萬	
相似模型訓練的不同使用者人數上限	100 萬	如果包含更多內容，則僅使用前 1 億名，按互動次數排名。
相似模型訓練的不同使用者人數下限	100,000	
匯出相似區段 (對象) 工作的使用者人數上限	10,000	

資源	預設	描述
用於模型訓練的不同項目數目上限。	100 萬	您最多可以包含 5000 萬個項目，但僅使用最受歡迎的 100 萬個項目。
訓練資料集中功能欄的最大數目。	10	
每位使用者的不同項目數下限	2	AWS Clean Rooms ML 要求每個資料列或使用者都有兩個或多個項目，包括重複的項目。
種子觀眾的最大尺寸	500,000	
種子受眾的最小規模	500	訓練資料提供者可將此值設定為低至 25。
API	每位客戶	
作用中訓練資料集總數	500	
作用中相似模型總數（受眾模型）	500	
作用中設定的相似模型總數 (受眾模型)	10,000	
已完成的相似區段 (對象) 產生工作總數	沒有限制	
已完成匯出相似區段 (對象) 工作總數	沒有限制	
相似模型 (受眾模型) 產生工作的最長持續時間	一天（24 小時）	
相似區段 (對象) 產生工作的最長持續時間	10 小時	提供種子後，潔淨室 ML 最多需要 10 小時才能產生相似的區段。

資源	預設	描述
區段 (對象) 大小資料桶的最小百分比	1%	
區段 (對象) 大小資料桶的最大百分比	20%	
區段 (對象) 大小資料桶的最小絕對大小	不同使用者數量的 1%	
區段 (對象) 大小資料桶的最大絕對大小	不同使用者數量的 20%	

AWS Clean Rooms 使用者指南的文件歷史記錄

下表說明的文件發行版本 AWS Clean Rooms。

如需有關此文件更新的通知，您可以訂閱 RSS 摘要。若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

變更	描述	日期
更新至現有政策	下列新權限已新增至受AWSCleanRoomsFullAccessNoQuerying 管理的策略：cleanrooms:BatchGetSchemaAnalysisRule	2024年5月13日
AWS Clean Rooms ML 現已完全可用	AWS Clean Rooms ML 為雙方提供了一種增強隱私的方法，以識別其數據中的相似用戶，而無需彼此共享數據。	2024年4月3日
更新至現有政策	AWSCleanRoomsFullAccess 受管理策略中的聲明 ID 已從更新ConsolePickQueryResultsBucket為更好地表示自權限SetQueryResultsBucket以來的權限。	2024年3月21日
適用於 AWS Clean Rooms ML 的新受管原則	已新增兩個新的受管理策略：AWSCleanRoomsMLReadOnlyAccess 和AWSCleanRoomsMLFullAccess 。	2023 年 11 月 29 日
AWS Clean Rooms 毫升 (預覽)	AWS Clean Rooms ML 為雙方提供了一種增強隱私的方法，	2023 年 11 月 29 日

	以識別其數據中的相似用戶，而無需彼此共享數據。	
AWS Clean Rooms 微分隱私（預覽）	客戶現在可以使用 AWS Clean Rooms 差分隱私來幫助保護其用戶的隱私。	2023 年 11 月 29 日
付款配置	共同作業建立者現在可以設定可以執行查詢的成員，或是在協同作業中設定不同的成員，以支付查詢運算成本的費用。	2023 年 11 月 14 日
查詢執行時間-更新	在逾時之前執行查詢的最長持續時間從 4 小時更新為 12 小時。	2023 年 10 月 6 日
AWS CloudFormation 資源-更新	AWS Clean Rooms 已新增下列新資源：`AWS::CleanRooms::Membership` `ProtectedQueryOutputConfiguration` `AWS::CleanRooms::MembershipProtectedQueryResultConfiguration` 、和`AWS::CleanRooms::Membership` `ProtectedQueryS3OutputConfiguration` 。	2023 年 9 月 7 日
AWS CloudFormation 資源-更新	AWS Clean Rooms 已新增下列新資源：`AWS::CleanRooms::AnalysisTemplate` 和`AWS::CleanRooms::ConfiguredTable AnalysisRuleCustom` 。	2023 年 8 月 31 日

單獨的會員能力	協同合作建立者現在可以指定一個成員為可以查詢的成員，另一個成員指定為可以接收結果的成員。這可讓協同合作建立者確定可以查詢的成員無法存取查詢結果。	2023 年 8 月 30 日
AWS Clean Rooms 詞彙表	僅限文件更新，可新增術語詞彙表。 AWS Clean Rooms	2023 年 8 月 30 日
Support Apache Iceberg 表格 (預覽)	AWS Clean Rooms 現在支援 Apache Iceberg表格 (預覽)。	2023 年 8 月 25 日
配額更新	「配額」區段已更新，以反映每個帳戶成員資格的新預設配額。	2023 年 8 月 9 日

更新至現有政策	下列新權限已新增至受AWSCleanRoomsFullAccessNoQuerying 管理的策略：cleanrooms:CreateAnalysisTemplate cleanrooms:GetAnalysisTemplate 、cleanrooms:UpdateAnalysisTemplate 、 cleanrooms:DeleteAnalysisTemplate 、cleanrooms:ListAnalysisTemplates 、cleanrooms:GetCollaborationAnalysisTemplate 、、cleanrooms:BatchGetCollaborationAnalysisTemplate 、和 cleanrooms:ListCollaborationAnalysisTemplates 。	2023 年 7 月 31 日
分析範本和自訂分析規則	AWS Clean Rooms 現在支援分析範本和自訂分析規則。分析範本可讓協同合作者建立或匯入自己的自訂 SQL 查詢，以便在協同作業中使用。透過自訂分析規則，資料表擁有者可以核准其已設定資料表上的自訂 SQL 查詢。	2023 年 7 月 31 日
分析規則支援OR邏輯條件	AWS Clean Rooms 分析規則現在支援JOIN子句中的OR邏輯條件。	2023 年 6 月 29 日

CloudFormation 整合	AWS Clean Rooms 現在與 AWS CloudFormation.	2023 年 6 月 15 日
分析建置器	可以查詢和接收結果的成員現在可以在某些資料表上執行查詢，而不需要使用 Analysis 建置器 UI 撰寫 SQL 程式碼。	2023 年 6 月 15 日
SQL 函數	僅限文件更新，以闡明支援的 SQL 函式。	2023 年 5 月 5 日
疑難排解	僅限文件更新，可新增常見問題的疑難排解區段。	2023 年 4 月 27 日
支援的資料類型 AWS Clean Rooms	僅限文件更新，以新增列出支援 AWS Glue Data Catalog 資料類型的新區段。	2023年4月26日
AWS CloudTrail 事件的例子	僅文檔更新，以添加 CloudTrail 事件的例子StartProtectedQuery（成功）和StartProtectedQuery（失敗）。	2023 年 4 月 20 日
更新至現有政策	下列新權限已新增至受`AWSCleanRoomsFullAccessNoQuerying` 管理的策略：`cleanrooms:ListTagsForResource` `cleanrooms:UntagResource` 、和`cleanrooms:TagResource` 。如需詳細資訊，請參閱AWS 受管理的策略。	2023 年 3 月 21 日
一般可用性	AWS Clean Rooms 現已正式推出。	2023 年 3 月 21 日

預覽版本	AWS Clean Rooms 使用者指南的預覽版	2023 年 1 月 12 日

AWS Clean Rooms 詞彙表

請參閱此詞彙表，以熟悉用於的術語 AWS Clean Rooms。

彙總分析規則

允許使用COUNT、SUM或AVG函數沿選用維度彙總分析的查詢限制。這些查詢不會顯示列層級資訊。

支援宣傳活動規劃、媒體觸及率、頻率和轉換測量等使用案例。

其他類型的分析規則是自訂和清單。

分析規則

授權特定查詢類型的查詢限制。

分析規則類型決定了可以在配置的表格上執行哪種分析類型。每種類型都有預先定義的查詢結構。您可以透過查詢控制項，控制如何在結構中使用資料表資料行。

分析規則的類型包括彙總、清單和自訂。

分析範本

可重複使用的共同作業特定、預先核准的查詢。

支援中支援的自訂 SQL 查詢 AWS Clean Rooms。

可以在常值通常出現在 SQL 查詢中的任何位置包含參數。如需有關支援參數類型的詳細資訊，請參閱 AWS Clean Rooms SQL 參考中的資料類型。

分析範本僅適用於自訂分析規則。

C3R 加密客戶端

Clean Rooms(C3R) 加密用戶端的密碼編譯運算。

C3R 用於加密和解密數據，是帶有命令行界面的客戶端加密 SDK。

明文字欄

未針對JOIN或 SELECT SQL 建構進行密碼編譯保護的資料行。

純文字資料行可用於 SQL 查詢的任何部分。

協作

一種安全的邏輯界限，成員可 AWS Clean Rooms 在其中對已設定的資料表執行 SQL 查詢。

協同合作是由協同合作建立者所建立。

只有受邀加入協同合作的成員才能加入協同合作。

一個共同作業只能有一個可以查詢資料的成員、一位可以接收結果的成員，以及一位成員支付查詢運算費用。

所有成員在加入協同合作之前，都可以查看共同作業中的受邀參與者清單。

協作建立者

建立協同作業的成員。

每個協同作業只有一位共同作業建立者。

只有協同合作建立者可以從協同合作中移除成員或刪除協同合作。

配置表

每個已配置的表格都代表中已配置為在中 AWS Glue Data Catalog 使用的現有表格的參照 AWS Clean Rooms。已配置的表格包含決定如何使用資料的分析規則。

目前， AWS Clean Rooms 支援將存放在 Amazon 簡單儲存服務 (Amazon S3) 中的資料建立關聯，並透過編目。 AWS Glue

如需詳細資訊 AWS Glue，請參閱AWS Glue 開發人員指南。

已配置的表格可以與一或多個協同作業相關聯。

> **Note**
>
> AWS Clean Rooms 目前不支援在註冊的 Amazon S3 儲存貯體位置 AWS Lake Formation。

自訂分析規則

一種查詢限制，允許一組特定的預先核准查詢 (分析範本)，或允許可提供使用您資料之查詢的特定帳戶集。

支援首次接觸歸因、增量分析和受眾探索分析等使用案例。

支持差分隱私。

解密

將加密資料轉換回原始格式的程序。只有在您有權存取密鑰時才能執行解密。

微分隱私

一種數學上嚴格的技術，可以保護協作數據免受能夠獲得有關特定個人的結果的成員的侵害。

加密

將數據編碼為使用稱為密鑰的秘密值隨機顯示的形式的過程。如果不訪問密鑰，則不可能確定原始明文。

指紋專欄

針對 JOIN SQL 建構受密碼編譯保護的資料行。

清單分析規則

此查詢限制可讓查詢輸出此資料表與可查詢之成員資料表之重疊的資料列層級屬性分析。

支援豐富和受眾建立或抑制等使用案例。

成員

身為協同作業參與者的 AWS 客戶。

使用成員來識別成員 AWS 帳戶。

所有成員都可以貢獻數據。

可以查詢的會員

可以在協同作業中查詢資料的成員。

每個協同作業只有一個成員可以查詢，而且該成員是不可變的。

管理使用者可以使用 AWS Identity and Access Management (IAM) 許可來控制哪些 IAM 主體 (例如使用者或角色) 可以在協同作業中查詢資料。如需詳細資訊，請參閱 建立服務角色以讀取資料。

可以獲得結果的會員

可以接收查詢結果的成員。可以接收結果的成員會指定 Amazon S3 目的地的查詢結果設定和查詢結果格式。

每次協同合作只有一個成員可以接收結果，而且該成員不可變。

支付查詢計算費用的會員

負責支付查詢計算費用的成員。

只有一個成員負責支付每次協同作業的查詢運算成本，而且該成員是不可變的。

如果共同作業建立者尚未指定任何人為支付查詢計算費用的成員，則可以查詢的成員就是預設付款人。

支付查詢計算成本的成員會收到已在合作中執行之查詢的帳單。

成員資格

成員加入協同合作時建立的資源。

成員與協同合作關聯的所有資源都是成員資格的一部分，或與成員資格相關聯。

只有擁有成員資格的成員才能新增、移除或編輯該成員資格中的資源。

密封柱

針對 SELECT SQL 建構受密碼編譯保護的資料行。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。