



使用者指南

# AWS Entity Resolution



# AWS Entity Resolution: 使用者指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

什麼是 AWS Entity Resolution ? .....	1
您是第一次 AWS Entity Resolution 使用嗎? .....	1
的功能 AWS Entity Resolution .....	1
相關服務 .....	4
存取 AWS Entity Resolution .....	4
定價 AWS Entity Resolution .....	5
設定 .....	6
註冊 AWS .....	6
建立管理員使用者 .....	6
為主控台使用者建立IAM角色 .....	7
建立工作流程任務角色 .....	8
準備輸入數據表 .....	15
準備第一方輸入資料 .....	15
步驟 1：以支援的資料格式儲存輸入資料表 .....	15
步驟 2：將您的輸入資料表上傳到 Amazon S3 .....	15
步驟 3：建立 AWS Glue table .....	16
準備第三方輸入資料 .....	17
步驟 1：訂閱提供者服務 AWS Data Exchange .....	18
步驟 2：準備第三方資料表 .....	19
步驟 3：以支援的資料格式儲存輸入資料表 .....	21
步驟 4：將您的輸入資料表上傳到 Amazon S3 .....	22
步驟 5：建立 AWS Glue table .....	22
綱要對映 .....	24
建立綱要對應 .....	24
複製綱要對應 .....	32
編輯資料架構對映 .....	32
刪除綱要對應 .....	33
ID 命名空間 .....	34
ID 命名空間來源 .....	34
建立 ID 命名空間來源 (以規則為基礎) .....	35
建立 ID 命名空間來源 (提供者服務) .....	38
ID 命名空間目標 .....	40
建立 ID 命名空間目標 (以規則為基礎的方法) .....	40
建立 ID 命名空間目標 (提供者服務方法) .....	43

編輯 ID 命名空間 .....	44
刪除 ID 命名空間 .....	44
新增或更新 ID 命名空間的資源策略 .....	44
比對工作流程 .....	46
建立規則型比對工作流程 .....	47
建立以機器學習為基礎的比對工作流程 .....	52
建立提供者服務型比對工作流程 .....	56
使用 建立相符的工作流程 LiveRamp .....	56
使用 建立相符的工作流程 TransUnion .....	63
使用 2.0 UID 建立相符的工作流程 .....	69
編輯相符的工作流程 .....	73
刪除相符的工作流程 .....	73
尋找規則型比對工作流程的比對 ID .....	73
從規則型或 ML 型比對工作流程刪除記錄 .....	74
故障診斷 .....	75
我在執行相符的工作流程後收到錯誤檔 .....	75
ID 映射工作流程 .....	77
一個的 ID 映射工作流程 AWS 帳戶 .....	78
必要條件 .....	78
建立 ID 映射工作流程 (規則型) .....	80
建立 ID 映射工作流程 (提供者服務) .....	84
跨兩個的 ID 映射工作流程 AWS 帳戶 .....	89
必要條件 .....	90
建立 ID 映射工作流程 (規則型) .....	91
建立 ID 映射工作流程 (提供者服務) .....	95
執行 ID 映射工作流程 .....	100
使用新的輸出目的地執行 ID 映射工作流程 .....	101
編輯 ID 映射工作流程 .....	103
刪除 ID 映射工作流程 .....	104
新增或更新 ID 映射工作流程的資源政策 .....	104
供應商整合 .....	105
要求 .....	105
列出提供者服務 AWS Data Exchange .....	105
識別您的屬性 .....	106
請求 AWS Entity Resolution 開放API規格 .....	107
使用「開啟」API 規格 .....	107

Batch 處理整合 .....	108
同步處理整合 .....	110
測試提供者整合 .....	111
安全性 .....	119
資料保護 .....	119
靜態資料加密 AWS Entity Resolution .....	120
金鑰管理 .....	121
AWS PrivateLink .....	130
身分與存取管理 .....	132
物件 .....	132
使用身分驗證 .....	133
使用政策管理存取權 .....	135
AWS Entity Resolution 如何使用 IAM .....	137
身分型政策範例 .....	143
AWS 受管理政策 .....	145
故障診斷 .....	150
法規遵循驗證 .....	152
AWS Entity Resolution 合規性最佳做法 .....	153
恢復能力 .....	153
監控 .....	154
CloudTrail 日誌 .....	154
AWS Entity Resolution 中的資訊 CloudTrail .....	154
瞭解 AWS Entity Resolution 記錄檔項目 .....	155
AWS CloudFormation 資源 .....	156
AWS實體解析度和 AWS CloudFormation 範本 .....	156
進一步了解 AWS CloudFormation .....	158
配額 .....	159
文件歷史紀錄 .....	165
詞彙表 .....	168
Amazon Resource Name ( ARN ) .....	168
自動處理 .....	168
AWS KMS key ARN .....	168
Cleartext .....	168
可信度層級 ( ConfidenceLevel ) .....	168
解密 .....	168
加密 .....	169

Group name (群組名稱) .....	169
雜湊 .....	169
雜湊通訊協定 ( HashingProtocol ) .....	169
ID 映射方法 .....	169
ID 映射工作流程 .....	170
ID 命名空間 .....	170
輸入欄位 .....	170
輸入來源 ARN ( InputSourceARN ) .....	170
輸入類型 .....	170
機器學習型比對 .....	171
手動處理 .....	171
Many-to-Many 比對 .....	171
比對 ID MatchID ) .....	171
比對金鑰 ( MatchKey ) .....	171
比對金鑰名稱 .....	172
比對規則 ( MatchRule ) .....	172
相符 .....	172
比對工作流程 .....	172
比對工作流程描述 .....	172
比對工作流程名稱 .....	172
比對工作流程中繼資料 .....	173
標準化 ( ApplyNormalization ) .....	173
名稱 .....	173
電子郵件 .....	174
Phone .....	174
Address .....	174
雜湊 .....	177
Source_ID .....	177
標準化 ( ApplyNormalization ) – 僅限 ML .....	177
名稱 .....	177
電子郵件 .....	177
Phone .....	178
One-to-One 比對 .....	178
輸出 .....	178
OutputS3Path .....	179
OutputSourceConfig .....	179

---

提供者服務型比對 .....	179
規則型比對 .....	179
結構描述 .....	180
結構描述描述 .....	180
結構描述名稱 .....	180
結構描述映射 .....	180
結構描述映射 ARN .....	180
唯一 ID .....	180
.....	clxxxii

# 什麼是 AWS Entity Resolution ？

AWS Entity Resolution 是一項服務，可協助您比對、連結和增強跨多個應用程式、通道和資料存放區儲存的相關記錄。您可以開始使用實體解決方案工作流程，這些工作流程既彈性又可擴充，而且可以連線到現有的應用程式和資料服務提供

AWS Entity Resolution 提供先進的匹配技術，例如基於規則的匹配，基於機器學習的匹配 ( ML 匹配 ) 以及數據服務提供商主導的匹配。這些技術可協助您更準確地連結並加強客戶資訊、產品代碼或業務資料代碼的相關記錄。

您可以用 AWS Entity Resolution 來建立客戶互動的統一檢視，方法是將最近的事件 (例如廣告點擊、購物車放棄和購買) 與來自資料服務提供者的匿名訊號連結至唯一的實體 ID。您還可以更好地跟踪在各個商店中使用不同代碼的產品 (例如SKU，UPC)。您可以用 AWS Entity Resolution 來控制匹配準確性並更好地保護數據安全性，同時將數據移動降到最低

## 主題

- [您是第一次 AWS Entity Resolution 使用嗎？](#)
- [的功能 AWS Entity Resolution](#)
- [相關服務](#)
- [存取 AWS Entity Resolution](#)
- [定價 AWS Entity Resolution](#)

## 您是第一次 AWS Entity Resolution 使用嗎？

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

- [的功能 AWS Entity Resolution](#)
- [存取 AWS Entity Resolution](#)
- [設定 AWS Entity Resolution](#)

## 的功能 AWS Entity Resolution

AWS Entity Resolution 包括以下功能：

- 靈活且可自訂的資料準備

AWS Entity Resolution 讀取您的數據，AWS Glue 用作匹配處理的輸入。您最多可以指定 20 個資料輸入。AWS Entity Resolution 將資料輸入表格的每一列作為記錄處理，並以唯一的實體做為主索引鍵。AWS Entity Resolution 可以對加密數據集進行操作。首先定義結構描述對應，AWS Entity Resolution 以瞭解您要在相符工作流程中使用哪些輸入欄位。您可以從現有資料輸入中使用自己的 AWS Glue 資料結構描述或藍圖。或者，您可以使用互動式使用者介面或 JSON 編輯器來建立自訂資料架構。依預設，AWS Entity Resolution 也會在比對之前將資料輸入標準化，以改善比對處理，例如移除特殊字元和多餘空格，以及將文字格式化為小寫。如果您的數據輸入已經標準化，則可以關閉規範化。我們還提供了一個 [GitHub 庫](#)，您可以使用它來進一步自定義數據標準化過程以滿足您的需求。

- 可設定的實體比對工

實體比對工作流程是您設定的一系列步驟，用來指示 AWS Entity Resolution 如何比對資料輸入，以及在何處寫入合併資料輸出。您可以設定一或多個相符的工作流程，以比較不同的資料輸入，並使用不同的比對技巧，例如規則式比對、機器學習比對或資料服務提供者主導的比對，而不需要實體解析或 ML 經驗。您也可以檢視現有相符工作流程和指標的工作狀態，例如資源編號、已處理的記錄數，以及找到的相符項目數。

- Ready-to-use 規則式比對

此比對技術包括 AWS Management Console or AWS Command Line Interface (AWS CLI) 中的一組 ready-to-use 規則。您可以使用這些規則，根據您的輸入欄位尋找相關記錄。您也可以透過新增或移除每個規則的輸入欄位、刪除規則、重新排列規則優先順序以及建立新規則來自訂規則。您也可以重設規則，使其返回原始組態。Amazon Simple Storage Service (Amazon S3) 貯體中的資料輸出具有使用規則型比對技術 AWS Entity Resolution 產生的比對群組。每個比對群組都有用來產生與其相關聯的相符項目的規則編號，以協助您瞭解相符項目。例如，規則編號可以展示每個相符群組的精確度，以便規則一比規則二更精確。

- 預先設定的機器學習型比對 (ML 比對)

此比對技術包括預先設定的 ML 模型，可在所有資料輸入中尋找相符項目，尤其是以消費者為基礎的記錄。該模型使用與姓名，電子郵件地址，電話號碼，地址和出生數據類型的日期相關聯的所有輸入字段。該模型生成相關記錄的匹配組，每個組中具有可信度分數，解釋相對於其他匹配組的匹配質量。模型會考慮遺失的輸入欄位，並一起分析整個記錄以代表實體。Amazon S3 儲存貯體中的資料輸出具有使用 ML 比對 AWS Entity Resolution 產生的匹配群組。這是每個比對群組的關聯置信度分數 0.0—1.0，表示相符項目的精確度。

- 與資料服務供應商配對記錄

AWS Entity Resolution 您可以與領先的資料服務供應商和授權資料集進行比對、連結和增強您的記錄，以擴大瞭解、觸及及服務客戶的能力。例如，您可以在資料中附加屬性以增強記錄，或者改善您使用的系統和平台的互通性，以符合業務目標。您只需按幾下滑鼠即可使用此相符工作流程，無需建立和維護複雜的專有整合。您必須與這些資料服務提供者簽訂授權合約，才能利用此比對技術。

- 手動批量處理和自動增量處理

您可以使用資料處理來協助您將資料輸入或輸入轉換為具有類似記錄的合併資料輸出表格，這些記錄具有使用實體比對工作流程組態產生的共同比對 ID。使用 API 和 AWS Management Console 或 AWS CLI，您可以根據現有的擷取、轉換和 load (ETL) 資料管線，根據需要執行[手動大量處理](#)，這些管道會重新處理任何新相符項目的所有資料，以及對現有相符項目的更新進行重新處理。此外，對於以規則為基礎的比對案例，您可以啟[動自動增量處理](#)，以便一旦 Amazon S3 儲存貯體中有新資料可用，服務就會讀取這些新記錄，並將它們與現有記錄進行比較。這可讓您的配對隨著 Amazon S3 資料的任何變更保持最新狀態。

- 近乎即時的查詢

透過[AWS Entity Resolution GetMatchId API 作業查詢](#)任何實體欄位可協助您同步擷取現有的符合 ID。您可以 AWS Entity Resolution 使用個人身份信息調用 (PII) 通過不同的來源和渠道獲取的屬性。AWS Entity Resolution 雜湊這些屬性以進行資料保護，並擷取對應的比對 ID 以連結和比對客戶。例如，您可以使用相關聯的名稱，電子郵件和郵寄地址進行網絡註冊。使用此 AWS Entity Resolution GetMatchId API 操作來查看存放在 S3 儲存貯體的相符結果中是否已存在此客戶或實體，以及與其相關聯的對應實體匹配 ID。取得實體比對 ID 後，您可以在來源應用程式 (例如客戶關係管理 (CRM) 或客戶資料平台 (CDP) 系統中找到與其相關聯的交易資訊。

- 依設計進行資料保護與區域化

AWS Entity Resolution 提供預設加密功能，可協助您保護資料，並為每次輸入到服務的資料配備加密金鑰。例如，您可以靈活地 AWS Entity Resolution 使用伺服器端加密和雜湊資料，以執行以規則為基礎的比對工作流程。AWS Entity Resolution 支持區域化，這意味著您的匹配工作流程運行以 AWS 區域 從您使用服務的位置處理數據。您也可以 Amazon S3 中加密和雜湊資料，然後再將已解析的資料用於其他應用程式。

- 多方轉碼

AWS Entity Resolution 可協助您定義資料來源，並在想要使用資料協同作業的多方之間進行比對設定，例如中 AWS Clean Rooms。

## 相關服務

以下 AWS 服務 是與之相關的 AWS Entity Resolution：

- Amazon Simple Storage Service (Amazon S3)

將您帶入的資料存放 AWS Entity Resolution 在 Amazon S3 中。

如需詳細資訊，請參閱[什麼是 Amazon S3？](#) 在 Amazon 簡單存儲服務用戶指南。

- AWS Glue

從 Amazon S3 中的資料建立 AWS Glue 表格，以便在中使用 AWS Entity Resolution。

如需詳細資訊，請參閱[什麼是 AWS Glue？](#) 在AWS Glue 開發人員指南中。

- AWS CloudTrail

AWS Entity Resolution 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[使用記錄 AWS Entity Resolution API 呼叫 AWS CloudTrail。](#)

- AWS CloudFormation

在中建立下列資源 AWS CloudFormation：AWS::EntityResolution::MatchingWorkflow, AWS::EntityResolution::SchemaMapping, AWS::EntityResolution::IdMappingWorkflow, AWS::EntityResolution::IdNamespace 和 AWS::EntityResolution::PolicyStatement

如需詳細資訊，請參閱[使用建立AWS實體解析資源 AWS CloudFormation。](#)

## 存取 AWS Entity Resolution

您可以通 AWS Entity Resolution 過以下選項訪問：

- 直接通過 AWS Entity Resolution 控制台在 <https://console.aws.amazon.com/entityresolution/>.
- 以編程方式通過 AWS Entity Resolution API. 如需詳細資訊，請[AWS Entity Resolution API參閱參考](#)。
  - 如果您打算 AWS Entity Resolution API在 AWS Lambda Runtime 中呼叫，請建立您自己的部署套件，並包含所需的 AWS SDK程式庫版本。如需詳細資訊，請參閱開AWS Lambda 發人員指南中的下列範例：
    - [使用 .zip 或JAR檔案封存來部署 Java Lambda 函數](#)

- [使用 .zip 文件存檔的 Python Lambda 函數](#)

## 定價 AWS Entity Resolution

如需定價資訊，請參閱 [AWS Entity Resolution 定價](#)。

# 設定 AWS Entity Resolution

AWS Entity Resolution 第一次使用 之前，請先註冊 AWS 並建立管理員使用者以建立角色。

## 註冊 AWS

如果您已有 AWS 帳戶，請略過此步驟。

如果您沒有 AWS 帳戶，請完成下列步驟以建立。

若要註冊 AWS 帳戶

1. 開啟<https://portal.aws.amazon.com/billing/註冊>。
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。

當您註冊時 AWS 帳戶，AWS 帳戶根使用者會建立。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，請將管理存取權指派給使用者，並且僅使用根使用者來執行[需要根使用者存取權的任務](#)。

## 建立管理員使用者

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身分中心 (建議)	使用短期憑證存取AWS。 這與安全性最佳實務一致。如需最佳實務的相關資訊，請參閱 IAM	請遵循 AWS IAM Identity Center 使用者指南的 <a href="#">入門</a> 中的說明。	透過在 AWS Command Line Interface 使用者指南 中設定 <a href="#">AWS CLI 以使用 來設定 AWS IAM Identity Center</a> 程式設計存取。

選擇一種管理管理員的方式	到	By	您也可以
	使用者指南 <a href="#">中的安全最佳實務IAM</a> 。		
在中 IAM (不建議使用)	使用長期憑證存取 AWS。	遵循 IAM 使用者指南 中 <a href="#">建立緊急存取IAM使用者</a> 的指示。	使用 IAM 使用者指南 中的 <a href="#">管理IAM使用者的存取金鑰</a> 來設定程式設計存取。

## 為主控台使用者建立IAM角色

如果您使用 AWS Entity Resolution 主控台，請完成下列程序。

### 建立 IAM 角色

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 Roles (角色)。

您可以使用角色來建立短期憑證，這是為了提高安全性而建議使用。您也可以選擇使用者來建立長期憑證。

3. 選擇建立角色。
4. 在建立角色精靈中，針對受信任實體類型，選擇 AWS 帳戶。
5. 保持選取此帳戶的選項，然後選擇下一步。
6. 對於新增許可，選擇建立政策。

新的標籤將開啟。

- a. 選取 JSON索引標籤，然後根據授予主控台使用者的能力新增政策。會根據常見使用案例 AWS Entity Resolution 提供下列受管政策：

- [AWS 受管理的策略：AWSEntityResolutionConsoleFullAccess](#)
- [AWS 受管理的策略：AWSEntityResolutionConsoleReadOnlyAccess](#)

- b. 選擇下一步：標籤，新增標籤（選用），然後選擇下一步：檢閱。
- c. 對於檢閱政策，輸入名稱和描述，然後檢閱摘要。
- d. 選擇 建立政策。

您已為協作成員建立政策。

- e. 返回原始索引標籤，然後在新增許可下，輸入您剛建立的政策名稱。（您可能需要重新載入頁面。）
  - f. 選取您建立的政策名稱旁邊的核取方塊，然後選擇下一步。
7. 針對名稱、檢閱和建立，輸入角色名稱和描述。
- a. 檢閱 選取信任的實體，AWS 帳戶輸入將擔任該角色的人員的（如有必要）。
  - b. 檢閱新增許可中的許可，並視需要編輯。
  - c. 檢閱標籤，並視需要新增標籤。
  - d. 選擇建立角色。

## 為 建立工作流程任務角色 AWS Entity Resolution

AWS Entity Resolution 使用工作流程任務角色來執行工作流程。如果您有必要的IAM許可，您可以使用主控台建立此角色。如果您沒有CreateRole許可，請您的管理員建立角色。

### 為 建立工作流程任務角色 AWS Entity Resolution

1. <https://console.aws.amazon.com/iam/> 使用您的管理員帳戶登入IAM主控台。
2. 在 Access management (存取管理) 下，請選擇 Roles (角色)。

您可以使用角色來建立短期憑證，這是為了提高安全性而建議使用。您也可以選擇使用者來建立長期憑證。

3. 選擇建立角色。
4. 在建立角色精靈中，針對受信任實體類型，選擇自訂信任政策。
5. 將下列自訂信任政策複製並貼到JSON編輯器中。

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

```

    "Principal": {
      "Service": [
        "entityresolution.amazonaws.com"
      ]
    },
    "Action": "sts:AssumeRole"
  }
]
}

```

6. 選擇 Next (下一步)。
7. 對於新增許可，選擇建立政策。

新索引標籤隨即出現。

- a. 將下列政策複製並貼到JSON編輯器中。

#### Note

下列範例政策支援讀取 Amazon S3 和 等對應資料資源所需的許可 AWS Glue。不過，您可能需要根據設定資料來源的方式修改此政策。

您的 AWS Glue 資源和基礎 Amazon S3 資源必須與 AWS 區域 位於相同位置 AWS Entity Resolution。

如果您的資料來源未加密或解密，則不需要授予 AWS KMS 許可。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::{{input-buckets}}",
        "arn:aws:s3:::{{input-buckets}}/*"
      ],
      "Condition": {

```

```

        "StringEquals":{
            "s3:ResourceAccount":[
                "{{accountId}}"
            ]
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": [
            "arn:aws:s3:::{{output-bucket}}",
            "arn:aws:s3:::{{output-bucket}}/*"
        ],
        "Condition":{
            "StringEquals":{
                "s3:ResourceAccount":[
                    "{{accountId}}"
                ]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "glue:GetDatabase",
            "glue:GetTable",
            "glue:GetPartition",
            "glue:GetPartitions",
            "glue:GetSchema",
            "glue:GetSchemaVersion",
            "glue:BatchGetPartition"
        ],
        "Resource": [
            "arn:aws:glue:{{aws-region}}:{{accountId}}:database/{{input-databases}}",
            "arn:aws:glue:{{aws-region}}:{{accountId}}:table/{{input-database}}/{{input-tables}}",
            "arn:aws:glue:{{aws-region}}:{{accountId}}:catalog"
        ]
    }

```

```

    }
  ]
}

```

取代每個 `{{user input placeholder}}` 使用您自己的資訊。

`aws-region`

AWS 區域 資源的。您的 AWS Glue 資源、基礎 Amazon S3 資源和資源 AWS KMS 必須與 AWS 區域 相同AWS Entity Resolution。

`accountId`

您的 AWS 帳戶 ID。

`input-buckets`

Amazon S3 儲存貯體，其中包含AWS Entity Resolution 將從 AWS Glue 中讀取的 基礎資料物件。

`output-buckets`

AWS Entity Resolution 將產生輸出資料的 Amazon S3 儲存貯體。

`input-databases`

AWS Glue AWS Entity Resolution 將從中讀取的資料庫。

- b. (選用) 如果輸入 Amazon S3 儲存貯體使用客戶KMS金鑰加密，請新增下列項目：

```

{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": [
    "arn:aws:kms:{{aws-region}}:{{accountId}}:key/{{inputKeys}}"
  ]
}

```

取代每個 `{{user input placeholder}}` 使用您自己的資訊。

<i>aws-region</i>	AWS 區域 資源的 。您的 AWS Glue 資源、基礎 Amazon S3 資源和資源 AWS KMS 必須與 AWS 區域 相同AWS Entity Resolution 。
<i>accountId</i>	您的 AWS 帳戶 ID。
<i>inputKeys</i>	中的受管金鑰 AWS Key Management Service。如果您的輸入來源已加密，AWS Entity Resolution 則必須使用金鑰解密資料。

- c. (選用) 如果寫入輸出 Amazon S3 儲存貯體的資料需要加密，請新增下列項目：

```
{
  "Effect": "Allow",
  "Action": [
    "kms:GenerateDataKey",
    "kms:Encrypt"
  ],
  "Resource": [
    "arn:aws:kms:{{aws-region}}:{{accountId}}:key/{{outputKeys}}"
  ]
}
```

取代每個 *{{user input placeholder}}* 使用您自己的資訊。

<i>aws-region</i>	AWS 區域 資源的 。您的 AWS Glue 資源、基礎 Amazon S3 資源和資源 AWS KMS 必須與 AWS 區域 相同AWS Entity Resolution 。
<i>accountId</i>	您的 AWS 帳戶 ID。
<i>outputKeys</i>	中的受管金鑰 AWS Key Management Service。如果您需要將輸出來源加密，AWS Entity Resolution 必須使用 金鑰加密輸出資料。

- d. (選用) 如果您透過 擁有具有提供者服務的訂閱 AWS Data Exchange，並想要將現有角色用於提供者服務型工作流程，請新增以下內容：

```
{
  "Effect": "Allow",
  "Sid": "DataExchangePermissions",
  "Action": "dataexchange:SendApiAsset",
  "Resource": [
    "arn:aws:dataexchange:{{aws-region}}::data-sets/{{datasetId}}/
revisions/{{revisionId}}/assets/{{assetId}}"
  ]
}
```

取代每個 *{{user input placeholder}}* 使用您自己的資訊。

*aws-region*

授予提供者資源 AWS 區域的。您可以在 ARN AWS Data Exchange 主控台的資產中找到此值。例如：`arn:aws:dataexchange:us-east-2::data-sets/111122223333/revisions/339ffc6444examplef3bc15cf0b2346b/assets/546468b8examplelea37bfc73b8f79fefafa`

*datasetId*

資料集的 ID，位於 AWS Data Exchange 主控台上。

*revisionId*

資料集的修訂，可在 AWS Data Exchange 主控台上找到。

*assetId*

在主控台上 AWS Data Exchange 找到的資產 ID。

8. 返回原始索引標籤，然後在新增許可下，輸入您剛建立的政策名稱。（您可能需要重新載入頁面。）
9. 選取您建立的政策名稱旁邊的核取方塊，然後選擇下一步。
10. 對於名稱、檢閱和建立，輸入角色名稱和描述。

 Note

角色名稱必須符合授予passRole成員許可中的模式，該成員可以傳遞 workflow job role來建立相符的工作流程。

例如，如果您使用的是 AWSEntityResolutionConsoleFullAccess 受管政策，請記得包含在您的角色名稱entityresolution中。

- a. 檢閱選取信任的實體，並視需要編輯。
- b. 檢閱新增許可 中的許可，並視需要編輯。
- c. 檢閱標籤，並視需要新增標籤。
- d. 選擇建立角色。

的工作流程任務角色 AWS Entity Resolution 已建立。

## 準備輸入數據表

In (入) AWS Entity Resolution，您的每個輸入資料表都包含來源記錄。這些記錄包含消費者識別碼，例如名字、姓氏、電子郵件地址或電話號碼。這些來源記錄可以與您在相同或其他輸入資料表格中提供的其他來源記錄相符。每個記錄都必須具有唯一的 Record ID ([唯一 ID](#))，並且在其中建立結構描述對應時，必須將其定義為主索引鍵 AWS Entity Resolution。

每個輸入數據表都可以作為 AWS Glue 表由 Amazon S3 支持。您可以使用已存在於 Amazon S3 中的第一方資料，或將其他第三方 SaaS 供應商的資料表匯入 Amazon S3。將資料上傳到 Amazon S3 之後，您可以使用 AWS Glue 爬蟲來創建一個數據表 AWS Glue Data Catalog。然後，您可以使用數據表作為輸入 AWS Entity Resolution。

以下各節說明如何準備第一方資料和第三方資料。

### 主題

- [準備第一方輸入資料](#)
- [準備第三方輸入資料](#)

## 準備第一方輸入資料

[下列步驟說明如何準備第一方資料，以便在規則型比對工作流程、以機器學習為基礎的比對工作流程或 ID 對應工作流程中使用。](#)

### 步驟 1：以支援的資料格式儲存輸入資料表

如果您已以支援的資料格式儲存第一方輸入資料，則可以略過此步驟。

使用 AWS Entity Resolution，輸入資料的格式必須為 AWS Entity Resolution 支持。AWS Entity Resolution 支援下列資料格式：

- 逗號分隔值 (,) CSV
- Parquet

### 步驟 2：將您的輸入資料表上傳到 Amazon S3

如果您已經在 Amazon S3 中擁有第一方資料表，則可以略過此步驟。

**Note**

輸入的數據必須存儲在 Amazon Simple Storage Service (Amazon S3) 中 AWS 帳戶 以及 AWS 區域 您要在其中執行相符的工作流程。

將您的輸入資料表上傳到 Amazon S3

1. 登入 AWS Management Console 並在打開 Amazon S3 控制台 <https://console.aws.amazon.com/s3/>。
2. 選擇「值區」，然後選擇儲存貯體來儲存資料表。
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表的資料夾。

### 步驟 3：建立 AWS Glue table

Amazon S3 中的輸入數據必須在 AWS Glue 並表示為 AWS Glue 表。有關如何創建的更多信息 AWS Glue 以 Amazon S3 做為輸入的表格，請參閱 [使用 AWS Glue 控制台](#) AWS Glue 開發人員指南。

**Note**

AWS Entity Resolution 不支援分區資料表。

在此步驟中，您可以在 AWS Glue 抓取 S3 存儲桶中的所有文件並創建一個 AWS Glue 表。

**Note**

AWS Entity Resolution 目前不支援使用註冊的 Amazon S3 位置 AWS Lake Formation。

若要建立 AWS Glue table

1. 登入 AWS Management Console 並打開 AWS Glue 控制台位於 <https://console.aws.amazon.com/glue/>。
2. 從導覽列選取爬行者程式。

3. 從清單中選取您的 S3 儲存貯體，然後選擇 [新增爬行者程式]。
4. 在「新增爬行者程式」頁面上，輸入爬行者程式名稱，然後選擇下一步。
5. 繼續執行「新增爬行者程式」頁面，指定詳細資訊。
6. 在 [選擇IAM角色] 頁面上，選擇 [選擇現有IAM角色]，然後選擇 [下一步]。

您也可以選擇 [建立IAM角色]，或視需要讓管理員建立IAM角色。

7. 對於「建立此爬行者程式」的排程，請保留「頻率」預設值 (視需求執行)，然後選擇下一步。
8. 若要設定爬行者程式的輸出，請輸入 AWS Glue 數據庫，然後選擇下一步。
9. 檢閱所有詳細資訊，然後選擇 [完成]。
10. 在 [爬行者程式] 頁面上，選取 S3 儲存貯體旁邊的核取方塊，然後選擇 [執行爬行者程式]。
11. 爬行者程式完成執行之後，在 AWS Glue 導覽列，選擇 [資料庫]，然後選擇您的資料庫名稱。
12. 在 [資料庫] 頁面上，選擇 {您的資料庫名稱} 中的 [表格]。
  - a. 檢視中的表格 AWS Glue 數據庫。
  - b. 若要檢視資料表的結構定義，請選取特定資料表。
  - c. 請記下 AWS Glue 資料庫名稱和 AWS Glue 表格名稱。

您現在可以建立綱要對應。如需詳細資訊，請參閱[建立綱要對應](#)。

## 準備第三方輸入資料

第三方資料服務提供的識別碼可與您的已知識別碼相符。

AWS Entity Resolution 目前支援下列第三方資料提供者服務：

### 資料提供者服務

公司名稱	可用性 AWS 區域	識別符
LiveRamp	美國東部 (維吉尼亞北部) (us-east-1)、美國東部 (俄亥俄) (us-east-2) 和美國西部 (奧勒岡) (us-west-2)	坡道識別碼
TransUnion	美國東部 (維吉尼亞北部) (us-east-1)、美國東部 (俄亥俄)	TransUnion 個人及家庭 IDs

公司名稱	可用性 AWS 區域	識別符
	(us-east-2) 和美國西部 (奧勒岡) (us-west-2)	
統一識別碼 2.0	美國東部 (維吉尼亞北部) (us-east-1)、美國東部 (俄亥俄) (us-east-2) 和美國西部 (奧勒岡) (us-west-2)	原始的 UID 2

下列步驟說明如何準備協力廠商資料，以使用[提供者服務型比對工作流程](#)或[提供者服務型 ID 對應](#)工作流程。

### 主題

- [步驟 1：訂閱提供者服務 AWS Data Exchange](#)
- [步驟 2：準備第三方資料表](#)
- [步驟 3：以支援的資料格式儲存輸入資料表](#)
- [步驟 4：將您的輸入資料表上傳到 Amazon S3](#)
- [步驟 5：建立 AWS Glue table](#)

## 步驟 1：訂閱提供者服務 AWS Data Exchange

如果您有提供者服務的訂閱 AWS Data Exchange，您可以使用下列其中一個提供者服務執行相符的工作流程，以將已知識別碼與您偏好的提供者相符。您的數據將與您首選的提供商定義的一組輸入進行匹配。

若要訂閱提供者服務 AWS Data Exchange

1. 檢視提供者清單 AWS Data Exchange。以下是可用的供應商清單：

- LiveRamp
  - [LiveRamp 身份解析](#)
  - [LiveRamp 轉碼](#)
- TransUnion
  - TransUnion TruAudience 無轉移的身份解析和豐富
  - TransUnion TruAudience 無轉移身份解析

- 統一識別碼 2.0
    - [統一 ID 2.0 身分識別解析](#)
2. 根據您的報價類型，完成下列其中一個步驟。
    - 私人報價 — 如果您與[供應商有現有關係](#)，請遵循「[私人產品和優惠](#)」程序 AWS Data Exchange 用戶指南接受私人報價 AWS Data Exchange.
    - 使用您自己的訂閱 — 如果您已經向供應商訂閱現有的資料，請遵循「[自攜訂閱](#)」(BYOS) [提供](#)程序 AWS Data Exchange 接受BYOS講價的使用者指南 AWS Data Exchange.
  3. 在您訂閱提供者服務之後 AWS Data Exchange之後，您可以使用該提供者服務建立相符的工作流程或 ID 對應工作流程。

如需有關如何[存](#)取包含的供應商產品的詳細資訊APIs，請參閱 API AWS Data Exchange 使用者指南。

## 步驟 2：準備第三方資料表

每個第三方服務都有不同的建議和準則集，以協助確保成功的比對工作流程。

若要準備協力廠商資料表，請參閱下表：

### 資料提供者服務指南

供應商服務	需要唯一的 ID 嗎？	動作
LiveRamp	是	<p>請確保以下事項：</p> <ul style="list-style-type: none"> <li>• <a href="#">唯一 ID</a> 可以是您自己的匿名識別碼，也可以是資料列 ID。</li> <li>• 您的數據輸入文件格式和規範化與 LiveRamp 指導方針一致。</li> </ul> <p>若要取得有關符合工作流程之輸入檔案格式化準則的詳細資訊，請參閱 LiveRamp 文件 ADX 中的<a href="#">執行識別解決</a>方式。</p> <p>如需 ID 對應工作流程之輸入檔案格式化準則的詳細資訊，請參閱 LiveRamp 文件 ADX 中的<a href="#">執行轉碼</a>至。</p>
TransUnion	是	<p>請確保以下事項：</p>

供應商服務	需要唯一的 ID 嗎？	動作
		<ul style="list-style-type: none"> <li>• TransUnion 資料擴充存在<u>唯一 ID</u>。</li> </ul> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> <b>Note</b></p> <p>沿著屬性傳遞被允許在輸入和輸出中持續存在 TransUnion。家庭 E 鍵和特定HHID於客戶端命名空間。</p> </div> <ul style="list-style-type: none"> <li>• <b>Phone number</b>應為 10 位數字，不含任何特殊字元，例如空格或連字號。</li> <li>• <b>Addresses</b> 應該分成 <ul style="list-style-type: none"> <li>• 單一地址行（如果存在，則結合地址行 1 和 2）</li> <li>• 城市</li> <li>• zip（或 zip plus4），沒有任何特殊字符，如空格或連字符</li> <li>• 狀態，指定為 2 個字母代碼 3</li> </ul> </li> <li>• <b>Email addresses</b> 應該是明文。</li> <li>• <b>First Name</b>可以是小寫或大寫，支持暱稱，但應排除標題和後綴。</li> <li>• <b>Last Name</b>可以是要排除的小寫或大寫，中間首字母縮寫。</li> </ul>

供應商服務	需要唯一的 ID 嗎？	動作
統一識別碼 2.0	是	<p>請確保以下事項：</p> <ul style="list-style-type: none"> <li>• <a href="#">唯一 ID</a> 不能是雜湊。</li> <li>• UID2支持電子郵件和電話號碼進行UID2生成。但是，如果結構描述對映中都存在兩個值，則工作流程會複製輸出中的每個記錄。一筆記錄使用電子郵件進行UID2產生，而第二筆記錄使用電話號碼。如果您的資料包含混合的電子郵件和電話號碼，而且您不想在輸出中重複記錄，最好的方法是為每個工作流程建立單獨的工作流程，並使用不同的結構描述對應。在這個案例中，請執行兩次步驟 — 為電子郵件建立一個工作流程，為電話號碼建立另一個工作流程。</li> </ul> <div data-bbox="852 947 1507 1646" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>無論是誰提出請求，在任何特定時間，特定的電子郵件或電話號碼都會產生相同的原始UID2值。</p> <p>原料UID2s是通過從鹽桶中添加鹽來創建的，鹽每年大約旋轉一次，從而導致UID2致原料也隨之旋轉。不同的鹽桶全年在不同的時間旋轉。AWS Entity Resolution 目前不跟踪旋轉的鹽桶和原料UID2s，因此建議您UID2s每天再生原料。如需詳細資訊，請參閱<a href="#">閱累加式更新UID2s應多久重新整理一次？</a>在UID 2.0 文檔中。</p> </div>

### 步驟 3：以支援的資料格式儲存輸入資料表

如果您已以支援的資料格式儲存第三方輸入資料，則可略過此步驟。

使用 AWS Entity Resolution，輸入資料的格式必須為 AWS Entity Resolution 支持。AWS Entity Resolution 支援下列資料格式：

- 逗號分隔值 (,) CSV

 Note

LiveRamp 僅支持 CSV 文件。

- Parquet

## 步驟 4：將您的輸入資料表上傳到 Amazon S3

如果您在 Amazon S3 中已有第三方資料表，則可以略過此步驟。

 Note

輸入的數據必須存儲在 Amazon Simple Storage Service (Amazon S3) 中 AWS 帳戶 以及 AWS 區域 您要在其中執行相符的工作流程。

將您的輸入資料表上傳到 Amazon S3

1. 登入 AWS Management Console 並在打開 Amazon S3 控制台 <https://console.aws.amazon.com/s3/>。
2. 選擇「值區」，然後選擇儲存貯體來儲存資料表。
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表的資料夾。

## 步驟 5：建立 AWS Glue table

Amazon S3 中的輸入數據必須在 AWS Glue 並表示為 AWS Glue 表。有關如何創建的更多信息 AWS Glue 以 Amazon S3 做為輸入的表格，請參閱 [使用 AWS Glue 控制台](#) AWS Glue 開發人員指南。

**Note**

AWS Entity Resolution 不支援分區資料表。

在此步驟中，您可以在 AWS Glue 抓取 S3 存儲桶中的所有文件並創建一個 AWS Glue 表。

**Note**

AWS Entity Resolution 目前不支援使用註冊的 Amazon S3 位置 AWS Lake Formation。

### 若要建立 AWS Glue table

1. 登入 AWS Management Console 並打開 AWS Glue 控制台位於 <https://console.aws.amazon.com/glue/>。
2. 從導覽列選取爬行者程式。
3. 從清單中選取您的 S3 儲存貯體，然後選擇 [新增爬行者程式]。
4. 在「新增爬行者程式」頁面上，輸入爬行者程式名稱，然後選擇下一步。
5. 繼續執行「新增爬行者程式」頁面，指定詳細資訊。
6. 在 [選擇IAM角色] 頁面上，選擇 [選擇現有IAM角色]，然後選擇 [下一步]。

您也可以選擇 [建立IAM角色]，或視需要讓管理員建立IAM角色。

7. 對於「建立此爬行者程式」的排程，請保留「頻率」預設值 (視需求執行)，然後選擇下一步。
8. 若要設定爬行者程式的輸出，請輸入 AWS Glue 數據庫，然後選擇下一步。
9. 檢閱所有詳細資訊，然後選擇 [完成]。
10. 在 [爬行者程式] 頁面上，選取 S3 儲存貯體旁邊的核取方塊，然後選擇 [執行爬行者程式]。
11. 爬行者程式完成執行之後，在 AWS Glue 導覽列，選擇 [資料庫]，然後選擇您的資料庫名稱。
12. 在 [資料庫] 頁面上，選擇 {您的資料庫名稱} 中的 [表格]。
  - a. 檢視中的表格 AWS Glue 數據庫。
  - b. 若要檢視資料表的結構定義，請選取特定資料表。
  - c. 請記下 AWS Glue 資料庫名稱和 AWS Glue 表格名稱。

# 使用模式對映定義輸入資料

結構描述對映會定義您要解析的輸入資料。它還提供有關輸入數據的元數據，例如列的屬性類型（輸入類型）以及要匹配的列。

建立結構描述對映時，首先定義輸入欄位和輸入類型，然後定義比對鍵和群組相關資料。下圖摘要說明如何建立綱要對應。



#### Define your data

Import columns from an AWS Glue table, build a custom schema, or use a JSON editor.



#### Select input types

Assign a pre-defined input type for each input field to classify your data.



#### Assign match keys

Define a match key for each input field to enable comparison for your matching workflow.



#### Create data groups

Group related data that is separated into two or more input fields.

建立綱要對應之前，您必須先設定 AWS Entity Resolution 並準備您的資料表。如需詳細資訊，請參閱 [設定 AWS Entity Resolution](#) 和 [準備輸入數據表](#)。

建立綱要對應之後，您可以執行下列其中一項作業：

- [創建匹配的工作流程](#) 以查找不同數據輸入之間的匹配項。
- [建立 ID 命名空間來源](#)，您可以在 ID 對應工作流程中使用該來源將資料從來源轉換為目標。
- [在同一工作流程中建立 ID 對應工作流程 AWS 帳戶](#) 使用您的模式對映作為來源。

## 主題

- [建立綱要對應](#)
- [複製綱要對應](#)
- [編輯資料架構對映](#)
- [刪除綱要對應](#)

## 建立綱要對應

此程序說明建立綱要對應的程序 [AWS Entity Resolution 控制台](#)。

建立綱要對應的方式有三種：

- 使用匯入來源匯入現有的輸入資料 AWS Glueoption — 使用此建立方法定義輸入欄位，以預先填入的欄位 AWS Glue 表使用引導流程。
- 使用 [建立自訂結構描述] 選項手動定義輸入資料 — 使用此建立方法可使用引導式流程手動定義輸入欄位。
- 使用 [使用JSON編輯器] 選項手動建立 — 使用JSON編輯器手動建立、使用範例或匯入現有的輸入資料。

#### Note

此選項無法使用「唯一 ID」和「輸入」欄位。

## Import from AWS Glue

透過匯入既有的輸入資料來建立資料架構對映的 AWS Glue

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [結構描述對映]。
3. 在「綱要對映」頁面的右上角，選擇「建立綱要對應」。
4. 對於步驟 1：指定結構描述詳細資訊，請執行下列動作：
  - a. 在名稱和建立方法中，輸入綱要對應名稱和選擇性說明。
  - b. 對於建立方式，選擇匯入自 AWS Glue。
  - c. 選擇 AWS Glue 從下拉列表中選擇數據庫，然後選擇 AWS Glue 表從下拉列表。

若要建立新資料表，請移至 AWS Glue 控制台 <https://console.aws.amazon.com/glue/>。如需詳細資訊，請參閱 [AWS Glue 「」](#) 中的表格 AWS Glue 使用者指南。

- d. 對於「唯一 ID」，請指定明確參照資料每一列的欄。

### Example

例如，**Primary\_key**、**Row\_ID** 或 **Record\_ID**。

#### Note

唯一 ID 欄是必需的。唯一 ID 必須是單一資料表中的唯一識別碼。但是，在不同的表中，唯一 ID 可以具有重複的值。如果未指定唯一 ID、在相同來源中不是唯一

的，或者在跨來源的屬性名稱方面重疊，則 AWS Entity Resolution 執行相符工作流程時拒絕記錄。如果您在以規則為基礎的相符工作流程中使用此綱要對應，唯一 ID 不得超過 38 個字元。

- e. 對於「輸入」欄位，請選擇要用於比對和選擇性傳遞的欄。

您最多可以選擇 34 列，以進行匹配和傳遞。

- i. 在「比對」下，選擇要用作輸入欄位以進行比對的欄。

您最多可以選擇 24 列進行匹配。

- ii. 如果您要指定不用於比對的資料行，請選取 [新增要傳遞的資料欄]。

- iii. (選擇性) 在「穿過」下，選擇要包含為通過欄的欄。

- f. (選擇性) 如果要為資源啟用標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。

- g. 選擇 Next (下一步)。

5. 對於步驟 2：對應輸入欄位，請定義要用於比對和選用傳遞的輸入欄位。

- a. 對於要比對的輸入欄位，請為每個「輸入」欄位指定「輸入類型」、「比對鍵」和「雜湊」狀態。

輸入類型可幫助您對數據進行分類。「比對」鍵可讓輸入欄位與符合的工作流程進行比較。散列狀態指示，如果該輸入字段的列值是散列或純文本。

 Note

如果您要建立結構描述對應以供應 LiveRamp 商服務為基礎的比對技術搭配使用，您可以：

- 將輸入類型指定為 LiveRampID。
- 將名稱欄位指定為多個欄位 (例如 **first\_name**、**last\_name**) 或在一個欄位中指定。
- 將街道地址欄位指定為多個欄位 (例如 **address1**、**address2**) 或在一個欄位中指定。

如果與地址進行匹配，則需要郵政編碼。

- 包括帶有名稱的電子郵件或電話，這些字段可以與街道地址匹配。

**Note**

如果您要建立結構描述對應以機器學習為基礎的比對工作流程搭配使用，您的資料集必須至少包含下列其中一個屬性：**phonenumber**、**emailaddress**、**fullnameaddresses**、或。**birthdate**  
請勿將任何這些屬性的「輸入」類型指定為「自訂」字串。

- b. (選擇性) 對於傳遞輸入欄位，請新增不符合的輸入欄位及其對應的雜湊狀態。

散列狀態指示，如果該輸入字段的列值是散列或純文本。

- c. 選擇 Next (下一步)。

6. 對於步驟 3：群組資料，請執行下列操作：

- a. 選擇相關的 [名稱] 欄位，然後輸入 [群組名稱] 和 [比對] 索引鍵。

**Example**

例如，選擇輸入欄位**First name****Middle name**、和**Last name**。然後輸入名為「**Full name**」的群組名稱和名為「**Full name**」的比對鍵以啟用比較。

- b. 選擇相關的 [位址] 欄位，然後輸入 [群組名稱] 和 [比對] 索引鍵。

**Example**

例如，選擇輸入欄位**Home street address 1****Home street address 2**、和**Home city**。然後輸入名為「**Shipping address**」的群組名稱和名為「**Shipping address**」的比對鍵以啟用比較。

- c. 選擇相關的電話號碼欄位，然後輸入群組名稱和比對鍵。

**Example**

例如，選擇輸入欄位**Home phone 1****Home phone 2**、和**Cell phone**。然後輸入名為「**Shipping phone number**」的群組名稱和名為「**Shipping phone number**」的比對鍵以啟用比較。

如果您有多種類型的資料，您可以新增更多群組。

- d. 選擇 Next (下一步)。

7. 對於步驟 4：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. 選擇建立綱要對應。

 Note

將結構描述對應與工作流程相關聯之後，就無法修改該結構描述對應。如果您要使用現有的組態來建立新的綱要對應，您可以複製綱要對應。

建立結構描述對應之後，您就可以[建立相符的工作流程](#)或[建立 ID 命名空間](#)。

## Build custom schema

使用建立自訂結構描述選項建立結構描述對應

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [結構描述對映]。
3. 在「綱要對映」頁面的右上角，選擇「建立綱要對應」。
4. 對於步驟 1：指定結構描述詳細資訊，請執行下列動作：
  - a. 對於名稱和建立方法，請輸入綱要對應名稱和選擇性說明。
  - b. 對於 [建立方法]，請選擇 [建立自訂結構]
  - c. 在「唯一 ID」中，輸入唯一 ID 以識別資料的每一列。

### Example

例如，**Primary\_key**、**Row\_ID** 或 **Record\_ID**。

 Note

唯一 ID 欄是必需的。唯一 ID 必須是單一資料表中的唯一識別碼。但是，在不同的表中，唯一 ID 可以具有重複的值。如果未指定唯一 ID、在相同來源中不是唯一的，或者在跨來源的屬性名稱方面重疊，則 AWS Entity Resolution 執行相符工作流程時拒絕記錄。如果您在以規則為基礎的相符工作流程中使用此綱要對應，唯一 ID 不得超過 38 個字元。

- d. (選擇性) 如果要為資源啟用標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。
  - e. 選擇 Next (下一步)。
5. 對於步驟 2：對應輸入欄位，請定義要用於比對和選用傳遞的輸入欄位。

您最多可以為相符和傳遞定義 34 欄總計。

- a. 對於要比對的輸入欄位，新增「輸入」欄位及其對應的「輸入類型」、「比對鍵」和「雜湊」狀態。

您最多可以新增 24 個輸入欄位以進行比對。

輸入類型可幫助您對數據進行分類。「比對」鍵可讓輸入欄位與符合的工作流程進行比較。散列狀態指示，如果該輸入字段的列值是散列或純文本。

 Note

如果您要建立結構描述對應以 LiveRamp 提供者服務為基礎的比對技術搭配使用，則可以將輸入類型指定為 LiveRamp ID。如果要在輸出中包含 PII 數據，則必須將輸入類型指定為自定義字符串。

 Note

如果您要建立結構描述對應以機器學習為基礎的比對工作流程搭配使用，您的資料集必須至少包含下列其中一個屬性：**phonenumber**、**emailaddress**、**fullnameaddresses**、或 **birthdate**  
請勿將任何這些屬性的「輸入」類型指定為「自訂」字符串。

- b. (選擇性) 對於傳遞的輸入欄位，請新增不符合的輸入欄位及其對應的雜湊狀態。
  - c. 選擇 Next (下一步)。
6. 對於步驟 3：分組資料：
- a. 選擇相關的 [名稱] 欄位，然後輸入 [群組名稱] 和 [比對] 索引鍵。

### Example

例如，選擇輸入欄位**First name****Middle name**、和**Last name**。然後輸入名為「**Full name**」的群組名稱和名為「**Full name**」的比對鍵以啟用比較。

- b. 選擇相關的 [位址] 欄位，然後輸入 [群組名稱] 和 [比對] 索引鍵。

### Example

例如，選擇輸入欄位**Home street address 1****Home street address 2**、和**Home city**。然後輸入名為「**Shipping address**」的群組名稱和名為「**Shipping address**」的比對鍵以啟用比較。

- c. 選擇相關的電話號碼欄位，然後輸入群組名稱和比對鍵。

### Example

例如，選擇輸入欄位**Home phone 1****Home phone 2**、和**Cell phone**。然後輸入名為「**Shipping phone number**」的群組名稱和名為「**Shipping phone number**」的比對鍵以啟用比較。

如果您有多種類型的資料，您可以新增更多群組。

- d. 選擇 Next (下一步)。
7. 對於步驟 4：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. 選擇建立綱要對應。

#### Note

將結構描述對應與工作流程建立關聯之後，就無法修改綱要對應。如果您要使用現有的組態來建立新的綱要對應，您可以複製綱要對應。

建立結構描述對應之後，您就可以[建立相符的工作流程](#)或[建立 ID 命名空間](#)。

## Use JSON editor

### 使用JSON編輯器建立資料架構對映的步驟

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [結構描述對映]。
3. 在「綱要對映」頁面的右上角，選擇「建立綱要對應」。
4. 對於步驟 1：指定結構描述詳細資訊，請執行下列動作：
  - a. 對於名稱和建立方法，請輸入綱要對應名稱和選擇性說明。
  - b. 對於建立方法，選擇使用JSON編輯器。
  - c. (選擇性) 如果要為資源啟用標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。
  - d. 選擇 Next (下一步)。
5. 對於步驟 2：指定對應：
  - a. 開始在JSON編輯器中建立結構定義，或根據您的目標選擇下列其中一個選項：

您的目標	推薦選項
開始建立您的綱要對應	插入樣本，JSON然後根據需要編輯信息。
使用現有的JSON檔案	從檔案匯入

- b. 選擇 Next (下一步)。
6. 對於步驟 3：檢閱並建立：
    - a. 檢閱您為先前步驟所做的選取，並視需要進行編輯。
    - b. 選擇建立綱要對應。

#### Note

將結構描述對應與工作流程建立關聯之後，就無法修改綱要對應。如果您要使用現有的組態來建立新的綱要對應，您可以複製綱要對應。

建立結構描述對應之後，您就可以[建立相符的工作流程](#)或[建立 ID 命名空間](#)。

## 複製綱要對應

如果您要使用現有的組態來建立新的綱要對應，您可以複製綱要對應。

複製綱要對應：

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [結構描述對映]。
3. 選擇綱要對應。
4. 選擇複製。
5. 在 [指定結構描述詳細資料] 頁面上進行必要的變更，然後選擇 [下一步]。
6. 在 [選擇相符技術] 頁面上，進行任何必要的變更，然後選擇 [下一步]。
7. 在 [地圖輸入欄位] 頁面上，進行任何必要的變更，然後選擇 [下一步]。
8. 在 [群組資料] 頁面上，進行任何必要的變更，然後選擇 [下一步]。
9. 在 [檢閱並儲存] 頁面上，進行任何必要的變更，然後選擇複製綱要對應。

## 編輯資料架構對映

您只能先編輯綱要對映，然後再將其與工作流程建立關聯。將結構描述對應關聯至工作流程後，就無法編輯它。如果您要使用現有的組態來建立新的綱要對應，您可以複製綱要對應。

編輯綱要對應：

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [結構描述對映]。
3. 選擇綱要對應。
4. 選擇編輯。
5. 在 [指定結構描述詳細資料] 頁面上進行必要的變更，然後選擇 [下一步]。
6. 在 [選擇相符技術] 頁面上，進行任何必要的變更，然後選擇 [下一步]。
7. 在 [地圖輸入欄位] 頁面上，進行任何必要的變更，然後選擇 [下一步]。

8. 在 [群組資料] 頁面上，進行任何必要的變更，然後選擇 [下一步]。
9. 在 [檢閱並儲存] 頁面上，進行必要的變更，然後選擇 [編輯綱要對應]。

## 刪除綱要對應

如果結構描述對映與相符的工作流程相關聯，則無法刪除該結構描述對應。您必須先從所有關聯的相符工作流程中移除資料架構對映，然後才能刪除它。

若要刪除綱要對應：

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [結構描述對映]。
3. 選擇綱要對應。
4. 選擇 刪除。
5. 確認刪除，然後選擇 [刪除]。

# 使用 ID 命名空間定義輸入資料

ID 命名空間是輸入資料表周圍的包裝函式。您可以使用 ID 命名空間來提供中繼資料，說明您的輸入資料和比對技巧，以及如何在 [ID 對應工作流程](#) 中使用這些資料。

ID 命名空間有兩種類型：來源和目標。

- 來源包含來源資料的組態 AWS Entity Resolution ID 對應工作流程中的程序。
- 「目標」包含所有來源解析為之目標資料的組態。

您可以選擇要跨兩個解析的輸入數據 AWS 帳戶 在 ID 對應工作流程中。一個參與者建立 ID 命名空間來源，另一個參與者建立 ID 命名空間目標。參與者建立來源和目標之後，您可以執行 ID 對應工作流程，將資料從來源轉譯至目標。

下圖摘要說明如何建立 ID 命名空間，以在 ID 對應工作流程中使用。



#### Prerequisite

An ID namespace that is a source requires a data input: [schema mapping](#) and an associated AWS Glue database. An ID namespace that is the target requires a target domain.



#### Create ID namespace

Provide the name and description, and then choose the type: source or target.



#### Configure your data

Select the configuration method and enter your source or target information.



#### Use in ID mapping workflows

Use your ID namespace as either a source or a target in an ID mapping workflow across two AWS accounts.

以下各節說明如何建立 ID 命名空間來源和 ID 命名空間目標。

## 主題

- [ID 命名空間來源](#)
- [ID 命名空間目標](#)
- [編輯 ID 命名空間](#)
- [刪除 ID 命名空間](#)
- [新增或更新 ID 命名空間的資源策略](#)

## ID 命名空間來源

ID 命名空間來源是 [ID 對應工作流程](#) 中資料的來源。

在建立 ID 命名空間來源之前，您必須先建立結構描述對應或相符的工作流程，視您的使用案例而定。如需詳細資訊，請參閱 [建立綱要對應](#) 和 [使用相符的工作流程比對輸入資料](#)。

建立 ID 命名空間來源之後，您可以在 ID 對應工作流程中將其與 ID 命名空間目標一起使用。如需詳細資訊，請參閱 [使用 ID 映射工作流程映射輸入資料](#)。

有兩種方法可以在 AWS Entity Resolution 控制台：[基於規則的方法](#) 或 [提供者服務](#) 方法。

## 主題

- [建立 ID 命名空間來源 \(以規則為基礎\)](#)
- [建立 ID 命名空間來源 \(提供者服務\)](#)

## 建立 ID 命名空間來源 (以規則為基礎)

本主題說明使用以規則為基礎的方法建立 ID 命名空間來源的程序。此方法使用相符規則將第一方資料從來源轉譯為 ID 對應工作流程中的目標。

### Note

如果輸入資料是來源，則它必須具有結構描述對映和相關聯 AWS Glue 數據庫。

### 若要建立 ID 命名空間來源 (以規則為基礎)

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [ID 命名空間]。
3. 在 [ID 命名空間] 頁面的右上角，選擇 [建立 ID 命名空間]。
4. 對於詳細資訊，請執行下列操作：
  - a. 針對 ID 命名空間名稱，輸入唯一的名稱。
  - b. (選擇性) 在說明中，輸入選擇性說明。
  - c. 針對 ID 命名空間類型，選擇來源。
5. 對於 ID 命名空間方法，請選擇以規則為基礎。
6. 在「資料輸入」中，選擇您要使用的輸入類型，然後採取建議的動作。

供應商服務	建議的動作
現有的綱要對映	<ol style="list-style-type: none"> <li>1. 選擇綱要對應。</li> <li>2. 選擇 AWS Glue 資料庫，AWS Glue 表格，以及下拉式清單中的綱要對應。</li> </ol> <p>您最多可以新增 20 個資料輸入。</p>
現有的匹配工作流程	<ol style="list-style-type: none"> <li>1. 選擇「比對」工作流程。</li> <li>2. 選擇與 ID 命名空間相關聯的帳戶：您的 AWS 帳戶或其他 AWS 帳戶。</li> <li>3. 根據帳戶類型，選取「比對」工作流程名稱或輸入「比對」工作流程ARN。</li> </ol>

7. 對於規則參數，請執行下列操作。

a. 根據您的目標選擇下列其中一個選項，以指定「規則」控制項。

您的目標	推薦選項
同時允許來源和目標的規則	無偏好
選擇來源、目標或兩者是否可以在 ID 對應工作流程中提供規則	有限的規則

來源與目標之間的規則控制項必須相容，才能在 ID 對應工作流程中使用。例如，如果來源 ID 命名空間將規則限制在目標上，但目標 ID 命名空間將規則限制為來源，則會導致錯誤。

b. 根據您的資料輸入類型選擇下列其中一個選項，以指定「比對」規則。

資料輸入類型	建議的動作
綱要對映	<p>選擇 [新增其他規則] 以新增相符規則。</p> <p>您最多可以套用 25 個比對規則來定義您的比對條件。</p>

資料輸入類型	建議的動作
匹配 workflow	選擇「使用比對工作流程中的規則」或「提供新規則」來定義「比對」規則。

8. 對於比較和比對參數，請執行下列操作。

a. 根據您的目標選擇下列其中一個選項，以指定「比較」類型。

您的目標	推薦選項
允許在建立 ID 對應 workflow 時使用任何比較類型。	無偏好
查找存儲在多個輸入字段中的數據匹配的任意組合，無論數據是在相同還是不同的輸入字段中。	多個輸入字段
當存儲在多個輸入字段中的類似數據不應匹配時，在單個輸入字段中限制比較。	單一輸入欄位

b. 根據您的目標選擇下列其中一個選項，以指定「記錄」比對類型。

您的目標	推薦選項
允許在建立 ID 對應 workflow 時使用任何比較類型。	無偏好
當您建立 ID 對應 workflow 時，將記錄比對類型限制為目標中每個相符記錄的來源中僅儲存一個相符記錄。	有限的記錄匹配 以及 一個來源到一個目標
當您建立 ID 對應 workflow 時，將記錄比對類型限制在目標中每個符合記錄的來源中儲存所有相符的記錄。	有限的記錄匹配 以及 許多來源到一個目標

**Note**

您必須指定來源和目標 ID 命名空間的相容限制。例如，如果來源 ID 命名空間將規則限制在目標上，但目標 ID 命名空間將規則限制為來源，則會導致錯誤。

9. 從下拉式清單中選擇現有的服務角色名稱，以指定服務存取權限。
10. (選擇性) 若要啟用資源的標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。
11. 選擇建立 ID 命名空間。

即會建立 ID 命名空間來源。您現在可以[建立 ID 命名空間目標](#)了。

## 建立 ID 命名空間來源 (提供者服務)

本主題說明使用提供者服務方法建立 ID 命名空間來源的程序。此方法使用名為的提供者服務 LiveRamp。LiveRamp 在 ID 對應工作流程期間，將協力廠商編碼的資料從來源轉換為目標。

**Note**

如果輸入資料是來源，則它必須具有結構描述對映和相關聯 AWS Glue 數據庫。

### 若要建立 ID 命名空間來源 (提供者服務)

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [ID 命名空間]。
3. 在 [ID 命名空間] 頁面的右上角，選擇 [建立 ID 命名空間]。
4. 對於詳細資訊，請執行下列操作：
  - a. 針對 ID 命名空間名稱，輸入唯一的名稱。
  - b. (選擇性) 在說明中，輸入選擇性說明。
  - c. 針對 ID 命名空間類型，選擇來源。
5. 針對 ID 命名空間方法，選擇提供者服務。

**Note**

AWS Entity Resolution 目前正在將 LiveRamp 提供者服務作為 ID 命名空間方法。如果您有訂閱 LiveRamp，則狀態會顯示為「已訂閱」。如需如何訂閱的詳細資訊 LiveRamp，請參閱 [步驟 1：訂閱提供者服務 AWS Data Exchange](#)。

6. 對於「資料輸入」，請選擇 AWS Glue 資料庫，AWS Glue 表格，以及下拉式清單中的綱要對應。

您最多可以新增 20 個資料輸入。

7. 若要指定服務存取權限，請選擇一個選項並採取建議的動作。

選項	建議的動作
建立並使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 建立具有此表格所需原則的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-id-mapping-workflow-&lt;timestamp&gt;</code>。</li> <li>• 您必須具有建立角色和附加原則的權限。</li> <li>• 如果您的輸入資料已加密，請選擇 [此資料已使用KMS金鑰加密] 選項。然後，輸入 AWS KMS 用於解密資料輸入的金鑰。</li> </ul>
使用現有的服務角色	<ol style="list-style-type: none"> <li>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，可以輸入要使用之角色的 Amazon 資源名稱 (ARN)。  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。</li> <li>2. 選擇「在IAM外部檢視」連結來檢視服務角色。</li> </ol>

選項	建議的動作
	默認情況下，AWS Entity Resolution 不會嘗試更新現有的角色原則以新增必要的權限。

8. (選擇性) 若要啟用資源的標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。
9. 選擇建立 ID 命名空間。

即會建立 ID 命名空間來源。您現在可以[建立 ID 命名空間目標](#)了。

## ID 命名空間目標

ID 命名空間目標是 [ID 對應工作流程](#) 中資料的目標。所有來源都會解析到目標。

在建立 ID 命名空間目標之前，您必須先建立相符的工作流程或訂閱提供者服務 (LiveRamp)，視您的使用案例而定。如需詳細資訊，請參閱 [使用相符的工作流程比對輸入資料](#) 和 [步驟 1：訂閱提供者服務 AWS Data Exchange](#)。

建立 ID 命名空間目標之後，您可以在 ID 對應工作流程中將其與 ID 命名空間來源搭配使用。如需詳細資訊，請參閱[使用 ID 映射工作流程映射輸入資料](#)。

有兩種方法可以在 AWS Entity Resolution 控制台：[基於規則的方法](#)或[提供者服務方法](#)。

### 主題

- [建立 ID 命名空間目標 \(以規則為基礎的方法\)](#)
- [建立 ID 命名空間目標 \(提供者服務方法\)](#)

## 建立 ID 命名空間目標 (以規則為基礎的方法)

本主題說明使用以規則為基礎的方法建立 ID 命名空間目標的程序。此方法使用相符規則，在 ID 對應工作流程期間，將第一方資料從來源轉換為目標。

若要建立 ID 命名空間目標 (以規則為基礎)

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。

2. 在左側導覽窗格的 [資料準備] 下，選擇 [ID 命名空間]。
3. 在 [ID 命名空間] 頁面的右上角，選擇 [建立 ID 命名空間]。
4. 對於詳細資訊，請執行下列操作：
  - a. 針對 ID 命名空間名稱，輸入唯一的名稱。
  - b. (選擇性) 在說明中，輸入選擇性說明。
  - c. 針對 ID 命名空間類型，選擇目標。
5. 對於 ID 命名空間方法，請選擇以規則為基礎。
6. 對於資料輸入，請在「比對」工作流程下，執行下列操作
  - a. 選擇與 ID 命名空間相關聯的帳戶：您的 AWS 帳戶或其他 AWS 帳戶。
  - b. 根據帳戶類型，選取「比對」工作流程名稱或輸入「比對」工作流程ARN。
7. 對於規則參數，請執行下列操作。
  - a. 根據您的目標選擇下列其中一個選項，以指定「規則」控制項。

您的目標	推薦選項
同時允許來源和目標的規則	無偏好
選擇來源、目標或兩者是否可以在 ID 對應工作流程中提供規則	有限的規則

來源與目標之間的規則控制項必須相容，才能在 ID 對應工作流程中使用。例如，如果來源 ID 命名空間將規則限制在目標上，但目標 ID 命名空間將規則限制為來源，則會導致錯誤。

- b. 對於匹配規則，AWS Entity Resolution 會自動從相符的工作流程新增規則。
8. 對於比較和比對參數，請執行下列操作。
  - a. 根據您的目標選擇下列其中一個選項，以指定「比較」類型。

您的目標	推薦選項
允許在建立 ID 對應工作流程時使用任何比較類型。	無偏好

您的目標	推薦選項
查找存儲在多個輸入字段中的數據匹配的任意組合，無論數據是在相同還是不同的輸入字段中。	多個輸入字段
當存儲在多個輸入字段中的類似數據不應匹配時，在單個輸入字段中限制比較。	單一輸入欄位

- b. 根據您的目標選擇下列其中一個選項，以指定「記錄」比對類型。

您的目標	推薦選項
允許在建立 ID 對應工作流程時使用任何比較類型。	無偏好
當您建立 ID 對應工作流程時，將記錄比對類型限制為目標中每個相符記錄的來源中僅儲存一個相符記錄。	有限的記錄匹配 以及 一個來源到一個目標
當您建立 ID 對應工作流程時，將記錄比對類型限制在目標中每個符合記錄的來源中儲存所有相符的記錄。	有限的記錄匹配 以及 許多來源到一個目標

 Note

您必須指定來源和目標 ID 命名空間的相容限制。例如，如果來源 ID 命名空間將規則限制在目標上，但目標 ID 命名空間將規則限制為來源，則會導致錯誤。

- 從下拉式清單中選擇現有的服務角色名稱，以指定服務存取權限。
- (選擇性) 若要啟用資源的標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。
- 選擇建立 ID 命名空間。

ID 命名空間目標隨即建立。建立 ID 對應工作流程所需的 ID 命名空間 (來源和目標) 之後，就可以[建立 ID 對應工作流程](#)了。

## 建立 ID 命名空間目標 (提供者服務方法)

本主題說明使用提供者服務方法建立 ID 命名空間目標的程序。此方法使用名為的提供者服務 LiveRamp。LiveRamp 在 ID 對應工作流程期間，將協力廠商編碼的資料從來源轉換為目標。

若要建立 ID 命名空間目標 (提供者服務)

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [ID 命名空間]。
3. 在 [ID 命名空間] 頁面的右上角，選擇 [建立 ID 命名空間]。
4. 對於詳細資訊，請執行下列操作：
  - a. 針對 ID 命名空間名稱，輸入唯一的名稱。
  - b. (選擇性) 在說明中，輸入選擇性說明。
  - c. 針對 ID 命名空間類型，選擇目標。
5. 對於 ID 命名空間方法，請選擇提供者服務。

### Note

AWS Entity Resolution 目前正在將 LiveRamp 提供者服務作為 ID 命名空間方法。如果您有訂閱 LiveRamp，則狀態會顯示為「已訂閱」。如需如何訂閱的詳細資訊 LiveRamp，請參閱[步驟 1：訂閱提供者服務 AWS Data Exchange](#)。

6. 針對 Target 網域，輸入轉碼所 LiveRamp 提供的目標 LiveRamp 用戶端網域識別碼。
7. (選擇性) 若要啟用資源的標籤，請選擇 [新增標籤]，然後輸入 [金鑰] 和 [值] 配對。
8. 選擇建立 ID 命名空間。

ID 命名空間目標隨即建立。建立 ID 對應工作流程所需的 ID 命名空間 (來源和目標) 之後，就可以[建立 ID 對應工作流程](#)了。

## 編輯 ID 命名空間

您只能在將 ID 命名空間與 ID 對應工作流程建立關聯之前，才能編輯該命名空間。將 ID 命名空間與 ID 對應工作流程相關聯之後，就無法編輯它。

若要編輯 ID 命名空間：

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶（如果你還沒有這樣做）。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [ID 命名空間]。
3. 選擇 ID 命名空間。
4. 選擇編輯。
5. 在 [編輯 ID 命名空間] 頁面上，進行任何必要的變更，然後選擇 [儲存]。

## 刪除 ID 命名空間

ID 命名空間與 ID 對應工作流程相關聯時，您無法刪除該命名空間。您必須先從所有關聯的 ID 對應工作流程中移除綱要對應，然後才能刪除它。

若要刪除 ID 命名空間：

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶（如果你還沒有這樣做）。
2. 在左側導覽窗格的 [資料準備] 下，選擇 [ID 命名空間]。
3. 選擇 ID 命名空間。
4. 選擇刪除。
5. 確認刪除，然後選擇刪除。

## 新增或更新 ID 命名空間的資源策略

資源策略可讓 ID 對應資源的建立者存取您的 ID 命名空間資源。

若要新增或更新資源策略

1. 登入 AWS Management Console 並打開 [AWS Entity Resolution](#) 與您的控制台 AWS 帳戶，如果你還沒有這樣做。

2. 在左側導覽窗格的 [工作流程] 下，選擇 [ID 命名空間]。
3. 選擇 ID 命名空間。
4. 在 ID 命名空間詳細資料頁面上，選擇權限索引標籤。
5. 在 [資源策略] 區段中，選擇 [編輯]。
6. 在JSON編輯器中新增或更新原則。
7. 選擇 Save changes (儲存變更)。

# 使用相符的工作流程比對輸入資料

比對工作流程是一種資料處理任務，結合了並比較來自不同輸入來源的資料，並根據不同的比對技術來判斷其中哪些相符。它會產生資料輸出表。

當您建立相符的工作流程時，首先指定您的資料輸入、標準化步驟，然後選擇所需的相符技術和資料輸出。會從您指定的位置 AWS Entity Resolution 讀取您的資料，並在資料中找到兩個或多個記錄之間的相符項目。然後，它會將相符 ID 指派給相符資料集中的記錄。AWS Entity Resolution 然後將資料輸出檔案寫入您選擇的位置。您可以視需要使用 AWS Entity Resolution 來雜湊輸出資料，協助您維持對資料的控制。

相符的工作流程可以有多个執行，結果（成功或錯誤）會寫入名稱jobId為的資料夾。

資料輸出同時包含成功比對的檔案，以及錯誤的檔案。資料輸出可以包含多個欄位。成功的結果會寫入包含多個檔案的success資料夾，每個檔案都包含成功記錄的子集。同樣地，錯誤會寫入具有多個欄位的error資料夾，每個欄位都包含錯誤記錄的子集。如需錯誤疑難排解的詳細資訊，請參閱 [疑難排解相符工](#)。

下圖摘要說明如何建立相符的工作流程。



#### Complete prerequisite

Create a schema mapping to define your data.



#### Choose your data input

Select the AWS Glue database and table that contains your data and the associated schema mapping.



#### Set up matching techniques

Configure rule-based matching, use machine learning matching, or choose a provider service.



#### Specify data output

Choose your data output fields and format to write to your S3 location.

建立相符的工作流程之前，您必須先建立結構描述映射。如需詳細資訊，請參閱 [建立綱要對應](#)。

建立相符工作流程有三種方法，根據相符技術：[規則型](#)、[機器學習型](#) 或 [提供者服務型](#)。

建立並執行相符的工作流程之後，您可以執行下列動作：

- 在您指定的 S3 位置檢視結果。資料編製索引IDs後產生的相符工作流程。
- 使用 [規則型比對](#) 或 [機器學習（ML）比對](#) 的輸出，作為 [提供者服務型比對](#) 的輸入，或反之亦然，以滿足您的業務需求。

例如，若要節省提供者訂閱成本，您可以先執行 [規則型比對](#)，以在資料上尋找相符項目。然後，您可以將不匹配記錄的子集傳送至 [提供者服務型比對](#)。

## 主題

- [建立規則型比對工作流程](#)
- [建立以機器學習為基礎的比對工作流程](#)
- [建立提供者服務型比對工作流程](#)
- [編輯相符的工作流程](#)
- [刪除相符的工作流程](#)
- [尋找規則型比對工作流程的比對 ID](#)
- [從規則型或 ML 型比對工作流程刪除記錄](#)
- [疑難排解相符工](#)

## 建立規則型比對工作流程

[規則型比對](#)是一套階層式的瀑布比對規則，由根據您輸入的資料建議 AWS Entity Resolution，且您可以完全設定。規則型比對工作流程可讓您比較純文字或雜湊資料，根據您自訂的條件尋找完全相符的項目。

當 AWS Entity Resolution 找到資料中兩個或多個記錄之間的相符項目時，它會指派：

- 與相符資料集中記錄相符的 [ID](#)
- 產生相符的[相符規則](#)。

若要建立規則型比對工作流程

1. 登入 AWS Management Console 並使用 開啟[AWS Entity Resolution 主控台](#) AWS 帳戶（如果您尚未這麼做）。
2. 在左側導覽窗格中的工作流程 下，選擇相符。
3. 在相符工作流程頁面上的右上角，選擇建立相符工作流程。
4. 對於步驟 1：指定相符的工作流程詳細資訊，請執行下列動作：
  - a. 輸入相符工作流程名稱和選用的描述。
  - b. 對於資料輸入，從下拉式清單中選擇AWS Glue 資料庫，選取AWS Glue 資料表，然後選擇對應的結構描述映射。

您最多可以新增 19 個資料輸入。

- c. 預設會選取標準化資料選項，以便在比對之前標準化資料輸入。如果您不想標準化資料，請取消選取標準化資料選項。
- d. 若要指定服務存取許可，請選擇 選項並採取建議的動作。

選項	建議的動作
建立和使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-matching-workflow-&lt;timestamp&gt;</code> 。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由KMS金鑰選項加密。然後，輸入用來解密資料輸入的AWS KMS 金鑰。</li> </ul>
使用現有的服務角色	<ol style="list-style-type: none"> <li>1. 從下拉式清單中選擇現有的服務角色名稱。 <ul style="list-style-type: none"> <li>如果您有列出角色的許可，則會顯示角色清單。</li> <li>如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name ( ARN ) 。</li> <li>如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</li> </ul> </li> <li>2. 選擇外部連結中的檢視IAM，以檢視服務角色。 <ul style="list-style-type: none"> <li>根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</li> </ul> </li> </ol>

- e. ( 選用 ) 若要為 資源啟用標籤，請選擇新增標籤 ，然後輸入金鑰和值對。
- f. 選擇 Next (下一步)。

## 5. 對於步驟 2：選擇相符的技術：

### a. 針對相符方法，選擇規則型相符。

[AWS Entity Resolution](#) > [Matching workflows](#) > Create matching workflow

**Choose matching technique** Info  
Specify how you want your data to be matched or choose a provider service.

**Matching method**

**Rule-based matching**  
Use customized rules to find exact matches.

**Machine learning-based matching**  
Use our machine learning model to help find a broader range of matches.

**Provider services**  
Use this option if you have a subscription to a preferred provider through AWS Data Exchange.

**Rule-based matching** Info  
Your data will be evaluated against a set of rules to find exact matches.

- Match keys are used as a basis for comparison and rules are automatically created based on your match keys.
- You can customize the rules for matching by editing the **Matching rules** section.

**Processing cadence** | Info  
Determine how often to run your matching workflow job. The first job runs after you create the matching workflow. [See pricing](#)

**Manual**  
Your matching workflow job is run on demand. Useful for bulk processing.

**Automatic**  
Your matching workflow job is run automatically when you add or update your data inputs. Useful for incremental updates. This option is available only for rule-based matching.

**Index only for ID mapping - new**

**Turn on**  
By default, matching workflows generate IDs after the data is indexed. If you want to use the matching workflow as a source or a target in an ID mapping workflow, choose to only index the data and not generate IDs.

### b. 對於處理節奏，請根據您的目標選擇下列其中一個選項。

您的目標	建議選項
執行大量更新的隨需工作流程	手動
新資料進入 S3 儲存貯體後，立即執行工作流程	自動

#### Note

如果您選擇自動，請確保您已為 S3 儲存貯體開啟 Amazon EventBridge 通知。如需使用 S3 主控台啟用 Amazon EventBridge 的指示，請參閱 Amazon S3 使用者指南中的[啟用 EventBridge Amazon](#)。Amazon S3

### c. (選用) 對於僅針對 ID 映射的索引，您可以選擇開啟僅索引資料的功能，而不是產生 IDs。

依預設，比對工作流程會在資料編製索引 IDs 後產生。

### d. 針對相符規則，輸入規則名稱，然後選擇該規則的相符金鑰。

您最多可以建立 15 個規則，並且可以在規則之間套用最多 15 個不同的相符金鑰來定義相符條件。

e. 對於比較類型，請根據您的目標選擇下列其中一個選項。

您的目標	建議選項
尋找儲存在多個輸入欄位中資料的相符項目的任何組合	多個輸入欄位
限制與單一輸入欄位的比較	單一輸入欄位

f. 選擇 Next (下一步)。

## 6. 對於步驟 3：指定資料輸出和格式：

- a. 對於資料輸出目的地和格式，選擇資料輸出的 Amazon S3 位置，以及資料格式是標準化資料還是原始資料。
- b. 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰 ARN。
- c. 檢視系統產生的輸出。
- d. 對於資料輸出，決定您要包含、隱藏或遮罩的欄位，然後根據您的目標採取建議的動作。

您的目標	建議選項
包含欄位	將輸出狀態保留為已包含。
隱藏欄位（從輸出中排除）	選擇輸出欄位，然後選擇隱藏。
遮罩欄位	選擇輸出欄位，然後選擇雜湊輸出。
重設先前的設定	選擇 Reset (重設)。

- e. 選擇 Next (下一步)。

## 7. 對於步驟 4：檢閱並建立：

- a. 檢閱您針對先前步驟所做的選擇，並視需要編輯。
- b. 選擇 Create and run (建立並執行)。

訊息隨即出現，指出已建立相符的工作流程，且任務已開始。

## 8. 在相符的工作流程詳細資訊頁面上，在指標索引標籤上，檢視上次任務指標下的下列項目：

- 任務 ID。
- 相符工作流程任務的狀態：已佇列、進行中、已完成、失敗
- 工作流程任務的完成時間。
- 已處理的記錄數目。
- 未處理的記錄數目。
- 產生的唯一相符 IDs 項目。
- 輸入記錄的數量。

您也可以檢視先前已在任務歷史記錄下執行的相符工作流程任務的任務指標。

9. 比對工作流程任務完成後（狀態為 已完成），您可以前往資料輸出索引標籤，然後選擇您的 Amazon S3 位置以檢視結果。
10. （僅限手動處理類型）如果您已使用手動處理類型建立規則型比對工作流程，您可以隨時在比對工作流程詳細資訊頁面上選擇執行工作流程，以執行比對工作流程。

## 建立以機器學習為基礎的比對工作流程

[機器學習型比對](#)是一種預設程序，會嘗試比對您輸入所有資料的記錄。機器學習型比對工作流程可讓您比較純文字資料，使用機器學習模型尋找廣泛的比對。

### Note

機器學習模型不支援雜湊資料的比較。

當 AWS Entity Resolution 找到資料中兩個或多個記錄之間的相符項目時，它會指派：

- 與相符資料集中記錄相符的 [ID](#)
- 相符的 [可信度層級](#) 百分比。

您可以使用 ML 型比對工作流程的輸出作為資料服務提供者比對的輸入，反之亦然，以達成您的特定目標。例如，您可以執行 ML 型比對，先在自己的記錄上尋找跨資料來源的比對。如果子集不相符，您可以執行 [提供者服務型比對](#)，以尋找其他比對。

若要建立 ML 型比對工作流程：

1. 登入 AWS Management Console 並使用 [開啟 AWS Entity Resolution 主控台](#) AWS 帳戶（如果您尚未這麼做）。
2. 在左側導覽窗格中的工作流程下，選擇相符。
3. 在相符工作流程頁面上的右上角，選擇建立相符工作流程。
4. 對於步驟 1：指定相符的工作流程詳細資訊，請執行下列動作：
  - a. 輸入相符工作流程名稱和選用的描述。
  - b. 對於資料輸入，從下拉式清單中選擇 AWS Glue 資料庫，選取 AWS Glue 資料表，然後選擇對應的結構描述映射。

您最多可以新增 20 個資料輸入。

- c. 預設會選取標準化資料選項，以便在比對之前標準化資料輸入。如果您不想標準化資料，請取消選取標準化資料選項。

機器學習型配對只會標準化 [名稱](#)、[Phone](#)和 [電子郵件](#)。

- d. 若要指定服務存取權限，請選擇 [選項](#)並採取建議的動作。

選項	建議的動作
建立和使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-matching-workflow-&lt;timestamp&gt;</code> 。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由KMS金鑰選項加密。然後，輸入用來解密資料輸入的AWS KMS 金鑰。</li> </ul>
使用現有的服務角色	<ol style="list-style-type: none"> <li>1. 從下拉式清單中選擇現有的服務角色名稱。 <ul style="list-style-type: none"> <li>• 如果您有列出角色的許可，則會顯示角色清單。</li> <li>• 如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name ( ARN ) 。</li> <li>• 如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</li> </ul> </li> <li>2. 選擇外部連結中的檢視IAM，以檢視服務角色。 <ul style="list-style-type: none"> <li>• 根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</li> </ul> </li> </ol>

- e. ( 選用 ) 若要為資源啟用標籤，請選擇新增標籤，然後輸入金鑰和值對。

- f. 選擇 Next (下一步)。
5. 對於步驟 2：選擇相符的技術：
    - a. 針對相符方法，選擇以機器學習為基礎的相符。

The screenshot shows the 'Choose matching technique' step in the AWS Entity Resolution console. The breadcrumb trail is 'AWS Entity Resolution > Matching workflows > Create matching workflow'. The left sidebar shows four steps: Step 1 (Specify matching workflow details), Step 2 (Choose matching technique), Step 3 (Specify data output), and Step 4 (Review and create). The main content area is titled 'Choose matching technique' and includes an 'Info' icon. Below the title is the instruction: 'Specify how you want your data to be matched or choose a provider service.' The 'Matching method' section has three options: 'Rule-based matching' (unselected), 'Machine learning-based matching' (selected), and 'Provider services' (unselected). The 'Machine learning-based matching' option is highlighted with a blue border and contains the text: 'Use our machine learning model to help find a broader range of matches.' Below this, the 'Machine learning-based matching' section includes an 'Info' icon and a description: 'Your data will be evaluated against a set of rules defining the criteria to find exact matches. This can help find matches across your data that may be incomplete or may not look exactly the same.' The 'Processing cadence' section has an 'Info' icon and a description: 'Determine how often to run your matching workflow job. The first job runs after you create the matching workflow. See pricing'. There are two options: 'Manual' (selected) and 'Automatic' (unselected). The 'Manual' option description is: 'Your matching workflow job is run on demand. Useful for bulk processing.' The 'Automatic' option description is: 'Your matching workflow job is run automatically when you add or update your data inputs. Useful for incremental updates. This option is available only for rule-based matching.' At the bottom, there is a warning message with an 'Info' icon: 'Using hashed data may limit matching functionality. Rule-based matching is recommended when comparing hashed data. The machine learning model is unable to compare hashed data. Learn more'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

- b. 對於處理節奏，會選取手動選項。  
此選項可讓您隨需執行工作流程以進行大量更新。
  - c. 選擇 Next (下一步)。
6. 對於步驟 3：指定資料輸出和格式：
    - a. 對於資料輸出目的地和格式，選擇資料輸出的 Amazon S3 位置，以及資料格式是標準化資料還是原始資料。
    - b. 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰 ARN。
    - c. 檢視系統產生的輸出。
    - d. 對於資料輸出，決定您要包含、隱藏或遮罩的欄位，然後根據您的目標採取建議的動作。

您的目標	建議選項
包含欄位	將輸出狀態保留為已包含。
隱藏欄位 ( 從輸出中排除 )	選擇輸出欄位 ，然後選擇隱藏。
遮罩欄位	選擇輸出欄位 ，然後選擇雜湊輸出。
重設先前的設定	選擇 Reset (重設)。

e. 選擇 Next (下一步)。

7. 對於步驟 4：檢閱並建立：

a. 檢閱您針對先前步驟所做的選擇，並視需要編輯。

b. 選擇 Create and run (建立並執行)。

訊息隨即出現，指出已建立相符的工作流程，且任務已開始。

8. 在相符的工作流程詳細資訊頁面上的指標索引標籤中，檢視上次任務指標 下的下列項目：

- 任務 ID。
- 相符工作流程任務的狀態：已佇列、進行中、已完成、失敗
- 工作流程任務的完成時間。
- 處理的記錄數目。
- 未處理的記錄數目。
- 產生的唯一相符IDs項目。
- 輸入記錄 的數量。

您也可以檢視先前已在任務歷史記錄 下執行的相符工作流程任務的任務指標。

9. 比對工作流程任務完成後 ( 狀態為 已完成 )，您可以前往資料輸出索引標籤，然後選擇您的 Amazon S3 位置以檢視結果。

10. ( 僅限手動處理類型 ) 如果您已使用手動處理類型建立機器學習型比對工作流程，您可以隨時在比對工作流程詳細資訊頁面上選擇執行工作流程，以執行比對工作流程。

# 建立提供者服務型比對工作流程

[提供者服務型比對](#)可讓您將已知的識別符與偏好的資料服務供應商比對。

AWS Entity Resolution 目前支援下列資料提供者服務：

- LiveRamp
- TransUnion
- 統一 ID 2.0

如需支援的提供者服務的詳細資訊，請參閱 [準備第三方輸入資料](#)。

您可以在上為這些提供者使用公有訂閱，AWS Data Exchange 或直接與資料提供者協商私有優惠。如需建立新訂閱或重複使用現有訂閱至提供者服務的詳細資訊，請參閱 [步驟 1：訂閱提供者服務 AWS Data Exchange](#)。

下列各節說明如何建立以提供者為基礎的比對工作流程。

## 主題

- [使用 建立相符的工作流程 LiveRamp](#)
- [使用 建立相符的工作流程 TransUnion](#)
- [使用 2.0 UID 建立相符的工作流程](#)

## 使用 建立相符的工作流程 LiveRamp

如果您有 LiveRamp 服務的訂閱，您可以建立與服務相符的工作流程 LiveRamp，以執行身分解析。

LiveRamp 服務提供名為 RampID 的識別碼。RampID 是 IDs 需求端平台中最常用於建立廣告行銷活動受眾的其中一個平台。使用與相符的工作流程 LiveRamp，您可以將雜湊電子郵件地址解析為 RAMPIDs。

### Note

AWS Entity Resolution 支援 PII 型 RampID 指派。

此工作流程需要一個 Amazon S3 資料暫存儲存貯體，其中您希望暫時寫入相符的工作流程輸出。使用建立 ID 映射工作流程之前 LiveRamp，請將下列許可新增至資料暫存儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::715724997226:root"
      },
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::<staging-bucket>",
        "arn:aws:s3:::<staging-bucket>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::715724997226:root"
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::<staging-bucket>",
        "arn:aws:s3:::<staging-bucket>/*"
      ]
    }
  ]
}
```

取代每個 *<user input placeholder>* 使用您自己的資訊。

*staging-bucket*

Amazon S3 儲存貯體，可在執行提供者服務型工作流程時暫時存放您的資料。

若要使用 建立相符的工作流程 LiveRamp：

1. 登入 AWS Management Console 並使用 開啟[AWS Entity Resolution 主控台](#) AWS 帳戶（如果您尚未這麼做）。
2. 在左側導覽窗格中的工作流程 下，選擇相符。
3. 在相符工作流程頁面上的右上角，選擇建立相符工作流程。
4. 對於步驟 1：指定相符的工作流程詳細資訊，請執行下列動作：
  - a. 輸入相符工作流程名稱和選用的描述。
  - b. 對於資料輸入，從下拉式清單中選擇AWS Glue 資料庫，選取AWS Glue 資料表，然後選取對應的結構描述映射。

您最多可以新增 20 個資料輸入。

- c. 預設會選取標準化資料選項，以便在比對之前標準化資料輸入。

如果您使用僅限電子郵件的解析程序，請取消選取標準化資料選項，因為輸入資料只會使用雜湊電子郵件。

- d. 若要指定服務存取權限，請選擇 選項並採取建議的動作。

選項	建議的動作
建立和使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-matching-workflow- timestamp</code>。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由KMS金鑰選項加密。然後，輸入用來解密資料輸入的AWS KMS 金鑰。</li> </ul>

選項	建議的動作
使用現有的服務角色	<p>1. 從下拉式清單中選擇現有的服務角色名稱。</p> <p>如果您有列出角色的許可，則會顯示角色清單。</p> <p>如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name ( ARN )。</p> <p>如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</p> <p>2. 選擇外部連結中的檢視IAM，以檢視服務角色。</p> <p>根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</p>

- e. ( 選用 ) 若要為資源啟用標籤，請選擇新增標籤，然後輸入金鑰和值對。
  - f. 選擇 Next ( 下一步 )。
5. 對於步驟 2：選擇相符的技術：
- a. 針對相符方法，選擇提供者服務。
  - b. 針對提供者服務，選擇 LiveRamp。

 Note

確保您的資料輸入檔案格式和標準化符合提供者服務的準則。

如需相符工作流程的輸入檔案格式指南的詳細資訊，請參閱 LiveRamp 文件中的 [執行身分解析ADX](#)。

- c. 對於LiveRamp 產品，請從下拉式清單中選擇產品。

**Matching method**

Rule-based matching  
Use customized rules to find exact matches.

Machine learning-based matching  
Use our machine learning model to help find a broader range of matches.

**Provider services**  
Use this option if you have a subscription to a preferred provider through AWS Data Exchange.

**Provider services** [Info](#)

You must have a provider agreement to use a provider service. Your data will be matched with a set of inputs defined by your preferred provider. Some information may be required and shared between you and your provider service.

LiveRamp  
**/LiveRamp**

TransUnion  
**TransUnion** 

Unified ID 2.0  
**Unified iD** <sub>2.0</sub>

**LiveRamp products**  
Choose from available products from LiveRamp.

Choose product 

Assignment Email

Assignment PII

Cancel [Previous](#) [Next](#)

**Note**

如果您選擇指派 PII，則在執行實體解析時必須至少提供一個非識別符資料欄。例如，GENDER。

- d. 針對 LiveRamp 組態，輸入 Client ID 管理員 ARN 和 Client Secret Manager ARN。

### LiveRamp configuration

These are the required fields to use the LiveRamp service.

**Client ID manager ARN**  
Enter the Client ID manager ARN provided by LiveRamp.

83 of 2,048 characters.

**Client secret manager ARN**  
Enter the Client secret manager ARN provided by LiveRamp.

87 of 2,048 characters.

### Data staging [Info](#)

Choose the Amazon S3 location for temporarily storing your data while it processes. Your information will not be saved permanently.

**Amazon S3 location**

View [↗](#)
Browse S3

Cancel
Previous
Next

- e. 對於資料暫存，選擇 Amazon S3 位置，以便在處理資料時暫時儲存資料。

您必須擁有資料暫存 Amazon S3 位置的許可。如需詳細資訊，請參閱 [為 建立工作流程任務角色 AWS Entity Resolution](#)。

- f. 選擇 Next (下一步)。

6. 對於步驟 3：指定資料輸出：

- a. 對於資料輸出目的地和格式，選擇資料輸出的 Amazon S3 位置，以及資料格式是標準化資料還是原始資料。
- b. 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰 ARN。
- c. 檢視 LiveRamp 產生的輸出。

這是產生的其他資訊 LiveRamp。

- d. 對於資料輸出，決定您要包含、隱藏或遮罩的欄位，然後根據您的目標採取建議的動作。

**Note**

如果您已選擇 LiveRamp，由於 LiveRamp 隱私篩選條件會移除個人身分識別資訊 (PII)，部分欄位會顯示無法使用的輸出狀態。

您的目標	建議選項
包含欄位	將輸出狀態保留為已包含。
隱藏欄位 (從輸出中排除)	選擇輸出欄位，然後選擇隱藏。
遮罩欄位	選擇輸出欄位，然後選擇雜湊輸出。
重設先前的設定	選擇 Reset (重設)。

AWS Entity Resolution > ID mapping workflows > Create ID mapping workflow

Step 1 Specify ID mapping workflow details

Step 2 Specify source and target

Step 3 - optional

**Step 4 Specify data output location**

Step 4 Review and create

### Specify data output location - optional Info

Choose your S3 location to write your data output.

**Data output destination Info**

Choose the Amazon S3 location for the data output.

**Amazon S3 location**

Q s3://bucket/prefix View Browse S3

**Encryption - optional Info**

Your data is encrypted by default with a key that AWS owns and manages for you. To specify a different key, customize your encryption settings.

Customize encryption settings  
Specify an AWS KMS key to customize your encryption settings.

**▼ LiveRamp generated output (2)**

Additional information generated by LiveRamp.

Output field	Description
RAMPID	LiveRamp's universal identifier that is tied to devices in the LiveRamp Identity Graph
TRANSCODED_IDENTIFIER	LiveRamp's universal identifier that is tied to devices in the LiveRamp Identity Graph

Cancel Previous Next

e. 選擇 Next (下一步)。

7. 對於步驟 4：檢閱並建立：

- a. 檢閱您針對先前步驟所做的選擇，並視需要編輯。
- b. 選擇 Create and run (建立並執行)。

訊息隨即出現，指出已建立相符的工作流程，且任務已開始。

8. 在相符的工作流程詳細資訊頁面上，在指標索引標籤上，檢視上次任務指標 下的下列項目：
  - 任務 ID。
  - 相符工作流程任務的狀態：已佇列、進行中、已完成、失敗
  - 工作流程任務的完成時間。
  - 已處理的記錄數目。
  - 未處理的記錄數目。
  - 產生的唯一相符IDs項目。
  - 輸入記錄 的數量。

您也可以檢視先前已在任務歷史記錄 下執行的相符工作流程任務的任務指標。

9. 比對工作流程任務完成後（狀態為 已完成），您可以前往資料輸出索引標籤，然後選擇您的 Amazon S3 位置以檢視結果。

## 使用 建立相符的工作流程 TransUnion

如果您有 TransUnion 服務訂閱，您可以透過將儲存在不同管道中的客戶相關記錄與 TransUnion 人員和家庭 E 金鑰以及超過 200 個資料屬性連結、比對和增強，以改善客戶理解。

TransUnion 服務提供稱為 TransUnion 個人和家庭的識別符IDs。TransUnion 提供已知識別符的 ID 指派（也稱為編碼），例如名稱、地址、電話號碼和電子郵件地址。

此工作流程需要一個 Amazon S3 資料暫存儲存貯體，其中您希望暫時寫入相符的工作流程輸出。使用 建立相符的工作流程之前 TransUnion，請將下列許可新增至資料暫存儲存貯體。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::103054336026:root"
      }
    }
  ]
}
```

```

    },
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:GetObjectVersion",
      "s3:DeleteObject"
    ],
    "Resource": [
      "arn:aws:s3:::<staging-bucket>",
      "arn:aws:s3:::<staging-bucket>/*"
    ]
  },
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::103054336026:root"
    },
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation",
      "s3:GetBucketPolicy",
      "s3:ListBucketVersions",
      "s3:GetBucketAcl"
    ],
    "Resource": [
      "arn:aws:s3:::<staging-bucket>",
      "arn:aws:s3:::<staging-bucket>/*"
    ]
  }
]
}

```

取代每個 *<user input placeholder>* 使用您自己的資訊。

*staging-bucket*

Amazon S3 儲存貯體，可在執行提供者服務型  
工作流程時暫時存放您的資料。

若要使用 建立相符的工作流程 TransUnion :

1. 登入 AWS Management Console 並使用 開啟[AWS Entity Resolution 主控台](#) AWS 帳戶 ( 如果您尚未這麼做 )。
2. 在左側導覽窗格中的工作流程 下，選擇相符。
3. 在相符工作流程頁面上的右上角，選擇建立相符工作流程。
4. 對於步驟 1：指定相符的工作流程詳細資訊，請執行下列動作：
  - a. 輸入相符工作流程名稱和選用的描述。
  - b. 對於資料輸入，從下拉式清單中選擇AWS Glue 資料庫，選取AWS Glue 資料表，然後選取對應的結構描述映射。

您最多可以新增 20 個資料輸入。

- c. 預設會選取標準化資料選項，以便在比對之前標準化資料輸入。如果您不想標準化資料，請取消選取標準化資料選項。
- d. 若要指定服務存取許可，請選擇 選項並採取建議的動作。

選項	建議的動作
建立和使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-matching-workflow- &lt;timestamp&gt;</code>。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由KMS金鑰選項加密。然後，輸入用來解密資料輸入的AWS KMS 金鑰。</li> </ul>
使用現有的服務角色	<ol style="list-style-type: none"> <li>1. 從下拉式清單中選擇現有的服務角色名稱。</li> </ol> <p>如果您有列出角色的許可，則會顯示角色清單。</p>

選項	建議的動作
	<p>如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name ( ARN )。</p> <p>如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</p> <p>2. 選擇外部連結中的檢視IAM，以檢視服務角色。</p> <p>根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</p>

- e. ( 選用 ) 若要為資源啟用標籤，請選擇新增標籤，然後輸入金鑰和值對。
  - f. 選擇 Next (下一步)。
5. 對於步驟 2：選擇相符的技術：
- a. 針對相符方法，選擇提供者服務。
  - b. 針對提供者服務，選擇 TransUnion。

 Note

確保您的資料輸入檔案格式和標準化符合提供者服務的準則。

- c. 對於TransUnion 產品，請從下拉式清單中選擇產品。

[AWS Entity Resolution](#) > [Matching workflows](#) > Create matching workflow

Step 1  
[Specify matching workflow details](#)

Step 2  
**Choose matching technique**

Step 3  
Specify data output

Step 4  
Review and create

## Choose matching technique [Info](#)

Specify how you want your data to be matched or choose a provider service.

### Matching method

Rule-based matching  
Use customized rules to find exact matches.

Machine learning-based matching  
Use our machine learning model to help find a broader range of matches.

Provider services  
Use this option if you have a subscription to a preferred provider through AWS Data Exchange.

### Provider services [Info](#)

You must have a provider agreement in order to use a provider service. Your data will be matched with a set of inputs defined by your preferred provider. Some information may be required and shared between you and your provider service.

LiveRamp

TransUnion

Unified ID 2.0

TransUnion products  
Choose from available products from TransUnion.

Choose product ▼

Cancel Previous **Next**

- d. 對於資料暫存，選擇 Amazon S3 位置，以便在處理資料時暫時儲存資料。

您必須擁有資料暫存 Amazon S3 位置的許可。如需詳細資訊，請參閱[the section called “建立工作流程任務角色”](#)。

6. 選擇 Next (下一步)。
7. 對於步驟 3：指定資料輸出：
- 對於資料輸出目的地和格式，選擇資料輸出的 Amazon S3 位置，以及資料格式是標準化資料還是原始資料。
  - 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰 ARN。
  - 檢視 TransUnion 產生的輸出。

這是產生的其他資訊 TransUnion。

- d. 對於資料輸出，決定您要包含、隱藏或遮罩的欄位，然後根據您的目標採取建議的動作。

您的目標	建議選項
包含欄位	將輸出狀態保留為已包含。
隱藏欄位（從輸出中排除）	選擇輸出欄位，然後選擇隱藏。
遮罩欄位	選擇輸出欄位，然後選擇雜湊輸出。
重設先前的設定	選擇 Reset (重設)。

- e. 對於系統產生的輸出，檢視包含的所有欄位。
- f. 選擇 Next (下一步)。
8. 對於步驟 4：檢閱並建立：
- a. 檢閱您針對先前步驟所做的選擇，並視需要編輯。
- b. 選擇 Create and run (建立並執行)。

訊息隨即出現，指出已建立相符的工作流程，且任務已開始。

9. 在相符的工作流程詳細資訊頁面上的指標索引標籤中，檢視上次任務指標下的下列項目：
- 任務 ID。
  - 相符工作流程任務的狀態：已佇列、進行中、已完成、失敗
  - 工作流程任務的完成時間。
  - 已處理的記錄數目。
  - 未處理的記錄數目。
  - 產生的唯一相符IDs項目。
  - 輸入記錄的數量。

您也可以檢視先前已在任務歷史記錄下執行的相符工作流程任務的任務指標。

10. 比對工作流程任務完成後（狀態為 已完成），您可以前往資料輸出索引標籤，然後選擇您的 Amazon S3 位置以檢視結果。

## 使用 2.0 UID 建立相符的工作流程

如果您有 Unified ID 2.0 服務的訂閱，您可以啟動具有決定性身分的廣告活動，並倚賴於與廣告生態系統中許多UID2已啟用的參與者的互通性。如需詳細資訊，請參閱 [Unified ID 2.0 概觀](#)。

統一 ID 2.0 服務提供原始 UID 2，用於在 Trade Desk 平台中建立廣告活動。UID 2.0 是使用開放原始碼架構產生的。

在一個工作流程中，您可以使用 **Email Address** 或 **Phone number** 進行原始UID2產生，但不能同時使用兩者。如果結構描述映射中同時存在兩者，則工作流程會挑選 **Email Address**，而 **Phone number** 將是傳遞欄位。若要支援兩者，請建立新的結構描述映射，其中 **Phone number** 已映射 **Email Address** 但未映射。然後，使用此新的結構描述映射建立第二個工作流程。

### Note

原始 UID2s 是藉由從鹽儲存貯體中新增鹽，而鹽儲存貯體大約每年輪換一次，導致原始 UID2 也會隨之輪換。因此，建議您 UID2s 每天重新整理原始。如需詳細資訊，請參閱 <https://unifiedid.com/docs/開始使用/gs-faqs#how-often-should-uid2s-be-refreshed-for-incremental-updates>。

若要使用 2.0 UID 建立相符的工作流程：

1. 登入 AWS Management Console 並使用 開啟 [AWS Entity Resolution 主控台](#) AWS 帳戶（如果您尚未這麼做）。
2. 在左側導覽窗格中的工作流程 下，選擇相符。
3. 在相符工作流程頁面上的右上角，選擇建立相符工作流程。
4. 對於步驟 1：指定相符的工作流程詳細資訊，請執行下列動作：
  - a. 輸入相符工作流程名稱和選用的描述。
  - b. 對於資料輸入，從下拉式清單中選擇 AWS Glue 資料庫，選取 AWS Glue 資料表，然後選取對應的結構描述映射。  
  
您最多可以新增 20 個資料輸入。
  - c. 選擇標準化資料選項，以便在比對之前標準化資料輸入（**Email Address** 或 **Phone number**）。

如需 **Email Address** 標準化的詳細資訊，請參閱 UID2.0 文件中的 [電子郵件地址標準化](#)。

如需 **Phone number** 標準化的詳細資訊，請參閱 UID2.0 文件中的 [電話號碼標準化](#)。

- d. 若要指定服務存取許可，請選擇 選項並採取建議的動作。

選項	建議的動作
建立和使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-matching-workflow-&lt;timestamp&gt;</code>。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由 KMS 金鑰選項加密。然後，輸入用來解密資料輸入的 AWS KMS 金鑰。</li> </ul>
使用現有的服務角色	<ol style="list-style-type: none"> <li>1. 從下拉式清單中選擇現有的服務角色名稱。 <ul style="list-style-type: none"> <li>• 如果您有列出角色的許可，則會顯示角色清單。</li> <li>• 如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name (ARN)。</li> <li>• 如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</li> </ul> </li> <li>2. 選擇外部連結中的檢視 IAM，以檢視服務角色。 <ul style="list-style-type: none"> <li>• 根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</li> </ul> </li> </ol>

- e. (選用) 若要為資源啟用標籤，請選擇新增標籤，然後輸入金鑰和值對。
- f. 選擇 Next (下一步)。

5. 對於步驟 2：選擇相符的技術：
  - a. 針對相符方法，選擇提供者服務。
  - b. 對於提供者服務，選擇統一 ID 2.0。

The screenshot shows the 'Choose matching technique' step in the AWS Entity Resolution console. The breadcrumb trail is 'AWS Entity Resolution > Matching workflows > Create matching workflow'. The left sidebar shows the progress: Step 1 (Specify matching workflow details), Step 2 (Choose matching technique), Step 3 (Specify data output), and Step 4 (Review and create). The main content area is titled 'Choose matching technique' with an 'Info' link. Below the title is the instruction: 'Specify how you want your data to be matched or choose a provider service.' Under the 'Matching method' section, three options are listed: 'Rule-based matching' (unselected), 'Machine learning-based matching' (unselected), and 'Provider services' (selected). Below this, the 'Provider services' section explains that a provider agreement is required. Two provider options are shown: 'LiveRamp' and 'TransUnion', both unselected. The 'Unified ID 2.0' option is selected and highlighted. Below it, the status 'Access to Unified ID 2.0 provider subscription' is shown as 'Subscribed' with a green checkmark. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

- c. 選擇 Next (下一步)。
6. 對於步驟 3：指定資料輸出：
  - a. 對於資料輸出目的地和格式，選擇資料輸出的 Amazon S3 位置，以及資料格式是標準化資料還是原始資料。
  - b. 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰 ARN。
  - c. 檢視 Unified ID 2.0 產生的輸出。

這是 2.0 UID 所產生的所有其他資訊清單

- d. 對於資料輸出，決定您要包含、隱藏或遮罩的欄位，然後根據您的目標採取建議的動作。

您的目標	建議選項
包含欄位	將輸出狀態保留為已包含。
隱藏欄位 ( 從輸出中排除 )	選擇輸出欄位 ，然後選擇隱藏。
遮罩欄位	選擇輸出欄位 ，然後選擇雜湊輸出。
重設先前的設定	選擇 Reset (重設)。

- e. 對於系統產生的輸出 ，檢視包含的所有欄位。
  - f. 選擇 Next (下一步)。
7. 對於步驟 4：檢閱並建立：
- a. 檢閱您針對先前步驟所做的選擇，並視需要編輯。
  - b. 選擇 Create and run (建立並執行)。

訊息隨即出現，指出已建立相符的工作流程，且任務已開始。

8. 在相符的工作流程詳細資訊頁面上，在指標索引標籤上，檢視上次任務指標 下的下列項目：
- 任務 ID。
  - 相符工作流程任務的狀態：已佇列、進行中、已完成、失敗
  - 工作流程任務的完成時間。
  - 已處理的記錄數目。
  - 未處理的記錄數目。
  - 產生的唯一相符IDs項目。
  - 輸入記錄 的數量。

您也可以檢視先前已在任務歷史記錄 下執行的相符工作流程任務的任務指標。

9. 比對工作流程任務完成後（狀態為 已完成），您可以前往資料輸出索引標籤，然後選擇您的 Amazon S3 位置以檢視結果。

## 編輯相符的工作流程

編輯相符的工作流程可讓您保持實體解析程序，up-to-date並因應組織隨時間變化的需求。您可能想要調整相符條件、技術或資料輸出，以提高實體解析程序的準確性和效率。如果您在目前工作流程的結果中發現問題或錯誤，編輯它可協助您診斷和解決這些問題。

若要編輯相符的工作流程：

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程 下，選擇相符。
3. 選擇相符的工作流程。
4. 在相符的工作流程詳細資訊頁面上的右上角，選擇編輯。
5. 在指定相符的工作流程詳細資訊頁面上，進行任何必要的變更，然後選擇下一步。
6. 在選擇相符的技術頁面上，進行任何必要的變更，然後選擇下一步。
7. 在指定資料輸出頁面上，進行任何必要的變更，然後選擇下一步。
8. 在檢閱並儲存頁面上，進行任何必要的變更，然後選擇儲存。

## 刪除相符的工作流程

如果不再使用相符的工作流程或已過時，刪除它有助於保持工作區井然有序和井然有序。如果您開發了新的改進工作流程來取代舊工作流程，刪除舊工作流程有助於確保您僅使用最多 up-to-date 的流程。

若要刪除相符的工作流程：

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程 下，選擇相符。
3. 選擇相符的工作流程。
4. 在相符的工作流程詳細資訊頁面上的右上角，選擇刪除。
5. 確認刪除，然後選擇刪除。

## 尋找規則型比對工作流程的比對 ID

執行規則型比對工作流程後，您可以找到已處理記錄的對應比對 ID 和相關規則。

若要尋找規則型比對工作流程的比對 ID：

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程 下，選擇相符。
3. 選擇已處理的規則型比對工作流程（工作狀態為 已完成 ）。
4. 在相符的工作流程詳細資訊頁面上，選擇尋找相符的 ID 索引標籤。
5. 執行以下任意一項：

如果 ...	然後 ...
只有一個結構描述映射與此工作流程相關聯。	檢視預設選取的結構描述映射。
有一個以上的結構描述映射與此工作流程相關聯。	從下拉式清單中選擇結構描述映射。

6. 展開相符規則。
7. 為每個相符金鑰 輸入值。

預設會選取標準化資料選項，以便在比對之前標準化資料輸入。如果您不想標準化資料，請取消選取標準化資料選項。

#### Tip

請盡可能輸入更多值，以協助尋找相符 ID。

8. 選擇 Look up (查閱)。
9. 檢視對應的比對 ID 和用於比對的相關規則。

## 從規則型或 ML 型比對工作流程刪除記錄

如果您需要遵守資料管理法規，您可以從規則型或 ML 型比對工作流程中刪除記錄。

從規則型或 ML 型比對工作流程中刪除記錄

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。

2. 在左側導覽窗格中的工作流程下，選擇相符。
3. 選擇規則型或 ML 型比對工作流程。
4. 在相符的工作流程詳細資訊頁面上，從動作下拉式清單中選擇刪除唯一IDs。
5. 在唯一區段中輸入要刪除的唯一 IDs ID。

您最多可以輸入 10 個唯一的 IDs。

6. 指定要從中刪除唯一的輸入來源IDs。

如果工作流程只有一個輸入來源，預設會列出輸入來源。

如果您只指定一個輸入來源，則其他輸入來源IDs中唯一的不會受到影響。

7. 選擇刪除唯一 IDs。

## 疑難排解相符工

使用下列資訊可協助您診斷並修正執行相符工作流程時可能會遇到的常見問題。

### 我在執行相符的工作流程後收到錯誤檔

#### 常見原因

一個相符的工作流程可以有多個執行，而且結果 (成功或錯誤) 會寫入名稱jobId為的資料夾中。

相符工作流程的成功結果會寫入包含多個檔案的success資料夾，且每個檔案都包含成功記錄的子集。

相符工作流程的錯誤會寫入含有多個欄位的error資料夾，每個欄位都包含錯誤記錄的子集。

您可以建立錯誤檔案的原因如下：

- [唯一識別碼](#)是：
  - null
  - 在一行數據中丟失
  - 在數據表中的記錄中丟失
  - 在數據表中的另一行數據重複
  - 未指定
  - 在相同來源中不是唯一的

- 在多個來源中不是唯一的
- 跨來源重疊
- 超過 38 個字元 (僅限於以規則為基礎的相符工作流程)
- [綱要對應](#)中的其中一個欄位包含保留名稱：
  - EmailAddress
  - InputSourceARN
  - MatchRule
  - 匹配 ID
  - HashingProtocol
  - ConfidenceLevel
  - 來源

#### Note

如果由於先前列出的原因而建立錯誤檔案中的記錄，則會向您收取費用，因為這會產生服務的處理成本。如果錯誤檔案中的記錄是因為內部伺服器錯誤，則不會向您收費。

## 解析度

### 若要解決此問題

1. 檢查[唯一 ID](#) 是否有效。

如果[唯一 ID](#) 無效，請更新資料表中的唯一 ID、儲存新資料表、建立新資料架構對映，然後再次執行相符的工作流程。

2. 檢查[綱要對應](#)中的其中一個欄位是否包含保留名稱。

如果其中一個欄位包含保留名稱，請使用新名稱建立新綱要對應，然後再次執行相符的工作流程。

## 使用 ID 映射工作流程映射輸入資料

ID 映射工作流程是一種資料處理任務，它會根據指定的 ID 映射方法，將資料從輸入資料來源映射到輸入資料目標。它會產生 ID 映射表。

ID 映射工作流程需要輸入資料來源和輸入資料目標。您的資料輸入來源和目標取決於您要執行的 ID 映射類型。有兩種方法可執行 ID 映射：規則型或提供者服務：

- 規則型 ID 映射 – 您可以使用相符的規則，將來源中的第一方資料轉換為目標。
- 提供者服務 ID 映射 – 您可以使用 LiveRamp 提供者服務將第三方資料從來源轉譯到目標。

### Note

中的提供者服務 ID 映射工作流程 AWS Entity Resolution 目前與整合 LiveRamp。如果您有 LiveRamp 服務的訂閱，則可以使用 [建立 ID 映射工作流程 LiveRamp](#)，以執行轉碼。透過 LiveRamp 轉碼，您可以將一組來源 R 轉換為 ampIDs 任何目標目的地 RampID。透過使用 RampID 作為權杖來代表客戶，您可以避免直接與廣告平台共用客戶資料。如需詳細資訊，請參閱 LiveRamp 文件網站上的 [執行轉譯ADX](#)。

您可以在下列任一情況下，在兩個資料集之間執行 ID 映射：

- 在您自己的內 AWS 帳戶
- 在兩個不同的 AWS 帳戶

下圖摘要說明如何設定 ID 映射工作流程。



#### Complete prerequisite

Create a [schema mapping](#) for ID mapping in your AWS account or an [ID namespace](#) for ID mapping across AWS accounts to define your data.



#### Specify ID mapping details

Provide details for your ID mapping workflow and choose an ID mapping method.



#### Specify source and target

Use a schema mapping or ID namespace to describe your input data depending on your ID mapping type.



#### Specify data output location - optional

Choose your S3 location to write your data output.

### 主題

- [一個的 ID 映射工作流程 AWS 帳戶](#)

- [跨兩個的 ID 映射工作流程 AWS 帳戶](#)
- [執行 ID 映射工作流程](#)
- [使用新的輸出目的地執行 ID 映射工作流程](#)
- [編輯 ID 映射工作流程](#)
- [刪除 ID 映射工作流程](#)
- [新增或更新 ID 映射工作流程的資源政策](#)

## 一個的 ID 映射工作流程 AWS 帳戶

其中一個的 ID 映射工作流程 AWS 帳戶可讓您在自己的上執行兩個資料集之間的 ID 映射 AWS 帳戶。

在您自己的上建立 ID 映射工作流程之前 AWS 帳戶，您必須先完成[先決條件](#)。

建立並執行 ID 映射工作流程之後，您可以檢視輸出（ID 映射表）並將其用於分析。

下列主題會引導您完成在相同中建立 ID 映射工作流程的一組步驟 AWS 帳戶。

### 主題

- [必要條件](#)
- [建立 ID 映射工作流程（規則型）](#)
- [建立 ID 映射工作流程（提供者服務）](#)

## 必要條件

AWS 帳戶使用規則型或提供者服務 ID 映射方法建立 ID 映射工作流程之前，您必須先執行下列動作：

- 完成[設定AWS實體解析](#)中的任務。
- [建立結構描述映射](#)或[建立相符的工作流程](#)。
- （僅限提供者服務 ID 映射）使用 [建立 ID 映射工作流程之前 LiveRamp](#)，您必須選擇要暫時寫入 ID 映射工作流程輸出的 Amazon Simple Storage Service（Amazon S3）資料暫存儲存貯體。

如果您使用 LiveRamp 提供者服務轉譯第三方資料，請新增下列許可政策，以允許您存取資料暫存儲存貯體。

```
{
  "Version": "2012-10-17",
```

```
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::715724997226:root"
    },
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:GetObjectVersion",
      "s3:DeleteObject"
    ],
    "Resource": [
      "arn:aws:s3:::<staging-bucket>",
      "arn:aws:s3:::<staging-bucket>/*"
    ]
  },
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::715724997226:root"
    },
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation",
      "s3:GetBucketPolicy",
      "s3:ListBucketVersions",
      "s3:GetBucketAcl"
    ],
    "Resource": [
      "arn:aws:s3:::<staging-bucket>",
      "arn:aws:s3:::<staging-bucket>/*"
    ]
  }
]
```

在上述許可政策中，取代每個 *<user input placeholder>* 使用您自己的資訊。

*staging-bucket*

Amazon S3 儲存貯體，可在執行提供者服務型  
工作流程時暫時存放您的資料。

## 建立 ID 映射工作流程（規則型）

本主題描述為使用相符規則將第一方資料從來源轉譯至目標的 ID AWS 帳戶 映射工作流程建立程序。

為 建立規則型 ID 映射工作流程 AWS 帳戶

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程 下，選擇 ID 映射。
3. 在 ID 映射工作流程頁面上的右上角，選擇建立 ID 映射工作流程。
4. 對於步驟 1：指定 ID 映射工作流程詳細資訊，請執行下列動作。
  - a. 輸入 ID 映射工作流程名稱和選用的描述。

- b. 針對 ID 映射方法，選擇規則型。
  - c. （選用）若要為 資源啟用標籤，請選擇新增標籤，然後輸入金鑰和值對。
  - d. 選擇 Next (下一步)。
5. 對於步驟 2：指定來源和目標，請執行下列動作。
  - a. 針對來源，選擇適用於您的案例，然後採取建議的動作。

案例	建議的動作
在 ID AWS 映射工作流程中使用您自己的 AWS Glue 資料庫、Glue 資料表和結構描述映射。	1. 選擇結構描述映射。

案例	建議的動作
	<p>2. 從下拉式清單中選取AWS Glue資料庫，選取AWS Glue 資料表，然後選取對應的結構描述映射。</p> <p>您最多可以新增 19 個資料輸入。</p>
使用現有的比對工作流程，指向您要在 ID 映射工作流程中使用的記錄資料。	<p>1. 選擇相符工作流程。</p> <p>2. 從下拉式清單中選取現有的相符工作流程。</p>

- b. 針對目標，從下拉式清單中選取現有的相符工作流程。
- c. 對於規則參數，請執行下列動作。
  - i. 根據您的來源類型選擇下列其中一個選項，以指定規則控制項。

來源類型	建議的動作
比對工作流程	<p>透過選擇來源、目標或兩者是否可以在 ID 映射工作流程中提供規則來指定規則控制項。</p> <p>規則控制項必須與要在 ID 映射工作流程中使用的來源和目標相容。</p> <p>例如，如果來源 ID 命名空間將規則限制為目標，但目標 ID 命名空間將規則限制為來源，則會導致錯誤。</p>
結構描述映射	跳過此步驟。

- ii. 對於比較和相符參數，比較類型會自動設定為多個輸入欄位。

這是因為兩位參與者先前都已選取此選項。

- d. 根據您的目標選擇下列其中一個選項，以指定記錄比對類型。

您的目標	建議選項
當您建立 ID 映射工作流程時，請限制記錄比對類型，在目標中每個比對記錄的來源中僅存放一個比對記錄。	一個來源到一個目標
限制記錄比對類型，以便在建立 ID 映射工作流程時，將目標中每個比對記錄的所有比對記錄存放在來源中。	一個目標的許多來源

 Note

您必須指定來源和目標 ID 命名空間的相容限制。

- e. 若要指定服務存取許可，請選擇 選項並採取建議的動作。

### Service access

AWS Entity Resolution requires permissions to read your data input from AWS Glue and write to S3 on your behalf. [View policy document](#)

#### Choose a method to authorize AWS Entity Resolution

- Create and use a new service role  
Automatically create the role and add the necessary permissions policy.
- Use an existing service role

#### Service role name

entityresolution-id-mapping-workflow-20240117121045

51 of 64 characters. Use alphanumeric and '+=, @-\_' characters. Don't include spaces. Name must be unique across all roles in the account.

- This data is encrypted with a KMS key  
Specify the associated KMS key to enable AWS Entity Resolution to access each of your data inputs.

選項	建議的動作
建立和使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-id-mapping-workflow- -&lt;timestamp&gt;</code> 。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由KMS金鑰選項加密。然後，輸入用來解密資料輸入的AWS KMS 金鑰。</li> </ul>
使用現有的服務角色	<ol style="list-style-type: none"> <li>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許可，則會顯示角色清單。  如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name ( ARN )。  如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</li> <li>2. 選擇外部連結中的檢視IAM，以檢視服務角色。  根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</li> </ol>

6. 選擇 Next (下一步)。

7. 對於步驟 3：指定資料輸出位置 – 選用，請執行下列動作。

a. 對於資料輸出目的地，請執行下列動作：

i. 選擇資料輸出的 Amazon S3 位置。

- ii. 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰 ARN 或選擇建立 AWS KMS 金鑰。
  - b. 選擇 Next (下一步)。
8. 對於步驟 4：檢閱並建立，執行下列動作。
  - a. 檢閱您針對先前步驟所做的選擇，並視需要加以編輯。
  - b. 選擇 Create (建立)。

訊息隨即出現，指出 ID 映射工作流程已建立。

建立 ID 映射工作流程之後，您就可以[執行 ID 映射工作流程](#)。

## 建立 ID 映射工作流程（提供者服務）

本主題描述 AWS 帳戶使用名為的提供者服務為建立一個 ID 映射工作流程的程序 LiveRamp。使用維護或衍生的 RampIDs 將一組來源 R LiveRamp 轉換為另一組 RampIDs。

為一個建立提供者服務型 ID 映射工作流程 AWS 帳戶

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程下，選擇 ID 映射。
3. 在 ID 映射工作流程頁面上的右上角，選擇建立 ID 映射工作流程。
4. 對於步驟 1：指定 ID 映射工作流程詳細資訊，請執行下列動作。
  - a. 輸入 ID 映射工作流程名稱和選用的描述。

The screenshot shows the AWS Entity Resolution console interface for creating an ID mapping workflow. The breadcrumb navigation at the top reads: AWS Entity Resolution > ID mapping workflows > Create ID mapping workflow. On the left, a vertical progress bar shows four steps: Step 1 (Specify ID mapping workflow details, currently active), Step 2 (Specify source and target), Step 3 - optional (Specify data output location), and Step 4 (Review and create). The main content area is titled 'Specify ID mapping workflow details' with an 'Info' icon. Below the title is the instruction: 'Provide details for your ID mapping workflow and choose an ID mapping method.' The form contains two input fields: 'Name' with the label 'ID mapping workflow name' and a character limit of '0 of 255 characters. Use alphanumeric, underscore (\_), or hyphen (-) characters. Name must be unique across all ID mapping workflows in your account.'; and 'Description - optional' with a character limit of '0 of 255 characters.'

- b. 針對 ID 映射方法，選擇提供者服務。

AWS Entity Resolution 目前提供 LiveRamp 提供者服務作為 ID 映射方法。如果您有的訂閱 LiveRamp，則狀態會顯示為已訂閱。如需如何訂閱的詳細資訊 LiveRamp，請參閱 [步驟 1：訂閱提供者服務 AWS Data Exchange](#)。

**ID mapping method** Info

## /LiveRamp

Currently we are only offering LiveRamp service as an ID mapping method.

**Access to LiveRamp provider subscription**  
✔ **Subscribed**

ⓘ To ensure a successful workflow run, your data input file format and normalization must be aligned with the provider service's guidelines. [Learn more](#) ↗

ⓘ **Note**

確保您的資料輸入檔案格式符合提供者服務的準則。如需 LiveRamp 輸入檔案格式指南的詳細資訊，請參閱 LiveRamp 文件網站上的 [執行轉譯 ADX](#)。

- c. 針對 LiveRamp 組態，輸入下列 LiveRamp 提供的值：

- 用戶端 ID 管理器 ARN
- 用戶端秘密管理員 ARN

**LiveRamp configuration** Info

**Client ID manager ARN**  
 Enter the Client ID manager ARN provided by LiveRamp.

Enter ARN

0 of 2,048 characters.

**Client secret manager ARN**  
 Enter the Client secret manager ARN provided by LiveRamp.

Enter ARN

0 of 2,048 characters.

- d. (選用) 若要為資源啟用標籤，請選擇新增標籤，然後輸入金鑰和值對。

- e. 選擇 Next (下一步)。
5. 對於步驟 2：指定來源和目標，請執行下列動作。
- a. 針對來源，選擇適用於您的案例，然後採取建議的動作。

案例	建議的動作
在 ID AWS 映射工作流程中使用您自己的 AWS Glue 資料庫、Glue 資料表和結構描述映射。	<ol style="list-style-type: none"> <li>1. 選擇結構描述映射。</li> <li>2. 從下拉式清單中選取AWS Glue資料庫，選取AWS Glue 資料表，然後選取對應的結構描述映射。</li> </ol> <p>您最多可以新增 19 個資料輸入。</p>
使用現有的比對工作流程，指向您要在 ID 映射工作流程中使用的記錄資料。	<ol style="list-style-type: none"> <li>1. 選擇相符工作流程。</li> <li>2. 從下拉式清單中選取現有的相符工作流程。</li> </ol>

- b. 針對目標，根據您選擇的 ID 映射方法採取下列其中一個動作。

ID 映射方法	建議的動作
規則型	從下拉式清單中選取現有的相符工作流程。
提供者服務	<p>輸入在目標網域 LiveRamp 中提供，用於轉碼的 LiveRamp 用戶端網域識別符。</p> 

- c. 對於資料暫存，選擇您要暫時寫入 ID 映射工作流程輸出的 Amazon S3 位置。

**Data staging** [Info](#)

Choose the Amazon S3 location for temporarily storing your data while it processes. Your information will not be saved permanently.

**Amazon S3 location**

[View](#)
[Browse S3](#)

- d. 若要指定服務存取許可，請選擇 選項並採取建議的動作。

**Service access**

AWS Entity Resolution requires permissions to read your data input from AWS Glue and write to S3 on your behalf. [View policy document](#)

**Choose a method to authorize AWS Entity Resolution**

- Create and use a new service role  
Automatically create the role and add the necessary permissions policy.
- Use an existing service role

**Service role name**


51 of 64 characters. Use alphanumeric and '+=, @-\_' characters. Don't include spaces. Name must be unique across all roles in the account.

- This data is encrypted with a KMS key  
Specify the associated KMS key to enable AWS Entity Resolution to access each of your data inputs.

選項	建議的動作
建立和使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-id-mapping-workflow-&lt;timestamp&gt;</code>。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由KMS金鑰選項加密。然後，輸入用來解密資料輸入的AWS KMS 金鑰。</li> </ul>

選項	建議的動作
使用現有的服務角色	<p>1. 從下拉式清單中選擇現有的服務角色名稱。</p> <p>如果您有列出角色的許可，則會顯示角色清單。</p> <p>如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name ( ARN )。</p> <p>如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</p> <p>2. 選擇外部連結中的檢視IAM，以檢視服務角色。</p> <p>根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</p>

6. 選擇 Next (下一步)。

7. 對於步驟 3：指定資料輸出位置 – 選用，請執行下列動作。

a. 對於資料輸出目的地，請執行下列動作：

i. 選擇資料輸出的 Amazon S3 位置。

ii. 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰，ARN或選擇建立 AWS KMS 金鑰。

b. 檢視LiveRamp 產生的輸出。

c. 選擇 Next (下一步)。

AWS Entity Resolution > ID mapping workflows > Create ID mapping workflow

Step 1  
Specify ID mapping workflow details

Step 2  
Specify source and target

Step 3 - optional  
**Specify data output location**

Step 4  
Review and create

### Specify data output location - *optional* Info

Choose your S3 location to write your data output.

**Data output destination** Info  
Choose the Amazon S3 location for the data output.

**Amazon S3 location**

Q s3://bucket/prefix View Browse S3

**Encryption - *optional*** Info  
Your data is encrypted by default with a key that AWS owns and manages for you. To specify a different key, customize your encryption settings.

Customize encryption settings  
Specify an AWS KMS key to customize your encryption settings.

▼ **LiveRamp generated output (2)**  
Additional information generated by LiveRamp.

Output field	Description
RAMPID	LiveRamp's universal identifier that is tied to devices in the LiveRamp Identity Graph
TRANSCODED_IDENTIFIER	LiveRamp's universal identifier that is tied to devices in the LiveRamp Identity Graph

Cancel Previous Next

8. 對於步驟 4：檢閱並建立，執行下列動作。
  - a. 檢閱您針對先前步驟所做的選擇，並視需要加以編輯。
  - b. 選擇 Create (建立)。

訊息隨即出現，指出 ID 映射工作流程已建立。

9. 建立 ID 映射工作流程之後，您就可以[執行 ID 映射工作流程](#)。

## 跨兩個的 ID 映射工作流程 AWS 帳戶

跨兩個的 ID 映射工作流程 AWS 帳戶可讓您在兩個的資料集之間執行 ID 映射 AWS 帳戶。這通常在您自己的 AWS 帳戶和另一個之間完成 AWS 帳戶。

例如，發佈者可以使用自己的目標 ID 命名空間（在自己的中 AWS 帳戶）和廣告商的來源 ID 命名空間（在另一個中）來建立 ID 映射工作流程 AWS 帳戶。

在兩個之間建立 ID 映射工作流程之前 AWS 帳戶，您必須先完成[先決條件](#)。

建立 ID 映射工作流程之後，您可以檢視輸出（ID 映射表）並將其用於分析。

下列主題會引導您完成一組步驟，以在兩個之間建立 ID 映射工作流程 AWS 帳戶：

## 主題

- [必要條件](#)
- [建立 ID 映射工作流程（規則型）](#)
- [建立 ID 映射工作流程（提供者服務）](#)

## 必要條件

在兩個之間建立 ID 映射工作流程之前 AWS 帳戶，您必須先執行下列動作：

- 完成 [設定 AWS Entity Resolution](#) 中的任務。
- [建立 ID 命名空間來源](#)。
- [建立 ID 命名空間目標](#)。
- ARN 如果您使用的是來自另一個的 ID 命名空間來源，請取得 ID 命名空間 AWS 帳戶。
- （僅限提供者服務）在兩個之間建立 ID 映射工作流程 AWS 帳戶需要的許可 LiveRamp，才能存取 S3 儲存貯體和 AWS Key Management Service（AWS KMS）客戶受管金鑰。

AWS 帳戶使用跨兩個建立 ID 映射工作流程之前 LiveRamp，請新增下列許可政策，LiveRamp 允許存取 S3 儲存貯體和客戶受管金鑰。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::715724997226:root"
    },
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": "<KMSKeyARN>",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "s3.amazonaws.com"
      }
    }
  ]
}
```

在上述許可政策中，取代每個 `<user input placeholder>` 使用您自己的資訊。

`<KMSKeyARN>`

AWS KMS 客戶受管金鑰ARN的。

## 建立 ID 映射工作流程（規則型）

完成[先決條件](#)後，您可以建立一或多個 ID 映射工作流程，以使用相符規則將第一方資料從來源轉譯到目標。

跨兩個建立規則型 ID 映射工作流程 AWS 帳戶

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程下，選擇 ID 映射。
3. 在 ID 映射工作流程頁面上的右上角，選擇建立 ID 映射工作流程。
4. 對於步驟 1：指定 ID 映射工作流程詳細資訊，請執行下列動作。
  - a. 輸入 ID 映射工作流程名稱和選用的描述。

AWS Entity Resolution > ID mapping workflows > Create ID mapping workflow

Step 1  
Specify ID mapping workflow details

Step 2  
Specify source and target

Step 3 - optional  
Specify data output location

Step 4  
Review and create

### Specify ID mapping workflow details Info

Provide details for your ID mapping workflow and choose an ID mapping method.

**Name**

ID mapping workflow name

Enter name

0 of 255 characters. Use alphanumeric, underscore (\_), or hyphen (-) characters. Name must be unique across all ID mapping workflows in your account.

**Description - optional**

Enter description

0 of 255 characters.

- b. 針對 ID 映射方法，選擇規則型。
  - c. （選用）若要為資源啟用標籤，請選擇新增標籤，然後輸入金鑰和值對。
  - d. 選擇 Next (下一步)。
5. 對於步驟 2：指定來源和目標，請執行下列動作。
    - a. 開啟進階選項。

- b. 針對來源，選擇相符工作流程，然後從下拉式清單中選取現有的相符工作流程。
- c. 針對目標，選擇相符工作流程，然後從下拉式清單中選取現有的相符工作流程。
- d. 對於規則參數，選擇來源或目標是否可以在 ID 映射工作流程中提供規則，以指定規則控制項。

規則控制項必須與要在 ID 映射工作流程中使用的來源和目標相容。例如，如果來源 ID 命名空間將規則限制為目標，但目標 ID 命名空間將規則限制為來源，則會導致錯誤。

- e. 對於比較和比對參數，請執行下列動作。
  - i. 根據您的目標選擇選項來指定比較類型。

您的目標	建議選項
尋找儲存在多個輸入欄位中資料的比對組合，無論資料是否位於相同或不同的輸入欄位中。	多個輸入欄位
不應比對跨多個輸入欄位存放的類似資料時，限制單一輸入欄位內的比較。	單一輸入欄位

- ii. 根據您的目標選擇選項來指定記錄比對類型。

您的目標	建議選項
當您建立 ID 映射工作流程時，請限制記錄比對類型，在目標中每個比對記錄的來源中僅存放一個比對記錄。	一個來源到一個目標
限制記錄比對類型，以便在建立 ID 映射工作流程時，將目標中每個比對記錄的所有比對記錄存放在來源中。	一個目標的許多來源

**Note**

您必須指定來源和目標 ID 命名空間的相容限制。

- f. 若要指定服務存取許可，請選擇 選項並採取建議的動作。

### Service access

AWS Entity Resolution requires permissions to read your data input from AWS Glue and write to S3 on your behalf. [View policy document](#)

#### Choose a method to authorize AWS Entity Resolution

- Create and use a new service role  
Automatically create the role and add the necessary permissions policy.
- Use an existing service role

#### Service role name

entityresolution-id-mapping-workflow-20240117121045

51 of 64 characters. Use alphanumeric and '+=, @-\_' characters. Don't include spaces. Name must be unique across all roles in the account.

- This data is encrypted with a KMS key  
Specify the associated KMS key to enable AWS Entity Resolution to access each of your data inputs.

選項	建議的動作
<p>建立和使用新的服務角色</p>	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-id-mapping-workflow- -&lt;timestamp&gt;</code>。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由KMS金鑰選項加密。然後，輸入用來解密資料輸入的AWS KMS 金鑰。</li> </ul>

選項	建議的動作
使用現有的服務角色	<p>1. 從下拉式清單中選擇現有的服務角色名稱。</p> <p>如果您有列出角色的許可，則會顯示角色清單。</p> <p>如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name ( ARN )。</p> <p>如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</p> <p>2. 選擇外部連結中的檢視IAM，以檢視服務角色。</p> <p>根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</p>

6. 選擇 Next (下一步)。
7. 對於步驟 3：指定資料輸出位置 – 選用，請執行下列動作。
  - a. 對於資料輸出目的地，請執行下列動作。
    - i. 選擇資料輸出的 Amazon S3 位置。
    - ii. 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰ARN或選擇建立 AWS KMS 金鑰。
  - b. 檢視LiveRamp 產生的輸出。
  - c. 選擇 Next (下一步)。
8. 對於步驟 4：檢閱並建立，執行下列動作。
  - a. 檢閱您針對先前步驟所做的選擇，並視需要加以編輯。
  - b. 選擇 Create (建立)。

訊息隨即出現，指出 ID 映射工作流程已建立。

建立 ID 映射工作流程之後，您就可以[執行 ID 映射工作流程](#)。

## 建立 ID 映射工作流程（提供者服務）

完成[先決條件](#)後，您可以使用 LiveRamp 提供者服務建立一或多個 ID 映射工作流程。會使用維護或衍生的 R ampIDs 將一組來源 R LiveRamp 轉換為另一組 ampIDs。

使用提供者服務建立 ID 映射工作流程

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程下，選擇 ID 映射。
3. 在 ID 映射工作流程頁面上的右上角，選擇建立 ID 映射工作流程。
4. 對於步驟 1：指定 ID 映射工作流程詳細資訊，請執行下列動作。
  - a. 輸入 ID 映射工作流程名稱和選用的描述。

AWS Entity Resolution > ID mapping workflows > Create ID mapping workflow

Step 1  
Specify ID mapping workflow details

Step 2  
Specify source and target

Step 3 - optional  
Specify data output location

Step 4  
Review and create

### Specify ID mapping workflow details Info

Provide details for your ID mapping workflow and choose an ID mapping method.

**Name**

ID mapping workflow name

Enter name

0 of 255 characters. Use alphanumeric, underscore (\_), or hyphen (-) characters. Name must be unique across all ID mapping workflows in your account.

**Description - optional**

Enter description

0 of 255 characters.

- b. 針對 ID 映射方法，選擇提供者服務。

AWS Entity Resolution 目前提供 LiveRamp 提供者服務作為 ID 映射方法。如果您有的訂閱 LiveRamp，則狀態會顯示為已訂閱。如需如何訂閱的詳細資訊 LiveRamp，請參閱[步驟 1：訂閱提供者服務 AWS Data Exchange](#)。

ID mapping method [Info](#)

# /LiveRamp

Currently we are only offering LiveRamp service as an ID mapping method.

## Access to LiveRamp provider subscription

 Subscribed

 To ensure a successful workflow run, your data input file format and normalization must be aligned with the provider service's guidelines. [Learn more](#) 

**Note**

確保您的資料輸入檔案格式符合提供者服務的準則。如需 LiveRamp 輸入檔案格式指南的詳細資訊，請參閱 LiveRamp 文件網站上的 [執行轉譯ADX](#)。

c. 針對 LiveRamp 組態，輸入下列 LiveRamp 提供的值：

- 用戶端 ID 管理器 ARN
- 用戶端秘密管理員 ARN

LiveRamp configuration [Info](#)

## Client ID manager ARN

Enter the Client ID manager ARN provided by LiveRamp.

0 of 2,048 characters.

## Client secret manager ARN

Enter the Client secret manager ARN provided by LiveRamp.

0 of 2,048 characters.

d. (選用) 若要為資源啟用標籤，請選擇新增標籤，然後輸入金鑰和值對。

e. 選擇 Next (下一步)。

5. 對於步驟 2：指定來源和目標，請執行下列動作。

- 開啟進階選項。
- 針對來源，選擇 ID 命名空間。

AWS Entity Resolution > ID mapping workflows > Create ID mapping workflow

Step 1  
Specify ID mapping workflow details

Step 2  
**Specify source and target**

Step 3 - optional  
Specify data output location

Step 4  
Review and create

## Specify source and target Info

Use a schema mapping or ID namespace to describe your input data depending on your ID mapping type.

**Advanced options**  
Use advanced options if you are creating an ID mapping across AWS accounts and have created ID namespace resources to manage AWS account permissions.

### Source Info

The source of the data in an ID mapping workflow.

**Schema mapping**  
Use AWS Glue database, AWS Glue table, and schema mapping for ID mapping on your own AWS account.

**ID namespace**  
Use an ID namespace to describe your source data for ID mapping across two AWS accounts.

### ID namespace Info

Choose an AWS account associated with the ID namespace source. [Create ID namespace](#)

**Your AWS account**  
 Another AWS account

**Your ID namespaces**

Select ID namespace ▼

- c. 針對 ID 命名空間，識別 ID 命名空間所在的位置，然後採取建議的動作。

ID 命名空間的位置	建議的動作
您自己的 AWS 帳戶	<ol style="list-style-type: none"> <li>選擇您的 AWS 帳戶。</li> <li>從您的 ID 命名空間下拉式清單中選取 ID 命名空間。</li> </ol>
其他人的 AWS 帳戶	<ol style="list-style-type: none"> <li>選擇另一個 AWS 帳戶。</li> <li>輸入 ID 命名空間 ARN。</li> </ol>

- d. 針對目標，選擇 ID 命名空間。

**Target** [Info](#)  
Select how you want to provide the domain to which you want to translate your data using ID mapping.

**Domain**  
Provide a specific target domain to which you want to translate the data to

**ID namespace**  
Use an ID namespace to describe your target configuration for ID mapping across two AWS accounts.

**ID namespace** [Info](#)  
Choose an AWS account associated with the ID namespace source. [Create ID namespace](#)

Your AWS account  
 Another AWS account

**Your ID namespaces**

- e. 若要指定服務存取權限，請選擇 選項並採取建議的動作。

**Service access**  
AWS Entity Resolution requires permissions to read your data input from AWS Glue and write to S3 on your behalf. [View policy document](#)

**Choose a method to authorize AWS Entity Resolution**

Create and use a new service role  
Automatically create the role and add the necessary permissions policy.

Use an existing service role

**Service role name**

51 of 64 characters. Use alphanumeric and '+=, @-\_' characters. Don't include spaces. Name must be unique across all roles in the account.

This data is encrypted with a KMS key  
Specify the associated KMS key to enable AWS Entity Resolution to access each of your data inputs.

選項	建議的動作
建立和使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-id-mapping-workflow- -&lt;timestamp&gt;</code> 。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由KMS金鑰選項加密。然後，輸入用來解密資料輸入的AWS KMS 金鑰。</li> </ul>
使用現有的服務角色	<ol style="list-style-type: none"> <li>1. 從下拉式清單中選擇現有的服務角色名稱。 <ul style="list-style-type: none"> <li>如果您有列出角色的許可，則會顯示角色清單。</li> <li>如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name ( ARN ) 。</li> <li>如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</li> </ul> </li> <li>2. 選擇外部連結中的檢視IAM，以檢視服務角色。 <ul style="list-style-type: none"> <li>根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</li> </ul> </li> </ol>

6. 選擇 Next (下一步)。

7. 對於步驟 3：指定資料輸出位置 – 選用，請執行下列動作。

a. 對於資料輸出目的地，請執行下列動作。

i. 選擇資料輸出的 Amazon S3 位置。

- ii. 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰，ARN或選擇建立 AWS KMS 金鑰。
- b. 檢視LiveRamp 產生的輸出。
- c. 選擇 Next (下一步)。

AWS Entity Resolution > ID mapping workflows > Create ID mapping workflow

Step 1 Specify ID mapping workflow details

Step 2 Specify source and target

Step 3 - optional Specify data output location

Step 4 Review and create

### Specify data output location - optional Info

Choose your S3 location to write your data output.

**Data output destination Info**  
Choose the Amazon S3 location for the data output.

**Amazon S3 location**

Q s3://bucket/prefix View Browse S3

**Encryption - optional Info**  
Your data is encrypted by default with a key that AWS owns and manages for you. To specify a different key, customize your encryption settings.

Customize encryption settings  
Specify an AWS KMS key to customize your encryption settings.

▼ **LiveRamp generated output (2)**  
Additional information generated by LiveRamp.

Output field	Description
RAMPID	LiveRamp's universal identifier that is tied to devices in the LiveRamp Identity Graph
TRANSCODED_IDENTIFIER	LiveRamp's universal identifier that is tied to devices in the LiveRamp Identity Graph

Cancel Previous Next

8. 對於步驟 4：檢閱並建立，執行下列動作。
  - a. 檢閱您針對先前步驟所做的選擇，並視需要加以編輯。
  - b. 選擇 Create (建立)。

訊息隨即出現，指出 ID 映射工作流程已建立。

建立 ID 映射工作流程之後，您就可以[執行 ID 映射工作流程](#)。

## 執行 ID 映射工作流程

為一個 [建立 ID 映射工作流程 AWS 帳戶](#) 或跨兩個 [建立 ID 映射工作流程 AWS 帳戶](#) 後，您可以執行 ID 映射工作流程。ID 映射工作流程會輸出 CSV 檔案。

## 執行 ID 映射工作流程

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程 下，選擇 ID 映射。
3. 選擇 ID 映射工作流程。
4. 在 ID 映射工作流程詳細資訊頁面上的右上角，選擇執行。
5. 在相符的工作流程詳細資訊頁面上，在指標索引標籤上，檢視上次任務指標 下的下列項目：
  - 任務 ID
  - 工作流程任務的完成時間
  - 相符工作流程任務的狀態：已佇列、進行中、已完成、失敗
  - 處理的記錄數目
  - 未處理的記錄數目
  - 輸入記錄的數量

在任務歷史記錄 下，您也可以檢視先前執行的 ID 映射工作流程任務的任務指標。

6. ID 映射工作流程任務完成後（狀態已完成），選擇 資料輸出，然後選擇您的 Amazon S3 位置以檢視結果。

取得 CSV 檔案後，您可以使用 加入 RAMPID\_TRANSCODED\_ID。

## 使用新的輸出目的地執行 ID 映射工作流程

為一個 [建立 ID 映射工作流程 AWS 帳戶](#) 或 [跨兩個 建立 ID 映射工作流程 AWS 帳戶](#) 後，您可以選擇不同的 S3 位置來寫入資料輸出。

### 使用新的輸出目的地執行 ID 映射工作流程

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程 下，選擇 ID 映射。
3. 選擇 ID 映射工作流程。
4. 在 ID 映射工作流程詳細資訊頁面上的右上角，從執行工作流程下拉式清單中選擇使用新輸出目的地執行。

5. 對於資料輸出目的地，請執行下列動作。
  - a. 選擇資料輸出的 Amazon S3 位置。
  - b. 對於加密，如果您選擇自訂加密設定，請輸入 AWS KMS 金鑰，ARN或選擇建立 AWS KMS 金鑰。
6. 若要指定服務存取許可，請選擇 選項並採取建議的動作。

選項	建議的動作
建立和使用新的服務角色	<ul style="list-style-type: none"> <li>• AWS Entity Resolution 會建立具有此資料表所需政策的服務角色。</li> <li>• 預設的服務角色名稱為 <code>entityresolution-id-mapping-workflow- &lt;timestamp&gt;</code>。</li> <li>• 您必須具有建立角色和連接政策的許可。</li> <li>• 如果您的輸入資料已加密，請選擇此資料由 KMS金鑰選項加密。然後，輸入用來解密資料輸入的AWS KMS 金鑰。</li> </ul>
使用現有的服務角色	<ol style="list-style-type: none"> <li>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許可，則會顯示角色清單。  如果您沒有列出角色的許可，您可以輸入要使用的角色的 Amazon Resource Name ( ARN )。  如果沒有現有的服務角色，則無法使用使用現有服務角色的選項。</li> <li>2. 選擇外部連結中的檢視IAM，以檢視服務角色。  根據預設，AWS Entity Resolution 不會嘗試更新現有的角色政策來新增必要的許可。</li> </ol>

7. 選擇執行。

8. 在相符的工作流程詳細資訊頁面上，在指標索引標籤上，檢視上次任務指標 下的下列項目：

- 任務 ID
- 工作流程任務的完成時間
- 相符工作流程任務的狀態：已佇列、進行中、已完成、失敗
- 處理的記錄數目
- 未處理的記錄數目
- 輸入記錄的數量

在任務歷史記錄 下，您也可以檢視先前執行的 ID 映射工作流程任務的任務指標。

9. ID 映射工作流程任務完成後（狀態已完成），選擇 資料輸出，然後選擇您的 Amazon S3 位置以檢視結果。

取得 CSV 檔案後，您可以使用 加入 RAMPID TRANSCODED\_ID。

## 編輯 ID 映射工作流程

編輯 ID 映射工作流程可讓您保持實體解析功能 up-to-date，並隨著時間的推移與不斷變化的業務需求保持一致。您可能想要調整映射規則、技術和參數，您可以最佳化工作流程，以提供更準確且可靠的 ID 比對結果。您也可以新增資料來源、展開 IDs 要映射的類型，或將其他相符條件納入工作流程。如果您發現 ID 映射結果中的問題或錯誤，使用工作流程編輯可協助您診斷和解決這些問題。

若要編輯 ID 映射工作流程：

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟 [AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程 下，選擇 ID 映射。
3. 選擇 ID 映射工作流程。
4. 在 ID 映射工作流程詳細資訊頁面上的右上角，選擇編輯。
5. 在指定 ID 映射工作流程詳細資訊頁面上，進行任何必要的變更，然後選擇下一步。
6. 在指定資料輸出頁面上，進行任何必要的變更，然後選擇下一步。
7. 在檢閱並儲存頁面上，進行任何必要的變更，然後選擇儲存。

## 刪除 ID 映射工作流程

如果您不再使用 ID 映射工作流程，刪除它有助於簡化工作流程管理。此外，刪除提供類似用途的多餘或效率較低的 ID 映射工作流程，可協助您合併程序。

若要刪除 ID 映射工作流程：

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程下，選擇 ID 映射。
3. 選擇 ID 映射工作流程。
4. 在 ID 映射工作流程詳細資訊頁面上的右上角，選擇刪除。
5. 確認刪除，然後選擇刪除。

## 新增或更新 ID 映射工作流程的資源政策

資源政策允許 ID 映射資源的建立者存取您的 ID 映射工作流程資源。

新增或更新資源政策

1. 如果您尚未登入 AWS 帳戶，請使用 AWS Management Console 開啟[AWS Entity Resolution 主控台](#)。
2. 在左側導覽窗格中的工作流程下，選擇 ID 映射。
3. 選擇 ID 映射工作流程。
4. 在 ID 映射工作流程詳細資訊頁面上，選擇許可索引標籤。
5. 在資源政策中，區段選擇編輯。
6. 在JSON編輯器中新增或更新政策。
7. 選擇 Save changes (儲存變更)。

# 與整合 AWS Entity Resolution 作為提供者

AWS Entity Resolution 第三方供應商整合可協助客戶保護消費者隱私，並維持遵守資料主權法規。第三方供應商，例如 LiveRamp 和 TransUnion，將消費者識別碼轉換為廣告IDs，例如 Ramp IDs 和 Fabrick IDs。這些廣告標識符通常用於廣告和營銷工具，以防止消費者數據導出到非-AWS 管理系統。本節為供應商提供與之整合的指引 AWS Entity Resolution 將消費者識別碼編碼或轉碼IDs為廣告，以便在[供應商服務型比對](#)工作流程中使用。

如需有關目前與之整合的提供者服務的詳細資訊 AWS Entity Resolution，請參閱[建立提供者服務型比對工作流程](#)。

## 主題

- [要求](#)
- [使用 AWS Entity Resolution 開放API規格](#)
- [測試提供者整合](#)

## 要求

在整合為提供者服務之前 AWS Entity Resolution，完成下列需求。

## 主題

- [列出提供者服務 AWS Data Exchange](#)
- [識別您的屬性](#)
- [請求 AWS Entity Resolution 開放API規格](#)

## 列出提供者服務 AWS Data Exchange

身為第三方供應商，您必須在「[AWSData Exchange](#)」(ADX) 產品目錄中列出產品。在您的產品上列出之後 AWS Data Exchange 產品目錄，訂閱者可以通過公開或私人報價訂閱您的產品。

若要列出提供者服務 AWS Data Exchange

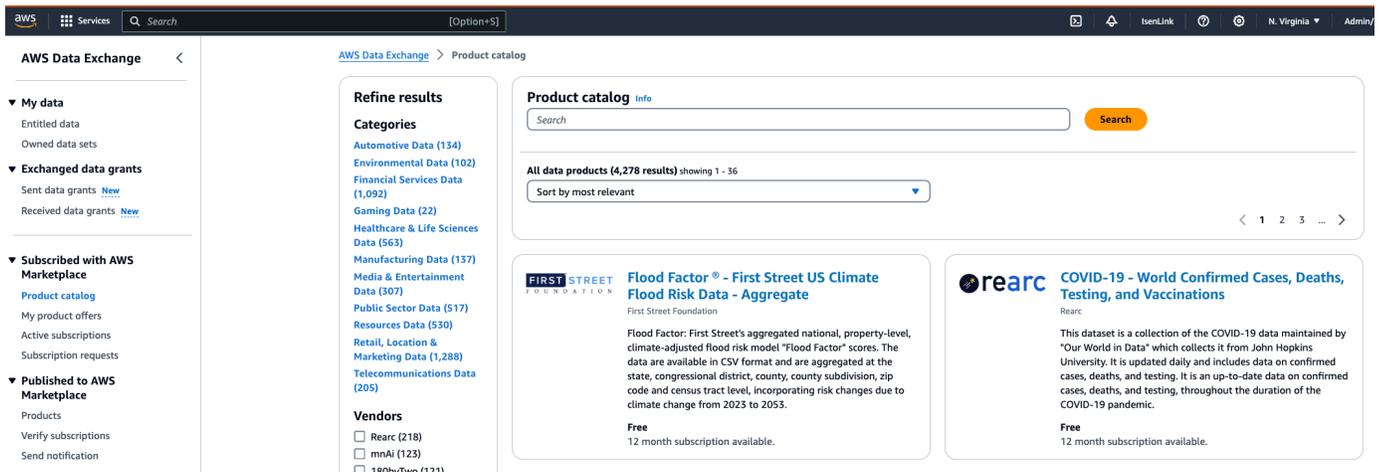
1. 如果您是新的資料產品提供者 AWS Data Exchange，完成「以[提供者身分入門](#)」一節中的步驟 AWS Data Exchange 用戶指南。

2. 建立RESTAPI資料集並發佈包含APIs的新產品 AWS Data Exchange 遵循「[如何發佈](#)」中包含的[產品](#)一節APIs中的步驟 AWS Data Exchange 用戶指南。您可以使用 AWS Data Exchange 主控台或 AWS Command Line Interface。

如果您已將產品可見度設定為「公開」，則所有訂閱者都可以使用公開方案。

如果您已將產品可見度設定為「私人」，請完成「[建立自訂選件](#)」一節中的步驟 AWS Data Exchange 使用者指南，視您的使用案例而定。

下圖顯示了中可用產品的範例 AWS Data Exchange 產品目錄。



3. 在產品上可用之後 AWS Data Exchange 產品目錄，用戶可以通過以下方式訂閱產品。

- 訂閱公開產品。
- 使用由[提供者服務核發](#)的不公開優惠 (自訂選件)。
- 使用[自攜訂閱 \(BYOS\)](#) 優惠。

如需詳細資訊，請參閱[訂閱和存取APIs中包含的產品](#) AWS Data Exchange 用戶指南。

## 識別您的屬性

輸入資料的屬性是要在工作流程中解析之實體的類型定義。屬性的一些範例為FirstNameLastName、Email、或Custom String。

當您識別屬性時，您應該注意任何要求或準則。

## Example 範例

以下是識別提供者屬性的驗證範例。

- FirstName或LastName屬性是強制性的。
- 如果該Email屬性存在，則必須對其進行散列。

身為提供者，您必須識別提供者服務產品中的屬性，然後將這些屬性傳達給 AWS Entity Resolution <aws-entity-resolution-bd@amazon .com> 的業務開發團隊在繼續之前進行其他驗證。

## 請求 AWS Entity Resolution 開放API規格

AWS Entity Resolution 具有 Open API 規格，您作為提供者可以用作包含與整合APIs相關的握手。如需詳細資訊，請參閱[使用 AWS Entity Resolution 開放API規格](#)。

若要要求開啟API定義，請連絡 AWS Entity Resolution 企業發展團隊，<### aws-entity-resolution-bd @amazon>。

## 使用 AWS Entity Resolution 開放API規格

Open API 規範定義了與相關聯的所有協議 AWS Entity Resolution。此規範對於實作整合是必要的。

「開啟」API 定義包含下列API作業：

- POST AssignIdentities
- POST CreateJob
- GET GetJob
- POST StartJob
- POST MapIdentities
- GET Schema

若要索取「開啟」API 規格，請連絡 AWS Entity Resolution 企業發展團隊，<### aws-entity-resolution-bd @amazon>。

Open API 規格支援兩種整合類型，用於編碼和轉碼消費者識別碼批次處理和同步處理。取得 Open API 規格之後，請針對您的使用案例實作處理整合類型。

## 主題

- [Batch 處理整合](#)
- [同步處理整合](#)

## Batch 處理整合

批次處理整合遵循非同步設計模式。在啟動工作流程之後 AWS Data Exchange，它會透過提供者整合端點提交工作，然後工作流程透過定期輪詢工作狀態來等待此工作完成。對於可能需要更長時間且提供者輸送量較低的工作執行，此解決方案更為理想。供應商將資料集位置以 Amazon S3 連結的形式取得，他們可以在結束時處理該連結，並將結果寫入預先確定的輸出 S3 位置。

使用三個API定義啟用批次處理整合。AWS Entity Resolution 將調用可通過以下方式獲得的提供程序端點 AWS Data Exchange 按以下順序：

1. POST CreateJob：此API作業會將工單資訊提交給提供者以進行處理。這些資訊與工作類型有關；編碼或轉碼、S3 位置、客戶提供的結構描述，以及任何所需的其他工作屬性。

這會API傳回一個JobId，且「Job 狀態」將會是下列其中一項：PENDINGREADYIN\_PROGRESS、COMPLETE、或FAILED。

### 編碼請求示例

```
POST /jobs
{
  "actionType": "ID_ASSIGNMENT",
  "s3SourceLocation": "string",
  "s3TargetLocation": "string",
  "jobProperties": {
    "assignmentJobProperties": {
      "fieldMappings": [
        {
          "name": "string",
          "type": "NAME"
        }
      ]
    }
  },
  "customerSpecifiedJobProperties": {
    "property1": "string",
    "property2": "string"
  },
  "outputSourceConfiguration": {
```

```
"KMSArn": "string"
}
}
```

### 回應範例

```
{
  "jobId": "string",
  "status": "PENDING"
}
```

2. POST StartJob : 這API可讓提供者知道根據JobId提供的開始工作。這允許提供者執行從CreateJob到之前StartJob所需的任何驗證。

這將API返回一個JobId , Status對於 JobstatusMessage , 和statusCode。

### 編碼請求示例

```
POST/jobs/{jobId}
{
  "customerSpecifiedJobProperties": {
    "property1": "string",
    "property2": "string"
  }
}
```

### 回應範例

```
{
  "jobId": "string",
  "status": "PENDING",
  "statusMessage": "string",
  "statusCode": 200
}
```

3. GET GetJob : 這API通知 AWS Entity Resolution 工作已完成或任何其他狀態。

這將API返回一個JobId , Status對於 JobstatusMessage , 和statusCode。

### 編碼請求示例

```
GET /jobs/{jobId}
```

## 回應範例

```
{
  "jobId": "string",
  "status": "PENDING",
  "statusMessage": "string",
  "statusCode": 200
}
```

這些APIs的完整定義在 [AWS Entity Resolution 開放式API規格](#)。

## 同步處理整合

同步處理解決方案對於具有接近即時回應時間、即時回應時間、較高輸送量和更高輸送量的供應商而言，更為理想TPS。這一個 AWS Entity Resolution 工作流程會分割資料集，parallel 同時提出多個API要求。所以此 AWS Entity Resolution 工作流程然後處理將結果寫入所需的輸出位置。

使用其中一個API定義啟用此程序。AWS Entity Resolution 調用可通過以下方式獲得的提供者端點 AWS Data Exchange:

POST AssignIdentities : 這API會使用source\_id識別碼將資料傳送至提供者，並recordFields與該記錄相關聯。

這將API返回assignedRecords.

## 編碼請求示例

```
POST /assignment
{
  "sourceRecords": [
    {
      "sourceId": "string",
      "recordFields": [
        {
          "name": "string",
          "type": "NAME",
          "value": "string"
        }
      ]
    }
  ]
}
```

```

    }
  ]
}
]
}

```

## 回應範例

```

{
  "assignedRecords": [
    {
      "sourceRecord": {
        "sourceId": "string",
        "recordFields": [
          {
            "name": "string",
            "type": "NAME",
            "value": "string"
          }
        ]
      },
      "identity": any
    }
  ]
}

```

這些APIs的完整定義在 [AWS Entity Resolution 開放式API規格](#)。

根據供應商選擇的方法，AWS Entity Resolution 將為將用於啟動編碼或轉碼的提供者創建一個配置。此外，使用APIs提供的客戶也可以使用這些組態 AWS Entity Resolution。

可使用 Amazon 資源名稱 (ARN) 存取此組態，該名稱衍生自提供者服務供應商的位置 AWS Data Exchange 託管，以及提供者服務的類型。AWS Entity Resolution 這稱之ARN 為providerServiceARN。

## 測試提供者整合

雖然 AWS Entity Resolution 託管數據匹配服務，提供商集成是 end-to-end 匹配工作流程的關鍵第三方組件。有幾個測試 AWS Entity Resolution 已針對在此整合失敗時增加保護的提供者定義。這種方法為供應商提供了根據這些 end-to-end 測試案例監視其服務健康狀態的機會。

提供者可以使用其測試帳戶和自己的資料來執行這些 end-to-end 測試案例 AWS Entity Resolution 軟體開發套件 (SDK)。如果提供商有任何問題，AWS Entity Resolution 使用首選的升級路徑來升級問題。此外，提供者還需要對測試結果實施自己的監控。供應商需要分享他們的 AWS 帳戶 IDs 用於運行這些測試 AWS Entity Resolution。

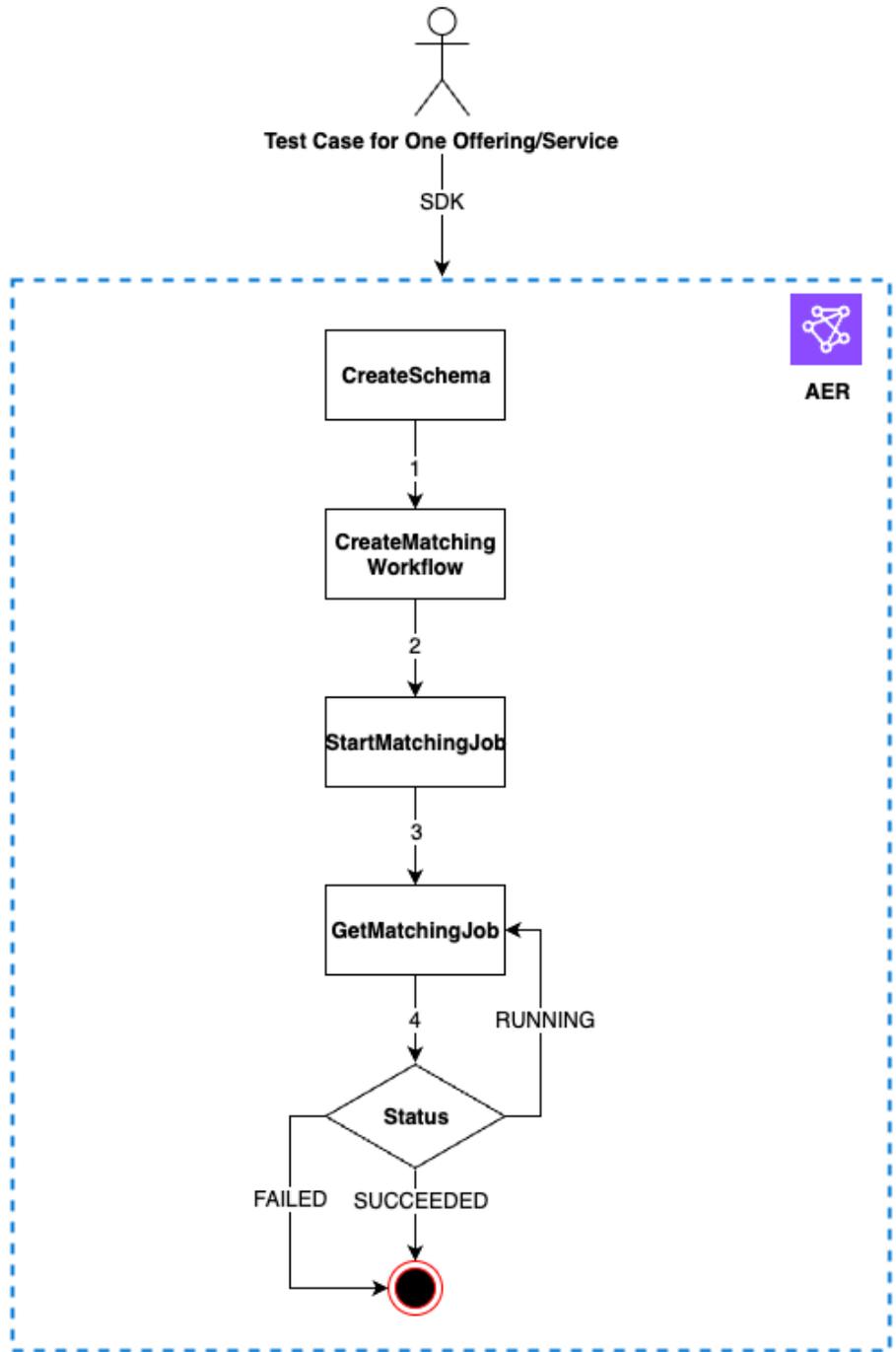
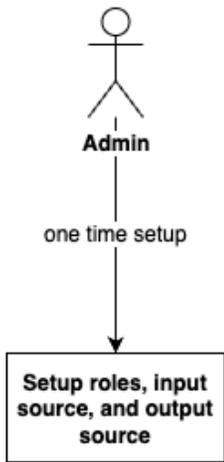
成功運行意味著提供者可以通過以下方式設置其數據，使用自己的服務 AWS Entity Resolution，且工作狀態會傳回「已完成」，但沒有錯誤。這可以通過使用 APIs 提供的以編程方式完成 AWS Entity Resolution。

例如，提供者可以根據其服務設定其 S3 儲存貯體、輸入來源、角色、結構描述和工作流程。完成這些設定後，提供者可以每天執行一次這些工作流程，其中包含 200 筆記錄來測試其服務。在這種方法中，提供者會使用他們選擇的服務 SDK 並對其提供的服務進行 end-to-end 測試 AWS Data Exchange 使用他們的測試帳戶。提供者應為其每個產品或服務執行這些測試。

#### Note

供應商需要提供 AWS Entity Resolution 該 AWS 帳戶 ID (它們 `accountId`) 用來執行這些工作流程以進行測試。此外，提供者需要監視這些測試並確保它們通過，這意味著提供者需要在失敗的情況下啟用通知，以相應地解決問題。

下圖顯示典型的 end-to-end 工作流程測試案例。



若要測試提供者整合

1. (一次性設定) 設定資源 AWS Entity Resolution 遵循中的程序 [設定 AWS Entity Resolution](#)。

完成一次性設定程序之後，您應該準備好角色、資料和資料來源。您現在可以使用以下任一項來測試提供者整合 AWS Entity Resolution 控制台或APIs。

2. 使用測試提供者整合 AWS Entity Resolution APIs或控制台。

## API

若要使用測試提供者整合 AWS Entity Resolution APIs

1. 使用建立綱要對應 [CreateSchemaMapping API](#)。如需受支援程式設計語言的完整清單，請參閱的 [〈另請參閱〉](#) 一節 [CreateSchemaMapping API](#)。

模式映射是您告訴的過程 AWS Entity Resolution 如何解釋您的數據以進行匹配。您可以定義要「AWS實體解析」讀入相符工作流程的輸入資料表的結構描述。

建立結構描述對應時，必須指定 [唯一識別碼](#)，並將其指派給「AWS實體解析」讀取的每一列輸入資料。例如 Primary\_key、Row\_ID、Record\_ID。

Example 為包含 **id** 和的資料來源建立結構描述對映 **email**

以下是包含 **id** 和的資料來源的結構描述對映範例 **email**：

```
[
  {
    "fieldName": "id",
    "type": "UNIQUE_ID"
  },
  {
    "fieldName": "email",
    "type": "EMAIL_ADDRESS"
  }
]
```

Example 為包含 **id** 和 **email** 使用 Java 的資料來源建立結構描述對映 SDK

以下是包含 **id** 並 **email** 使用 Java 之資料來源的結構描述對映範例 SDK：

```
EntityResolutionClient.createSchemaMapping(
    CreateSchemaMappingRequest.builder()
        .schemaName(<schema-name>)
        .mappedInputFields([
```

```

SchemaInputAttribute.builder().fieldName("id").type("UNIQUE_ID").build(),
SchemaInputAttribute.builder().fieldName("email").type("EMAIL_ADDRESS").build()
    ])
    .build()
)

```

2. 使用建立相符的工作流程 [CreateMatchingWorkflow API](#)。如需受支援程式設計語言的完整清單，請參閱的 [〈另請參閱〉](#) 一節 [CreateMatchingWorkflow API](#)。

Example 使用 Java 創建匹配的工作流程 SDK

以下是使用 Java 的匹配工作流程的示例 SDK：

```

EntityResolutionClient.createMatchingWorkflow(
    CreateMatchingWorkflowRequest.builder()
        .workflowName(<workflow-name>)
        .inputSourceConfig(
            InputSource.builder().inputSourceARN(<glue-inputsource-from-
            step1>).schemaName(<schema-name-from-step2>).build()
        )
        .outputSourceConfig(OutputSource.builder().outputS3Path(<output-s3-
        path>).output(<output-1>, <output-2>, <output-3>).build())
        .resolutionTechniques(ResolutionTechniques.builder()
            .resolutionType(PROVIDER)
            .providerProperties(ProviderProperties.builder()
                .providerServiceArn(<provider-arn>)
                .providerConfiguration(<configuration-
                depending-on-service>)
            .intermediateSourceConfiguration(<intermedaite-s3-path>)
            .build())
    )
)

```

```
.build()
                                .roleArn(<role-from-step1>)
                                .build()
)
```

設定相符的工作流程後，您可以執行工作流程。

3. 使用執行相符的工作流程 [StartMatchingJob API](#)。若要執行相符的工作流程，您必須使用 `CreateMatchingWorkflow` 端點建立相符的工作流程。

如需受支援程式設計語言的完整清單，請參閱的 [〈另請參閱〉](#) 一節 [StartMatchingJob API](#)。

Example 使用 Java 執行相符的工作流程 SDK

以下是使用 Java 執行相符工作流程的範例 SDK：

```
EntityResolutionClient.startMatchingJob(StartMatchingJobRequest.builder()
    .workflowName(<name-of-workflow-from-step3>)
    .build()
)
```

4. 使用監視工作流程的狀態 [GetMatchingJob API](#)。

這會API傳回與工作相關聯的狀態、測量結果和錯誤 (如果有的話)。

Example 使用 Java 監視相符的工作流程 SDK

以下是使用 Java 監視相符工作流程工作的範例 SDK：

```
EntityResolutionClient.getMatchingJob(GetMatchingJobRequest.builder()
    .workflowName(<name-of-workflow-from-step3>)
    .jobId(jobId-from-startMatchingJob)
    .build()
)
```

如果工作流程已成功完成，則 end-to-end 測試完成。

## Console

若要使用測試提供者整合 AWS Entity Resolution 主控台

1. 依照中的步驟建立綱要對應[建立綱要對應](#)。

模式映射是您告訴的過程 AWS Entity Resolution 如何解釋您的數據以進行匹配。您可以定義所需的輸入資料表的結構描述 AWS Entity Resolution 以讀取相符的工作流程。

建立綱要對應時，必須指定[唯一識別碼](#)，並將其指派給每一列輸入資料，AWS Entity Resolution 讀取。例如 Primary\_key、Row\_ID、Record\_ID。

Example 包含id和的資料來源的結構描述對映 **email**

以下是包含id和的資料來源的結構描述對映範例email：

```
[
  {
    "fieldName": "id",
    "type": "UNIQUE_ID"
  },
  {
    "fieldName": "email",
    "type": "EMAIL_ADDRESS"
  }
]
```

2. 依照中的步驟建立並執行相符的工作流程[建立提供者服務型比對工作流程](#)。

建立相符的工作流程是您設定用來指定要一起比對的輸入資料以及執行比對方式的程序。在以提供者為基礎的工作流程中，如果帳戶具有提供者服務的訂閱 AWS Data Exchange，您可以將已知的識別碼與您偏好的供應商進行比對。根據您使用哪個提供者和服務來執行端對端測試，您可以相應地配置匹配的工作流程。

所以此 AWS Entity Resolution 控制台結合創建和運行在一個單一的按鈕的操作。選取 [建立並執行] 之後，會出現一則訊息，指出已建立相符的工作流程，且工作已開始。

3. 在「匹配」工作流程頁面上監視工作流程的狀態。

如果 Job 流程已成功完成 ([工作] 狀態為 [已完成])，則 end-to-end 測試即完成。

在相符工作流程詳細資訊頁面的「測量結果」標籤上，您可以在「最後一個工作測量結果」下檢視

- Job 識別碼。
- 相符工作流程工作的狀態：已佇列、進行中、已完成、失敗
- 工作流程工作的完成時間。
- 處理的記錄數。
- 未處理的記錄數。
- IDs生成的唯一匹配。
- 輸入記錄的數目。

您也可以檢視先前在「Job 歷程記錄」下執行之工作流程工作的相符工作流程工作的工作量度。

# AWS Entity Resolution 中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 的客戶，您將能從資料中心和網路架構中獲益，這些都是專為最重視安全的組織而設計的。

安全是 AWS 與您共同肩負的責任。[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：

- 雲端本身的安全 – AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 [AWS 合規計劃](#) 的一部分。若要了解適用於 AWS Entity Resolution 的合規計劃，請參閱 [合規計劃的 AWS 服務範圍](#)。
- 雲端內部的安全：您的責任取決於所使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 AWS Entity Resolution 時套用共同責任模型。下列主題說明如何將 AWS Entity Resolution 設定為達到您的安全及合規目標。您也會了解如何使用其他 AWS 服務來協助監控並保護 AWS Entity Resolution 資源。

## 主題

- [資料保護 AWS Entity Resolution](#)
- [的身分和存取管理 AWS Entity Resolution](#)
- [符合性驗證 AWS Entity Resolution](#)
- [韌性在 AWS Entity Resolution](#)

## 資料保護 AWS Entity Resolution

所以此 AWS [共同責任模型](#)適用於資料保護 AWS Entity Resolution。如本模型所述，AWS 負責保護運行所有的全球基礎設施 AWS 雲端。您有責任維持對託管在此基礎結構上的內容的控制權。您也必須負責安全性設定與管理工作 AWS 服務 你使用。如需有關資料隱私權的詳細資訊，請參閱 [資料隱私權 FAQ](#)。如需歐洲資料保護的相關資訊，請參閱 [AWS 共同責任模型和GDPR](#) 博客文章 [AWS 安全部落格](#)。

出於數據保護目的，我們建議您進行保護 AWS 帳戶 憑據並設置個別用戶 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM)。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：

- 對每個帳戶使用多重要素驗證 (MFA)。

- 使用SSL/TLS與之溝通 AWS 的費用。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 設定API和使用者活動記錄 AWS CloudTrail。如需使用 CloudTrail 軌跡進行擷取的相關資訊 AWS 活動，請參閱[使用 CloudTrail 系統線](#) AWS CloudTrail 使用者指南。
- 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。
- 如果您在訪問時需要 FIPS 140-3 驗證的加密模塊 AWS 透過指令行介面或API使用FIPS端點。如需有關可用FIPS端點的詳細資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

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 AWS Entity Resolution 或其他 AWS 服務 使用控制台API，AWS CLI，或 AWS SDKs。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URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

## 靜態資料加密 AWS Entity Resolution

AWS Entity Resolution 默認情況下提供加密，以保護靜態客戶敏感數據 AWS 擁有的加密金鑰。

AWS擁有的金鑰 — AWS Entity Resolution 預設會使用這些金鑰來自動加密個人識別資料。您無法檢視、管理或使用 AWS 擁有的密鑰，或審核其使用。不過，您不需要採取任何動作來保護加密資料的金鑰。[如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南](#)。

依預設加密靜態資料，有助於降低保護敏感資料所涉及的營運開銷和複雜性。同時，您可以使用它來建置符合嚴格加密合規性和法規要求的安全應用程式。

或者，您也可以在建建立相符的工作流程資源時，提供用於加密的客戶管理KMS金鑰。

客戶管理的金鑰 — AWS Entity Resolution 支持使用您創建，擁有和管理的對稱客戶託管密KMS鑰，以允許對敏感數據進行加密。您可以完全控制此層加密，因此能執行以下任務：

- 建立和維護金鑰政策
- 建立和維護IAM政策和補助金
- 啟用和停用金鑰政策
- 輪換金鑰密碼編譯資料
- 新增標籤
- 建立金鑰別名
- 安排金鑰供刪除

如需詳細資訊，請參閱中的[客戶管理金鑰](#) AWS Key Management Service 開發人員指南。

如需關於 AWS KMS，請參閱[什麼是AWS金鑰管理服務？](#)

## 金鑰管理

### 方法 AWS Entity Resolution 使用補助金 AWS KMS

AWS Entity Resolution 需要[授權](#)才能使用您的客戶管理金鑰。當您建立使用客戶管理金鑰加密的相符工作流程時，AWS Entity Resolution 通過發送[CreateGrant](#)請求以代表您創建授予 AWS KMS。中的補助金 AWS KMS 都是用來給 AWS Entity Resolution 訪問客戶帳戶中的KMS密鑰。AWS Entity Resolution 需要授權才能使用您的客戶管理密鑰進行以下內部操作：

- 傳送[GenerateDataKey](#)請求至 AWS KMS 產生由您的客戶管理金鑰加密的資料金鑰。
- 傳送[解密](#)請求至 AWS KMS 解密加密的數據密鑰，以便它們可以用來加密您的數據。

您可以隨時撤銷授予的存取權，或移除服務對客戶受管金鑰的存取權。如果你這樣做 AWS Entity Resolution 將無法存取由客戶管理金鑰加密的任何資料，這會影響依賴該資料的作業。例如，如果您透過授權移除對金鑰的服務存取權，並嘗試針對使用客戶金鑰加密的相符工作流程啟動工作，則作業會傳回錯AccessDeniedException誤。

### 建立客戶管理的金鑰

您可以使用建立對稱的客戶管理金鑰 AWS Management Console，或 AWS KMS APIs.

#### 建立對稱客戶受管金鑰

AWS Entity Resolution 支持使用[對稱加密密KMS鑰進行加密](#)。遵循中[建立對稱客戶管理金鑰](#)的步驟 AWS Key Management Service 開發人員指南。

#### 主要政策聲明

金鑰政策會控制客戶受管金鑰的存取權限。每個客戶受管金鑰都必須只有一個金鑰政策，其中包含決定誰可以使用金鑰及其使用方式的陳述式。在建立客戶受管金鑰時，可以指定金鑰政策。如需詳細資訊，請參閱「[管理客戶受管金鑰的存取權](#)」AWS Key Management Service 開發人員指南。

若要將您的客戶管理金鑰搭配您的 AWS Entity Resolution 資源，必須在密鑰策略中允許以下API操作：

- [kms:DescribeKey](#)— 提供金鑰ARN、建立日期 (以及刪除日期，如果適用)、金鑰狀態，以及金鑰材料的來源和到期日 (如果有的話) 等資訊。它包含欄位，例

如KeySpec，可協助您區分不同類型的KMS金鑰。它也會顯示金鑰使用方式 (加密、簽章或產生和驗證MACs) 以及KMS金鑰支援的演算法。AWS Entity Resolution 驗證是SYMMETRIC\_DEFAULT和KeySpecKeyUsage是ENCRYPT\_DECRYPT。

- [kms:CreateGrant](#)：新增客戶受管金鑰的授權。授予對指定KMS密鑰的控制訪問權限，該密鑰允許訪問[授予操作](#) AWS Entity Resolution 需要。如需有關[使用授權](#)的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。

這允許 AWS Entity Resolution 若要執行下列動作：

- 呼叫 GenerateDataKey 以產生加密的資料金鑰並加以儲存，因為資料金鑰不會立即用來加密。
- 呼叫 Decrypt 以使用儲存的加密資料金鑰來存取加密的資料。
- 設定退休本金以允許服務。RetireGrant

以下是您可以新增的政策陳述式範例 AWS Entity Resolution:

```
{
  "Sid" : "Allow access to principals authorized to use AWS Entity Resolution",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "*"
  },
  "Action" : ["kms:DescribeKey","kms:CreateGrant"],
  "Resource" : "*",
  "Condition" : {
    "StringEquals" : {
      "kms:ViaService" : "entityresolution.region.amazonaws.com",
      "kms:CallerAccount" : "111122223333"
    }
  }
}
```

## 使用者權限

當您將KMS金鑰設定為加密的預設金鑰時，預設KMS金鑰原則會允許任何具有必要KMS動作存取權的使用者使用此KMS金鑰來加密或解密資源。您必須授與使用者呼叫下列動作的權限，才能使用客戶管理的KMS金鑰加密：

- kms:CreateGrant
- kms:Decrypt

- kms:DescribeKey
- kms:GenerateDataKey

在[CreateMatchingWorkflow](#)請求期間，AWS Entity Resolution 將發送一個[DescribeKey](#)和[CreateGrant](#)請求 AWS KMS 代表您。這將要求IAM實體使用客戶管理的KMS金鑰發出要CreateMatchingWorkflow求，才能擁有KMS金鑰原則的kms:DescribeKey權限。

在[CreateIdMappingWorkflow](#)和請[StartIdMappingJob](#)求期間，AWS Entity Resolution 將發送一個[DescribeKey](#)和[CreateGrant](#)請求 AWS KMS 代表您。這需要使用客戶管理的KMS金鑰發出CreateIdMappingWorkflow和要StartIdMappingJob求的IAM實體，才能擁有KMS金鑰原則的kms:DescribeKey權限。供應商將能夠存取客戶管理的金鑰，以解密 AWS Entity Resolution Amazon S3 儲存貯體。

以下是您可以為提供者新增的政策陳述式範例，以解密 AWS Entity Resolution Amazon S3 桶：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::715724997226:root"
    },
    "Action": [
      "kms:Decrypt"
    ],
    "Resource": "<KMSKeyARN>",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "s3.amazonaws.com"
      }
    }
  ]
}
```

替換每個 *<user input placeholder>* 使用您自己的信息。

*<KMSKeyARN>*

AWS KMS Amazon Resource Name (Amazon 資源名稱)。

同樣地，叫用的IAM實體[StartMatchingJobAPI](#)必須擁有相符工作流程中所提供之客戶管理KMS金鑰的kms:GenerateDataKey權限kms:Decrypt和權限。

如需有關在[原則中指定權限](#)的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。

如需有關[疑難排解金鑰存取](#)的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。

## 指定客戶管理的金鑰 AWS Entity Resolution

您可以將客戶自管金鑰指定為下列資源的第二層加密：

「[匹配工作流程](#)」— 當您創建相匹配的工作流程資源時，您可以輸入，以指定數據關鍵字 KMSArn，AWS Entity Resolution 用於對資源存儲的可識別個人數據進行加密。

KMSArn— 輸入一個密鑰ARN，這是一個[密鑰標識符](#) AWS KMS 客戶管理的金鑰。

如果您要跨兩個資源建立或執行 ID 對應工作流程，則可以將客戶管理的金鑰指定為下列資源的第二層加密 AWS 帳戶：

[ID 對應工作流程](#)或「[開始 ID 對應](#)」[工作流程](#)— 當您建立 ID 對應工作流程資源或啟動 ID 對應工作流程作業時，您可以輸入，以指定資料金鑰 KMSArn，AWS Entity Resolution 用於對資源存儲的可識別個人數據進行加密。

KMSArn— 輸入一個密鑰ARN，這是一個[密鑰標識符](#) AWS KMS 客戶管理的金鑰。

## 監控您的加密金鑰 AWS Entity Resolution 服務

當您使用 AWS KMS 使用您的客戶管理金鑰 AWS Entity Resolution 服務資源，您可以使用 [Amazon CloudWatch 日誌](#)[AWS CloudTrail](#)或跟踪請求 AWS Entity Resolution 發送到 AWS KMS。

下面的例子是 AWS CloudTrail DescribeKey要監視CreateGrantGenerateDataKey、Decrypt、和的事件 AWS KMS 作業呼叫 AWS Entity Resolution 存取由客戶管理金鑰加密的資料：

### 主題

- [CreateGrant](#)
- [DescribeKey](#)
- [GenerateDataKey](#)
- [解密](#)

## CreateGrant

當您使用 AWS KMS 客戶管理密鑰，用於加密匹配的工作流程資源，AWS Entity Resolution 代表您發CreateGrant送訪問KMS密鑰的請求 AWS 帳戶。該授予 AWS Entity Resolution 創建特定於與相關聯的資源 AWS KMS 客戶管理的金鑰。此外，AWS Entity Resolution 刪除資源時，會使用此RetireGrant作業移除授權。

下面的範例事件會記錄 CreateGrant 操作：

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-22T17:02:00Z"
      }
    },
    "invokedBy": "entityresolution.amazonaws.com"
  },
  "eventTime": "2021-04-22T17:07:02Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateGrant",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "172.12.34.56",
  "userAgent": "ExampleDesktop/1.0 (V1; OS)",
  "requestParameters": {
    "retiringPrincipal": "entityresolution.region.amazonaws.com",
    "operations": [
```

```

        "GenerateDataKey",
        "Decrypt",
    ],
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "granteePrincipal": "entityresolution.region.amazonaws.com"
},
"responseElements": {
    "grantId":
"0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
},
"requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
"readOnly": false,
"resources": [
    {
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "111122223333"
}

```

## DescribeKey

AWS Entity Resolution 使用DescribeKey操作來驗證是否 AWS KMS 與您比對資源相關聯的客戶管理金鑰存在於帳戶和區域中。

下列範例事件會記錄DescribeKey作業。

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",

```

```

    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-22T17:02:00Z"
      }
    },
    "invokedBy": "entityresolution.amazonaws.com"
  },
  "eventTime": "2021-04-22T17:07:02Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "DescribeKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "172.12.34.56",
  "userAgent": "ExampleDesktop/1.0 (V1; OS)",
  "requestParameters": {
    "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
  },
  "responseElements": null,
  "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"

```

```
}
```

## GenerateDataKey

當您啟用 AWS KMS 客戶管理的密鑰為您匹配的工作流程資源，AWS Entity Resolution GenerateDataKey 通過 Amazon Simple Storage Service (Amazon S3) 發送請求 AWS KMS 指定 AWS KMS 客戶管理的資源密鑰。

下列範例事件會記錄 GenerateDataKey 作業。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "s3.amazonaws.com"
  },
  "eventTime": "2021-04-22T17:07:02Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "172.12.34.56",
  "userAgent": "ExampleDesktop/1.0 (V1; OS)",
  "requestParameters": {
    "keySpec": "AES_256",
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
  },
  "responseElements": null,
  "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
```

```
"sharedEventID": "57f5dbee-16da-413e-979f-2c4c6663475e"
}
```

## 解密

當您啟用 AWS KMS 客戶管理的密鑰為您匹配的工作流程資源，AWS Entity Resolution Decrypt 通過 Amazon Simple Storage Service (Amazon S3) 發送請求 AWS KMS 指定 AWS KMS 客戶管理的資源密鑰。

下列範例事件會記錄 Decrypt 作業。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "s3.amazonaws.com"
  },
  "eventTime": "2021-04-22T17:10:51Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "172.12.34.56",
  "userAgent": "ExampleDesktop/1.0 (V1; OS)",
  "requestParameters": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
  },
  "responseElements": null,
  "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "readOnly": true,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "AWS::KMS::Key",
      "ARN": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
}
```

```
"recipientAccountId": "111122223333",  
"sharedEventID": "dc129381-1d94-49bd-b522-f56a3482d088"  
}
```

## 考量事項

AWS Entity Resolution 不支援使用新的客戶管理KMS金鑰更新相符的工作流程。在這種情況下，您可以使用客戶管理的KMS金鑰建立新的工作流程。

## 進一步了解

下列資源會提供有關靜態資料加密的詳細資訊。

如需[AWS金鑰管理服務基本概念](#)的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。

如需[AWS金鑰管理服務之安全性最佳作法](#)的詳細資訊，請參閱 AWS Key Management Service 開發人員指南。

## 存取 AWS Entity Resolution 使用介面端點 (AWS PrivateLink)

您可以使用... AWS PrivateLink 在您的VPC和之間創建私人連接 AWS Entity Resolution。您可以訪問 AWS Entity Resolution 就好像它在你的VPC，沒有使用互聯網網關，NAT設備，VPN連接或 AWS Direct Connect 連接。您中的執行個體VPC不需要公用 IP 位址即可存取 AWS Entity Resolution.

您可以通過創建一個接口端點來建立此私人連接，由 AWS PrivateLink。我們會在您為介面端點啟用的每個子網路中建立端點網路介面。這些是由請求者管理的網路介面，可做為目的地流量的入口點 AWS Entity Resolution.

如需詳細資訊，請參閱[存取 AWS 服務 通過 AWS PrivateLink](#)中的AWS PrivateLink 指南。

## 的注意事項 AWS Entity Resolution

設定的介面端點之前 AWS Entity Resolution，檢閱「[注意事項](#)」AWS PrivateLink 指南。

AWS Entity Resolution 支援透過介面端點呼叫其所有API動作。

VPC端點策略支援 AWS Entity Resolution。默認情況下，完全訪問 AWS Entity Resolution 允許透過介面端點。或者，您可以將安全群組與端點網路介面建立關聯，以控制 AWS Entity Resolution 通過接口端點。

## 建立的介面端點 AWS Entity Resolution

您可以為下列項目建立介面端點 AWS Entity Resolution 使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI). [如需詳細資訊，請參閱 AWS PrivateLink 指南。](#)

建立的介面端點 AWS Entity Resolution 使用下列服務名稱：

```
com.amazonaws.region.entityresolution
```

如果您DNS為介面端點啟用私有，您可以API向 AWS Entity Resolution 使用其默認的區域DNS名稱。例如：`entityresolution.us-east-1.amazonaws.com`。

## 為您的介面端點建立端點政策

端點策略是您可以附加到介面端點的IAM資源。預設端點策略允許完整存取 AWS Entity Resolution 通過接口端點。若要控制允許的存取 AWS Entity Resolution 從您的VPC，將自定義端點策略附加到接口端點。

端點政策會指定以下資訊：

- 可以執行動作的主參與者 (AWS 帳戶、IAM使用者和IAM角色)。
- 可執行的動作。
- 可供執行動作的資源。

有關詳情，請參閱[使用端點策略控制對服務的存取 AWS PrivateLink 指南](#)。

範例：VPC端點策略 AWS Entity Resolution actions

以下是自訂端點政策的範例。當您將此原則附加到介面端點時，它會授予對列出的端點的存取權 AWS Entity Resolution 所有資源上所有主參與者的動作。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "entityresolution:CreateMatchingWorkflow",
        "entityresolution:StartMatchingJob",

```

```
        "entityresolution:GetMatchingJob"  
    ],  
    "Resource": "*" ]  
]  
}
```

## 的身分和存取管理 AWS Entity Resolution

AWS Identity and Access Management ( IAM ) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員會控制誰可以驗證 ( 登入 ) 和授權 ( 具有許可 ) 使用 AWS Entity Resolution 資源。IAM 是 AWS 服務 您可以免費使用的 。

### Note

AWS Entity Resolution 支援跨帳戶政策。如需詳細資訊，請參閱 IAM 使用者指南 [中的跨帳戶資源存取權IAM](#)。

### 主題

- [物件](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [AWS Entity Resolution 如何使用 IAM](#)
- [AWS Entity Resolution 的身分型政策範例](#)
- [AWS 受管理的政策 AWS Entity Resolution](#)
- [對 AWS Entity Resolution 身分和存取權進行故障診斷](#)

## 物件

使用 AWS Identity and Access Management ( IAM ) 的方式會有所不同，取決於您在 中執行的工作 AWS Entity Resolution。

服務使用者 – 如果您使用 AWS Entity Resolution 服務來執行您的工作，則管理員會為您提供所需的憑證和許可。當您使用更多 AWS Entity Resolution 功能來執行工作時，您可能需要額外的許可。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 Entity Resolution 中的某項功能，請參閱 [對 AWS Entity Resolution 身分和存取權進行故障診斷](#)。

**服務管理員** – 如果您負責公司 AWS Entity Resolution 的資源，您可能擁有的完整存取權 AWS Entity Resolution。您的任務是判斷您的服務使用者應該存取哪些 AWS Entity Resolution 功能和資源。然後，您必須向 IAM 管理員提交請求，以變更服務使用者的許可。請檢閱此頁面上的資訊，以了解的基本概念 IAM。若要進一步了解貴公司如何 IAM 搭配使用 AWS Entity Resolution，請參閱 [AWS Entity Resolution 如何使用 IAM](#)。

**IAM 管理員** – 如果您是 IAM 管理員，您可能想要了解如何撰寫政策以管理存取權的詳細資訊 AWS Entity Resolution。若要檢視您可以在中使用的以 AWS Entity Resolution 身分為基礎的政策範例 IAM，請參閱 [AWS Entity Resolution 的身分型政策範例](#)。

## 使用身分驗證

驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證（登入 AWS）。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分登入。AWS IAM Identity Center（IAM Identity Center）使用者、您的單一登入身分驗證，以及您的 Google 或 Facebook 憑證，都是聯合身分的範例。當您以聯合身分登入時，您的管理員先前會使用 IAM 角色設定身分聯合。當您 AWS 使用聯合來存取時，您會間接擔任角色。

您可以登入 AWS Management Console 或 AWS 存取入口網站，視您是的使用者類型而定。如需登入的詳細資訊 AWS，請參閱使用者指南中的 [如何登入 AWS 帳戶](#) 您的。AWS 登入

如果您以 AWS 程式設計方式存取，AWS 會提供軟體開發套件（SDK）和命令列介面（CLI），以使用您的憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的 [AWS 簽章第 4 版以取得 API 請求](#)。

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身分驗證（MFA）來提高帳戶的安全性。若要進一步了解，請參閱 AWS IAM Identity Center 使用者指南中的 [多重要素驗證](#)，以及 IAM 使用者指南 [AWS 中的多重要素驗證 IAM](#)。

## 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，該身分可完全存取帳戶中的所有 AWS 服務和資源。此身分稱為 AWS 帳戶 根使用者，透過您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。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。如需需要您以根使用者身分登入的任務完整清單，請參閱 IAM 使用者指南中的 [需要根使用者憑證的任務](#)。

## 聯合身分

作為最佳實務，會要求人類使用者，包括需要管理員存取權的使用者，使用 AWS 服務 臨時憑證來與身分提供者使用聯合來存取。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、AWS Directory Service、身分中心目錄，或使用透過身分來源提供的 AWS 服務 憑證存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任角色，而角色會提供臨時憑證。

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，或者您可以連線並同步到您身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有和應用程式中使用。如需 IAM Identity Center 的相關資訊，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 中具有單一個人或應用程式特定許可 AWS 帳戶 的身分。在可能的情況下，我們建議依賴臨時憑證，而不是建立具有密碼和存取金鑰等長期憑證IAM的使用者。不過，如果您有特定使用案例需要IAM使用者長期憑證，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南 中的[針對需要長期憑證的使用案例定期輪換存取金鑰](#)。

[IAM 群組](#)是指定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，您可以擁有一名名為的群組IAMAdmins，並授予該群組管理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。若要進一步了解，請參閱 IAM 使用者指南 中的[IAM使用者使用案例](#)。

## IAM 角色

[IAM 角色](#)是 中具有特定許可 AWS 帳戶 的身分。它類似於IAM使用者，但與特定人員無關。若要暫時在中擔任IAM角色 AWS Management Console，您可以從[使用者切換至IAM角色（主控台）](#)。您可以呼叫 AWS CLI 或 AWS API 操作，或使用自訂 來擔任角色URL。如需使用角色方法的詳細資訊，請參閱 IAM 使用者指南 中的[擔任角色的方法](#)。

IAM 具有臨時憑證的角色在下列情況下很有用：

- 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（聯合）建立角色](#)。如果您使用 IAM Identity Center，您可以設定許可集。若要控制身分在身分驗證後可以存取的內容，IAM Identity Center 會將許可集與 中的角色相關聯IAM。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](#)。

- 臨時IAM使用者許可 – IAM使用者或角色可以擔任IAM角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM角色，允許不同帳戶中的某人（受信任的委託人）存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。不過，使用某些 AWS 服務，您可以將政策直接連接至資源（而不是使用角色作為代理）。若要了解跨帳戶存取的角色和資源型政策之間的差異，請參閱 IAM 使用者指南 [中的跨帳戶資源存取IAM](#)。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在 服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式，EC2或在 Amazon S3 中儲存物件。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。
- 轉送存取工作階段（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 使用呼叫的委託人許可 AWS 服務，並結合請求向下游服務 AWS 服務 提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。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請求的政策詳細資訊，請參閱[轉送存取工作階段](#)。
- 服務角色 – 服務角色是服務代表您執行動作時擔任[IAM的角色](#)。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的[建立角色以將許可委派給 AWS 服務](#)。IAM
- 服務連結角色 – 服務連結角色是連結至 的服務角色類型 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，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon 上執行的應用程式 EC2 – 您可以使用 IAM角色來管理在EC2執行個體上執行之應用程式的臨時憑證，以及提出 AWS CLI 或 AWS API請求。最好將存取金鑰存放在EC2執行個體中。若要將 AWS 角色指派給EC2執行個體並將其提供給其所有應用程式，您可以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 角色，並啟用在EC2執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱 IAM 使用者指南 中的[使用 IAM角色將許可授予在 Amazon EC2執行個體上執行的應用程式](#)。

## 使用政策管理存取權

您可以透過建立政策並將其連接至 AWS 身分或資源 AWS 來控制 中的存取。政策是 AWS 其中的物件，當與身分或資源建立關聯時，會定義其許可。當主體（使用者、根使用者或角色工作階段）發出請求時，會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以JSON文件

AWS 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。

預設情況下，使用者和角色沒有許可。若要授予使用者對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，使用者可以擔任角色。

IAM 無論您用來執行操作的方法為何，政策都會定義動作的許可。例如，假設您有一個允許 iam:GetRole 動作的政策。具有該政策的使用者可以從 AWS Management Console、AWS CLI或 AWS 取得角色資訊API。

## 身分型政策

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。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型政策，請參閱 IAM 使用者指南 中的[使用客戶受管政策定義自訂IAM許可](#)。

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。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。若要了解如何在受管政策或內嵌政策之間進行選擇，請參閱 IAM 使用者指南 中的在[受管政策與內嵌政策之間進行選擇](#)。

## 資源型政策

資源型政策是您附加至資源JSON的政策文件。資源型政策的範例包括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](#)。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策IAM中使用來自的 AWS 受管政策。

## 存取控制清單 ( ACLs )

存取控制清單 ( ACLs ) 控制哪些主體 ( 帳戶成員、使用者或角色 ) 具有存取資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC是支援的服務範例ACLs。若要進一步了解 ACLs，請參閱 Amazon Simple Storage Service 開發人員指南 中的[存取控制清單 \( ACL \) 概觀](#)。

## 其他政策類型

AWS 支援其他較不常見的政策類型。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** – 許可界限是一項進階功能，您可以在其中設定身分型政策可授予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](#)。
- **服務控制政策（SCPs）** – SCPs是在 中指定組織或組織單位（OU）最大許可JSON的政策 AWS Organizations。AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個的服務。如果您啟用組織中的所有功能，則可以將服務控制政策（SCPs）套用至任何或所有帳戶。SCP 限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需 Organizations 和 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南 中的[服務控制政策](#)。
- **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。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱 IAM 使用者指南 中的[政策評估邏輯](#)。

## AWS Entity Resolution 如何使用 IAM

在您使用 IAM 管理對 的存取之前 AWS Entity Resolution，請先了解哪些IAM功能可與 搭配使用 AWS Entity Resolution。

IAM 您可以搭配 使用的功能 AWS Entity Resolution

IAM 功能	AWS Entity Resolution 支援
<a href="#">身分型政策</a>	是
<a href="#">資源型政策</a>	是
<a href="#">政策動作</a>	是

IAM 功能	AWS Entity Resolution 支援
<a href="#">政策資源</a>	是
<a href="#">政策條件索引鍵</a>	是
<a href="#">ACLs</a>	否
<a href="#">ABAC ( 政策中的標籤 )</a>	部分
<a href="#">臨時憑證</a>	是
<a href="#">轉送存取工作階段 ( FAS )</a>	是
<a href="#">服務角色</a>	是
<a href="#">服務連結角色</a>	否

若要取得 AWS Entity Resolution 和其他 AWS 服務如何與大多數 IAM 功能搭配使用的高階檢視，請參閱 IAM 使用者指南 中的 [AWS 服務IAM](#)。

## 的身分型政策 AWS Entity Resolution

支援身分型政策：是

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。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型政策，請參閱 IAM 使用者指南 中的 [使用客戶受管政策定義自訂IAM許可](#)。

透過身分IAM型政策，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。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。若要了解您可以在JSON政策中使用的所有元素，請參閱 IAM 使用者指南 中的 [IAMJSON政策元素參考](#)。

## 的身分型政策範例 AWS Entity Resolution

若要檢視 AWS Entity Resolution 身分型政策的範例，請參閱 [AWS Entity Resolution的身分型政策範例](#)。

## 中的資源型政策 AWS Entity Resolution

支援資源型政策：是

資源型政策是您附加至資源JSON的政策文件。資源型政策的範例包括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](#)。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

若要啟用跨帳戶存取，您可以將另一個帳戶中的整個帳戶或IAM實體指定為資源型政策中的主體。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的時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授予主體實體（使用者或角色）存取資源的許可。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 [中的跨帳戶資源存取權IAM](#)。

## 的政策動作 AWS Entity Resolution

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。

JSON 政策的 Action元素說明您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API操作相同的名稱。有一些例外狀況，例如沒有相符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 Entity Resolution 動作清單，請參閱服務授權參考 中的[由定義的動作 AWS Entity Resolution](#)。

中的政策動作在動作之前 AWS Entity Resolution 使用下列字首：

```
entityresolution
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [  
  "entityresolution:action1",  
  "entityresolution:action2"  
]
```

若要檢視 AWS Entity Resolution 身分型政策的範例，請參閱 [AWS Entity Resolution 的身分型政策範例](#)。

## 的政策資源 AWS Entity Resolution

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 政策元素會指定動作套用的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \( ARN \) 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 Entity Resolution 資源類型及其的清單 ARNs，請參閱服務授權參考中的 [由定義的資源 AWS Entity Resolution](#)。若要了解您可以使用哪些動作來指定每個資源 ARN 的，請參閱 [定義的動作 AWS Entity Resolution](#)。

若要檢視 AWS Entity Resolution 身分型政策的範例，請參閱 [AWS Entity Resolution 的身分型政策範例](#)。

## 的政策條件索引鍵 AWS Entity Resolution

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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，會使用邏輯 OR 操作 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，只有在IAM使用者使用其IAM使用者名稱標記時，您才能授予使用者存取資源的許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 [IAM政策元素：變數和標籤](#)。

AWS 支援全域條件索引鍵和服務特定條件索引鍵。若要查看所有 AWS 全域條件索引鍵，請參閱 IAM 使用者指南 中的 [AWS 全域條件內容索引鍵](#)。

若要查看 AWS Entity Resolution 條件金鑰清單，請參閱服務授權參考 中的 [的條件金鑰 AWS Entity Resolution](#)。若要了解您可以使用條件金鑰的動作和資源，請參閱 [定義的動作 AWS Entity Resolution](#)。

若要檢視 AWS Entity Resolution 身分型政策的範例，請參閱 [AWS Entity Resolution的身分型政策範例](#)。

## ACLs 在 中 AWS Entity Resolution

支援 ACLs：否

存取控制清單（ACLs）控制哪些主體（帳戶成員、使用者或角色）具有存取資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

## ABAC 使用 AWS Entity Resolution

支援 ABAC（政策中的標籤）：部分

屬性型存取控制（ABAC）是一種根據屬性定義許可的授權策略。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接至IAM實體（使用者或角色）和許多 AWS 資源。標記實體和資源是 的第一步 ABAC。然後，您可以設計ABAC政策，以便在主體的標籤與其嘗試存取之資源上的標籤相符時允許操作。

ABAC 有助於快速成長的環境，並有助於處理政策管理變得繁瑣的情況。

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 的詳細資訊ABAC，請參閱 IAM 使用者指南 中的 [使用ABAC授權定義許可](#)。若要檢視包含設定 之步驟的教學課程ABAC，請參閱 IAM 使用者指南 中的 [使用屬性型存取控制（ABAC）](#)。

## 搭配使用臨時憑證 AWS Entity Resolution

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括 AWS 服務 使用哪些臨時憑證，請參閱 IAM 使用者指南 中的 [AWS 服務 與 搭配使用IAM](#)。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入，則表示您正在使用臨時憑證。例如，當您 AWS 使用公司的單一登入（SSO）連結存取時，該程序會自動建立臨時憑證。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 [從使用者切換至IAM角色（主控台）](#)。

您可以使用 AWS CLI 或 手動建立臨時憑證 AWS API。然後，您可以使用這些臨時憑證來存取 AWS。AWS recommends，您動態產生臨時憑證，而不是使用長期存取金鑰。如需詳細資訊，請參閱 [中的臨時安全憑證IAM](#)。

## 轉送 的存取工作階段 AWS Entity Resolution

支援轉送存取工作階段（FAS）：是

當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，並結合請求向下游服務 AWS 服務 提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。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請求的政策詳細資訊，請參閱[轉送存取工作階段](#)。

## AWS Entity Resolution的服務角色

支援服務角色：是

服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 [中的建立角色以將許可委派給 AWS 服務](#)。IAM

### Warning

變更服務角色的許可可能會中斷 AWS Entity Resolution 功能。只有在 AWS Entity Resolution 提供指引時，才能編輯服務角色。

## 的服務連結角色 AWS Entity Resolution

支援服務連結角色：否

服務連結角色是連結至的服務角色類型 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，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服务連結角色的詳細資訊，請參閱[AWS 使用的服務IAM](#)。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇 Yes (是) 連結，以檢視該服務的服務連結角色文件。

## AWS Entity Resolution的身分型政策範例

根據預設，使用者和角色不具備建立或修改 AWS Entity Resolution 資源的權限。他們也無法使用 AWS Management Console、AWS Command Line Interface (AWS CLI) 或來執行任務 AWS API。若要授予使用者對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，使用者可以擔任角色。

若要了解如何使用這些範例政策文件來建立IAM身分型JSON政策，請參閱 IAM 使用者指南 中的[建立IAM政策 \(主控台\)](#)。

如需定義的動作和資源類型詳細資訊 AWS Entity Resolution，包括ARNs每種資源類型的格式，請參閱服務授權參考 中的 [的動作、資源和條件索引鍵 AWS Entity Resolution](#)。

### 主題

- [政策最佳實務](#)
- [使用 AWS Entity Resolution 主控台](#)
- [允許使用者檢視他們自己的許可](#)

## 政策最佳實務

身分型政策會決定是否有人可以在您的帳戶中建立、存取或刪除 AWS Entity Resolution 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用針對許多常見使用案例授予許可的 AWS 受管政策。它們可在您的中使用 AWS 帳戶。建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 [AWS 受管政策](#)或 [AWS 任務功能的受管政策](#)。
- 套用最低權限許可 – 當您使用IAM政策設定許可時，只會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 套用許可的詳細資訊，請參閱 IAM 使用者指南 [中的政策和許可IAM](#)。

- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，例如 AWS 服務，您也可以使用 條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南 中的 [IAMJSON政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證您的IAM政策，以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，讓政策遵循IAM政策語言（JSON）和IAM最佳實務。IAM Access Analyzer 提供超過 100 個政策檢查和可操作的建議，協助您撰寫安全且實用的政策。如需詳細資訊，請參閱 IAM 使用者指南中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素身分驗證（MFA）– 如果您有需要IAM使用者或 根使用者的案例 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求，請將MFA條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的 [使用 安全API存取MFA](#)。

如需 中最佳實務的詳細資訊IAM，請參閱 IAM 使用者指南 [中的安全最佳實務IAM](#)。

## 使用 AWS Entity Resolution 主控台

若要存取 AWS Entity Resolution 主控台，您必須具有一組最低許可。這些許可必須允許您列出和檢視中 AWS Entity Resolution 資源的詳細資訊 AWS 帳戶。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。

對於僅對 AWS CLI 或 進行呼叫的使用者，您不需要允許最低主控台許可 AWS API。相反地，僅允許存取與其API嘗試執行的操作相符的動作。

若要確保使用者和角色仍然可以使用 AWS Entity Resolution 主控台，也請將 AWS Entity Resolution *ConsoleAccess* 或 *ReadOnly* AWS 受管政策連接至實體。如需詳細資訊，請參閱 IAM 使用者指南 中的 [新增許可給使用者](#)。

## 允許使用者檢視他們自己的許可

此範例示範如何建立政策，允許使用者檢視連接至其IAM使用者身分的內嵌和受管政策。此政策包含在 主控台上完成此動作或使用 AWS CLI 或 以程式設計方式完成此動作的許可 AWS API。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
```

```

        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

## AWS 受管理的政策 AWS Entity Resolution

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 操作可供現有服務使用時，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：AWSEntityResolutionConsoleFullAccess

您可將 AWSEntityResolutionConsoleFullAccess 政策連接到 IAM 身分。

此原則會授與 AWS Entity Resolution 端點和資源的完整存取權。

此政策還允許對 S3、標記 AWS 服務 等相關的某些讀取存取權限 AWS Glue，以 AWS KMS 便主控台可以顯示選項，並使用選取的選項來執行實體解析動作。有些資源會縮小以包含服務名稱 entityresolution。

由 AWS Entity Resolution 於依賴傳遞的角色對相關 AWS 資源執行動作，因此此原則也會授與選取和傳遞所需角色的權限。

### 許可詳細資訊

此政策包含以下許可。

- EntityResolutionAccess— 允許主參與者完全存取 AWS Entity Resolution 端點和資源。
- GlueSourcesConsoleDisplay— 授與清單 AWS Glue 表格作為資料來源選項的存取權，以及匯入資料來源的資料表結構描述，以提供使用者體驗。
- S3BucketsConsoleDisplay— 授予將所有 S3 儲存貯體列為資料來源選項的存取權。
- S3SourcesConsoleDisplay— 授予將 S3 儲存貯體顯示為資料來源選項的存取權。
- TaggingConsoleDisplay— 授予讀取標記鍵和值的存取權。
- KMSConsoleDisplay— 授予在中描述金鑰和列出別名的存取權，AWS Key Management Service 以解密和加密資料來源。
- ListRolesToPickForPassing— 授與列出所有角色的存取權，以便使用者可以選擇要傳遞的角色。
- PassRoleToEntityResolutionService— 授與將縮小角色傳遞給 AWS Entity Resolution 服務的存取權。
- ManageEventBridgeRules— 授予建立、更新和刪除 Amazon EventBridge 規則以取得 S3 通知的存取權。
- ADXReadAccess— 授予驗證客戶是否具有權利或訂閱的存取權。AWS Data Exchange

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EntityResolutionAccess",
```

```
    "Effect": "Allow",
    "Action": [
      "entityresolution:*"
    ],
    "Resource": "*"
  },
  {
    "Sid": "GlueSourcesConsoleDisplay",
    "Effect": "Allow",
    "Action": [
      "glue:GetSchema",
      "glue:SearchTables",
      "glue:GetSchemaByDefinition",
      "glue:GetSchemaVersion",
      "glue:GetSchemaVersionsDiff",
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:GetTable",
      "glue:GetTables",
      "glue:GetTableVersion",
      "glue:GetTableVersions"
    ],
    "Resource": "*"
  },
  {
    "Sid": "S3BucketsConsoleDisplay",
    "Effect": "Allow",
    "Action": [
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  },
  {
    "Sid": "S3SourcesConsoleDisplay",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation",
      "s3:ListBucketVersions",
      "s3:GetBucketVersioning"
    ],
    "Resource": "*"
  },
  {
```

```
    "Sid": "TaggingConsoleDisplay",
    "Effect": "Allow",
    "Action": [
        "tag:GetTagKeys",
        "tag:GetTagValues"
    ],
    "Resource": "*"
},
{
    "Sid": "KMSConsoleDisplay",
    "Effect": "Allow",
    "Action": [
        "kms:DescribeKey",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Sid": "ListRolesToPickRoleForPassing",
    "Effect": "Allow",
    "Action": [
        "iam:ListRoles"
    ],
    "Resource": "*"
},
{
    "Sid": "PassRoleToEntityResolutionService",
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::*:role/*entityresolution*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "entityresolution.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "ManageEventBridgeRules",
    "Effect": "Allow",
    "Action": [
```

```

        "events:PutRule",
        "events>DeleteRule",
        "events:PutTargets",
    ],
    "Resource": [
        "arn:aws:events:*:*:rule/entity-resolution-automatic*"
    ]
},
{
    "Sid": "ADXReadAccess",
    "Effect": "Allow",
    "Action": [
        "dataexchange:GetDataSet"
    ],
    "Resource": "*"
},
]
}

```

## AWS 受管理的策略：AWSEntityResolutionConsoleReadOnlyAccess

您可以將 `AWSEntityResolutionConsoleReadOnlyAccess` 連接到 IAM 實體。

此策略會授與 AWS Entity Resolution 端點和資源的唯讀存取權。

### 許可詳細資訊

此政策包含以下許可。

- `EntityResolutionRead`— 允許主參與者對 AWS Entity Resolution 端點和資源進行唯讀存取。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EntityResolutionRead",
      "Effect": "Allow",
      "Action": [
        "entityresolution:Get*",
        "entityresolution:List*"
      ],
      "Resource": "*"
    }
  ]
}

```

```
    },
  ]
}
```

## AWS Entity Resolution AWS 受管理策略的更新

檢視 AWS Entity Resolution 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 Entity Resolution 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AWSEntityResolutionConsoleFullAccess 更新現有政策	已新增ADXReadAccess 並啟ManageEventBridgeRules 用相符工作流程中的提供者服務選項。	2023 年 10 月 16 日
AWS Entity Resolution 開始追蹤變更	AWS Entity Resolution 開始追蹤其 AWS 受管理策略的變更。	2023 年 8 月 18 日

## 對 AWS Entity Resolution 身分和存取權進行故障診斷

使用下列資訊來協助您診斷和修正使用 AWS Entity Resolution 和 時可能遇到的常見問題IAM。

### 主題

- [我無權在 中執行動作 AWS Entity Resolution](#)
- [我無權執行 iam : PassRole](#)
- [我想要允許 以外的人員 AWS 帳戶 存取我的 AWS Entity Resolution 資源](#)

### 我無權在 中執行動作 AWS Entity Resolution

如果 AWS Management Console 告訴您未獲授權執行動作，則必須聯絡管理員以取得協助。您的管理員是提供您使用者名稱和密碼的人員。

當mateojacksonIAM使用者嘗試使用主控台檢視虛構`my-example-widget`資源的詳細資訊，但沒有虛構entityresolution:`GetWidget`許可時，會發生下列錯誤範例。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
entityresolution:GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 `my-example-widget` 動作存取 `entityresolution:GetWidget` 資源。

## 我無權執行 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 Entity Resolution。

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。

當名為 `marymajor` IAM 的使用者嘗試使用主控台在 中執行動作時，會發生下列錯誤範例 AWS Entity Resolution。但是，動作請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 管理員。您的管理員提供您的簽署憑證。

## 我想要允許 以外的人員 AWS 帳戶 存取我的 AWS Entity Resolution 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。對於支援資源型政策或存取控制清單（ACLs）的服務，您可以使用這些政策來授予人員對資源的存取權。

如需進一步了解，請參閱以下內容：

- 若要了解 是否 AWS Entity Resolution 支援這些功能，請參閱 [AWS Entity Resolution 如何使用 IAM](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 IAM 使用者指南 中的 [在您 AWS 帳戶 擁有的另一個資源中為IAM使用者提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 使用者指南 中的 [提供存取權給第三方 AWS 帳戶 擁有](#)。IAM
- 若要了解如何透過身分聯合提供存取權，請參閱 IAM 使用者指南 中的 [為外部驗證的使用者提供存取權（身分聯合）](#)。

- 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 [中的跨帳戶資源存取IAM](#)。

## 符合性驗證 AWS Entity Resolution

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 上進行HIPAA安全與合規架構](#) — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

### Note

並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合[HIPAA格服務參考資料](#)。

- [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 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並將其對應至安全性控制。ISO
- [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 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。

- [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。

## AWS Entity Resolution 合規性最佳做法

本節提供使用時符合性的最佳做法和建議 AWS Entity Resolution。

### 支付卡產業資料安全標準 (PCIDSS)

AWS Entity Resolution 支援商家或服務供應商處理、儲存和傳輸信用卡資料，並且已通過驗證符合支付卡產業 (PCI) 資料安全標準 (DSS)。如需有關 PCI DSS (包括如何要求 AWS PCI 符合性 Package 件副本) 的詳細資訊，請參閱[PCIDSS 層級 1](#)。

### 系統與組織控制 (SOC)

AWS Entity Resolution 符合「系統與組織控制」(SOC) 措施，包括 SOC 1、SOC 2 和 SOC 3。SOC 報告是獨立的第三方檢查報告，展示如何 AWS 實現關鍵合規性控制和目標。這些稽核可確保執行恰當得宜的安全防禦措施與程序，以針對可能影響到客戶與公司資料安全性、機密性和可用性的風險，提供安全防護。這些協力廠商稽核的結果可在 [\[AWS SOC 法規遵循\] 網站](#) 上取得，您可以在其中檢視已發佈的報告，以取得有關支援 AWS 作業和法規遵循之控制項的詳細資訊。

## 韌性在 AWS Entity Resolution

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。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 AWS 區域 和可用區域的詳細資訊，請參閱[AWS 全域基礎結構](#)。

除了 AWS 全球基礎架構之外，還 AWS Entity Resolution 提供多種功能，協助支援您的資料恢復能力和備份需求。

# 監控 AWS Entity Resolution

監控是維持其他 AWS 解決方案的可靠性、可用性和效能的 AWS Entity Resolution 重要組成部分。AWS 提供下列監控工具來監視 AWS Entity Resolution、在發生錯誤時回報，並在適當時自動採取行動：

- 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》](#)。

## 主題

- [使用記錄 AWS Entity Resolution API 呼叫 AWS CloudTrail](#)

## 使用記錄 AWS Entity Resolution API 呼叫 AWS CloudTrail

AWS Entity Resolution 與 (提供中的使用者 AWS CloudTrail、角色或服務所採取的動作記錄) 的 AWS 服務整合 AWS Entity Resolution。CloudTrail 擷取 AWS Entity Resolution 作為事件的所有 API 呼叫。擷取的呼叫包括來自 AWS Entity Resolution 主控台的呼叫和 AWS Entity Resolution API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 AWS Entity Resolution。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷提出的要求 AWS Entity Resolution、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 [AWS CloudTrail 用者指南](#)。

## AWS Entity Resolution 中的資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動發生在中時 AWS Entity Resolution，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。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 事件歷程記錄檢視事件](#)。

對於您的事件的持續記錄 AWS 帳戶，包括事件 AWS Entity Resolution，請創建一個跟踪。追蹤可 CloudTrail 將日誌檔交付到 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。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。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 Amazon SNS 通知 CloudTrail](#)
- [從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件](#)

所有 AWS Entity Resolution 動作均由「API 參考」記錄 CloudTrail 並記錄在「[AWS Entity Resolution API 參考](#)」中。

每一筆事件或日誌專案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：

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 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。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱[CloudTrail 使 userIdentity 元素](#)。

## 瞭解 AWS Entity Resolution 記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

# 使用建立AWS實體解析資源 AWS CloudFormation

AWS Entity Resolution 與這項服務整合在一起 AWS CloudFormation，可協助您建立 AWS 資源模型和設定資源，以減少建立和管理資源和基礎結構的時間。您可以建立描述您想要的所有 AWS 資源 (例如 `AWS::EntityResolution::MatchingWorkflow`, `AWS::EntityResolution::SchemaMapping`, `AWS::EntityResolution::IdMappingWorkflow`, `AWS::EntityResolution::IdNamespace` 和 `AWS::EntityResolution::PolicyStatement`) 的範本，並為您 AWS CloudFormation 佈建和設定這些資源。

使用時 AWS CloudFormation，您可以重複使用範本，以一致且重複地設定AWS實體解析資源。描述您的資源一次，然後在多個區域中一遍又一遍地佈建相同 AWS 帳戶 的資源。

## AWS實體解析度和 AWS CloudFormation 範本

若要佈建和設定AWS實體解析及相關服務的資源，您必須瞭解[AWS CloudFormation 範本](#)。範本是在JSON或中格式化的文字檔案YAML。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 Designer 來協助您開始使用 AWS CloudFormation 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實體解析度支援建立 `AWS::EntityResolution::MatchingWorkflow`, `AWS::EntityResolution::SchemaMapping`, `AWS::EntityResolution::IdMappingWorkflow`, `AWS::EntityResolution::IdNamespace` 和 `AWS::EntityResolution::PolicyStatement` 中 AWS CloudFormation。如需詳細資訊，包括JSON和的範例和YAML範本 `AWS::EntityResolution::PolicyStatement`，請參閱AWS CloudFormation 使用指南中的「[AWS實體解決方案](#)」[資源類型參考](#)。 `AWS::EntityResolution::MatchingWorkflow`, `AWS::EntityResolution::SchemaMapping`, `AWS::EntityResolution::IdMappingWorkflow`, `AWS::EntityResolution::IdNamespace`

可使用以下範本：

- 匹配工作流

建立MatchingWorkflow物件，儲存要執行之資料處理工作的組態。

如需詳細資訊，請參閱下列主題：

[AWS::EntityResolution::MatchingWorkflow](#) 《AWS CloudFormation 使用者指南》中的

[CreateMatchingWorkflow](#)在「AWS Entity Resolution API參考」中

- 綱要對映

建立結構描述對應，定義輸入客戶記錄表格的結構描述。

如需詳細資訊，請參閱下列主題：

[AWS::EntityResolution::SchemaMapping](#) 《AWS CloudFormation 使用者指南》中的

[CreateSchemaMapping](#)在「AWS Entity Resolution API參考」中

- ID 對應工作流程

建立IdMappingWorkflow物件，儲存要執行之資料處理工作的組態。

如需詳細資訊，請參閱下列主題：

[AWS::EntityResolution::IdMappingWorkflow](#) 《AWS CloudFormation 使用者指南》中的

[CreateIdMappingWorkflow](#)在「AWS Entity Resolution API參考」中

- ID 命名空間

建立IdNamespace物件，儲存說明資料集及其使用方式的中繼資料。

如需詳細資訊，請參閱下列主題：

[AWS::EntityResolution::IdNamespace](#) 《AWS CloudFormation 使用者指南》中的

[CreateIdNamespace](#)在「AWS Entity Resolution API參考」中

- PolicyStatement

建立 PolicyStatement 物件。

如需詳細資訊，請參閱下列主題：

[AWS::EntityResolution::PolicyStatement](#) 《AWS CloudFormation 使用者指南》中的

[AddPolicyStatement](#)在「AWS Entity Resolution API參考」中

## 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 指令行介面使用者指南](#)

## 的配額 AWS Entity Resolution

您的 AWS 帳戶 具有每個的預設配額，先前稱為限制 AWS 服務。除非另有說明，否則每個配額都是區域特定規定。您可以為某些配額請求增加，但其他配額無法增加。

若要檢視的配額 AWS Entity Resolution，請開啟 [Service Quotas 主控台](#)。在導覽窗格中，選擇 AWS 服務，然後選擇 AWS Entity Resolution。

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 中尚無法使用配額，請使用[限制增加表單](#)。

您的 AWS 帳戶 具有與相關的下列配額 AWS Entity Resolution。

名稱	預設	可調整	描述
並行 ID 映射任務	1	否	在目前 中可同時處理的 ID 映射任務數目上限 AWS 區域。
並行比對任務	1	否	在目前 中可同時處理的相符任務數量上限 AWS 區域。
並行提供者服務比對任務	1	否	在目前 中可同時處理的提供者服務比對任務數量上限 AWS 區域。
資料輸入	20	否	這是您要在相符工作流程中使用的輸入資料表清單。每個輸入對應於 AWS Glue 輸入資料表中的資料欄，其中包含資料欄名稱和 AWS Entity Resolution 用於比對目的的其他資訊。輸入必須包含唯一 ID 加上至少一個額外的輸入欄位。
資料輸出	750	否	這是 OutputAttribute 物件清單，每個物件都有欄位名稱和雜湊。這些物件都代表要包含在 AWS Glue 輸出資料表中的資料欄，以及您是否希望雜湊資料欄中的值。
資料結構描述	25	否	資料結構描述輸入欄位的數量上限。

名稱	預設	可調整	描述
ID 映射工作流程	10	<a href="#">是</a>	您可以在目前中在此 AWS 帳戶中建立的 ID 映射工作流程數目上限 AWS 區域。
ID 命名空間	10	是	您可以在目前中在此 AWS 帳戶中建立的 ID 命名空間數目上限 AWS 區域。
相符 IDs	500	否	每個工作負載一個 MatchID 下可合併的記錄數目上限。
比對規則	15	否	對於規則型比對，這是產生相符記錄集的套用規則編號。這是相符工作流程中繼資料的一部分，該中繼資料將包含在輸出中。
比對工作流程	10	<a href="#">是</a>	相符工作流程的數量上限。
每個工作流程的規則數目	15	否	每個相符工作流程的規則數目上限。
GetMatchId API 請求率	50	<a href="#">是</a>	每秒GetCustomerID API請求數上限。
結構描述映射	50	<a href="#">是</a>	您可以在目前 AWS 區域中的此帳戶中建立的結構描述映射數量上限。
跨規則集每個的唯一相符金鑰	15	否	每個規則集的唯一相符金鑰數目上限。比對金鑰會指示 AWS Entity Resolution 哪些輸入欄位會被視為類似資料，哪些會被視為不同資料。這有助於 AWS Entity Resolution 自動設定規則型比對規則，並比較儲存在不同輸入欄位中的類似資料。

## API 調節配額

資源	速率限制	描述
CreateMatchingWorkflow 請求率	5 TPS	每秒的CreateMatchingWorkflow API呼叫數量上限。
DeleteMatchingWorkflow 請求速率	5 TPS	每秒的DeleteMatchingWorkflow API呼叫數量上限。
GetMatchingWorkflow 請求速率	5 TPS	每秒的GetMatchingWorkflow API呼叫數量上限。
ListMatchingWorkflows 請求速率	5 TPS	每秒的ListMatchingWorkflows API呼叫數量上限。
UpdateMatchingWorkflow 請求速率	5 TPS	每秒的UpdateMatchingWorkflow API呼叫數量上限。
CreateSchemaMapping 請求速率	5 TPS	每秒的CreateSchemaMapping API呼叫數量上限。
DeleteSchemaMapping 請求速率	5 TPS	每秒的DeleteSchemaMapping API呼叫數量上限。
GetSchemaMapping 請求率	5 TPS	每秒的GetSchemaMapping API呼叫數量上限。
ListSchemaMappings 請求速率	5 TPS	每秒的ListSchemaMappings API呼叫數量上限。

資源	速率限制	描述
UpdateSchemaMapping 請求速率	5 TPS	每秒的UpdateSchemaMapping API呼叫數量上限。
GetPartnerComponent 請求速率	5 TPS	每秒的GetPartnerComponent API呼叫數量上限。
ListPartnerComponents 請求速率	5 TPS	每秒的ListPartnerComponents API呼叫數量上限。
TagResource 請求速率	5 TPS	每秒的TagResource API呼叫數量上限。
UntagResource 請求率	5 TPS	每秒UntagResource API呼叫數量上限。
ListTagsForResource 請求率	5 TPS	每秒的ListTagsForResource API呼叫數量上限。
CreateIdMappingWorkflow 請求速率	5 TPS	每秒CreateIdMappingWorkflow API呼叫數量上限。
DeleteIdMappingWorkflow 請求率	5 TPS	每秒的DeleteIdMappingWorkflow API呼叫數量上限。
GetIdMappingWorkflow 請求率	5 TPS	每秒GetIdMappingWorkflow API呼叫數量上限。
ListIdMappingWorkflow 請求速率	5 TPS	每秒的ListIdMappingWorkflow API呼叫數量上限。

資源	速率限制	描述
UpdateIdMappingWorkflow 請求速率	5 TPS	每秒的UpdateIdMappingWorkflow API呼叫數量上限。
ListProviderServices 請求率	5 TPS	每秒的ListProviderServices API呼叫數量上限。
GetProviderService 請求速率	5 TPS	每秒的GetProviderService API呼叫數量上限。
CreateIdNamespace 請求速率	5 TPS	每秒的CreateIdNamespace API呼叫數量上限。
DeleteIdNamespace 請求率	5 TPS	每秒的DeleteIdNamespace API呼叫數量上限。
GetIdNamespace 請求速率	5 TPS	每秒的GetIdNamespace API呼叫數量上限。
ListIdNamespaces 請求速率	5 TPS	每秒ListIdNamespaces API呼叫數量上限。
UpdateIdNamespace 請求率	5 TPS	每秒的UpdateIdNamespace API呼叫數量上限。
AddPolicyStatement 請求速率	5 TPS	每秒的AddPolicyStatement API呼叫數量上限。
DeletePolicyStatement 請求速率	5 TPS	每秒的DeletePolicyStatement API呼叫數量上限。

資源	速率限制	描述
GetPolicy 請求率	5 TPS	每秒的GetPolicy API呼叫數量上限。
PutPolicy 請求率	5 TPS	每秒的PutPolicy API呼叫數量上限。
GetMatchingJob 請求率	10 TPS	每秒的GetMatchingJob API呼叫數量上限。
ListMatchingJobs 請求速率	5 TPS	每秒的ListMatchingJobs API呼叫數量上限。
StartMatchingJob 請求率	5 TPS	每秒的StartMatchingJob API呼叫數量上限。
GetMatchId 請求速率	50 TPS	每秒的GetMatchId API呼叫數量上限。
GetIdMappingJob 請求速率	10 TPS	每秒的GetIdMappingJob API呼叫數量上限。
ListIdMappingJobs 請求率	5 TPS	每秒ListIdMappingJobs API呼叫數量上限。
StartIdMappingJob 請求率	5 TPS	每秒的StartIdMappingJob API呼叫數量上限。
BatchDeleteUniqueId 請求率	5 TPS	每秒的BatchDeleteUniqueId API呼叫數量上限。

# AWS Entity Resolution 使用者指南的文件歷史記錄

下表說明的文件版本 AWS Entity Resolution。

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
<a href="#">供應商整合</a>	僅文件更新。客戶可以瞭解如何整合為提供者服務 AWS Entity Resolution。	2024年8月8日
<a href="#">ID 對應工作流程 — 更新</a>	客戶現在可以使用比對規則，在 ID 對應工作流程中轉譯第一方資料。	2024年7月23 日
<a href="#">匹配工作流程 — 更新</a>	客戶現在可以從規則式或以 ML 為基礎的比對工作流程中刪除記錄，以協助遵守資料管理法規。	2024年4月8日
<a href="#">ID 對應工作流程 — 更新</a>	客戶現在可以跨多個使用 ID 對應工作流程 AWS 帳戶。	2024年4月2日
<a href="#">AWS CloudFormation 資源-新的和更新的資源</a>	AWS實體解析已新增下列資源：AWS::EntityResolution::IdNamespace AWS::EntityResolution::PolicyStatement 並更新了下列資源：AWS::EntityResolution::IdMappingWorkflow	2024年4月2日
<a href="#">尋找符合 ID</a>	客戶現在可以找到已處理規則型工作流程的對應比對 ID 和相關規則。	2024年3月25日

[匹配工作流程 — 更新](#)

AWS Entity Resolution 現在支援PII以 LiveRamp 提供者服務 RAMPID 務為基礎的比對工作流程中的指派。

2024年2月12日

[AWS PrivateLink](#)

AWS Entity Resolution 現在支援額外的資料安全性 AWS PrivateLink ，可協助客戶私下存取託管的服務 AWS。

2023 年 10 月 20 日

[AWS CloudFormation 資源 — 新的和更新的資源](#)

AWS Entity Resolution 已新增下列資源：`AWS::EntityResolution::IdMappingWorkflow` 並更新下列資源：`AWS::EntityResolution::MatchingWorkflow` 和 `AWS::EntityResolution::Schemamapping` 。

2023 年 10 月 19 日

[更新至現有政策](#)

下列新權限已新增至 `AWS::EntityResolution::ConsoleFullAccess` 受管理的策略：`ADXReadAccess` 和 `ManageEventBridgeRules` 。

2023 年 10 月 16 日

[結構描述對應 — 更新](#)

客戶現在可以編輯和更新現有的資料結構描述。

2023 年 10 月 16 日

[匹配工作流程 — 更新](#)

客戶現在可以選擇偏好的資料提供者服務，以協助比對和連結其資料。

2023 年 10 月 16 日

---

<a href="#">ID 對應工作流程</a>	客戶可以使用此新工作流程來指定 ID 對應詳細資訊、選擇所需的 ID 對應方式，以及指定資料輸入和輸出欄位。	2023 年 10 月 16 日
<a href="#">AWS CloudFormation 整合</a>	AWS Entity Resolution 現在整合了 AWS CloudFormation.	2023 年 8 月 24 日
<a href="#">AWS 受管策略更新-新策略</a>	AWS Entity Resolution 新增了兩個新的受管理策略。	2023 年 8 月 18 日
<a href="#">初始版本</a>	AWS Entity Resolution 使用者指南的初始版本	2023 年 7 月 26 日

# AWS Entity Resolution 詞彙表

## Amazon Resource Name ( ARN )

資源的唯一識別碼 AWS 。ARNs 當您需要在整個 中明確指定資源時 AWS Entity Resolution ，例如在 AWS Entity Resolution 政策、Amazon Relational Database Service ( Amazon RDS ) 標籤和API呼叫中，是必要的。

## 自動處理

比對工作流程任務的處理節奏選項，可在資料輸入變更時自動在 上執行。

此選項僅適用於[規則型比對](#)。

根據預設，相符工作流程任務的處理節奏會設定為[手動](#)，使其可隨需執行。您可以設定自動處理，以便在資料輸入變更時自動執行相符的工作流程任務。這可保留相符的工作流程輸出 up-to-date。

## AWS KMS key ARN

這是靜態加密的 AWS KMS Amazon Resource Name ( ARN )。如果未提供，系統將使用 AWS Entity Resolution 受管KMS金鑰。

## Cleartext

未受到密碼編譯保護的資料。

## 可信度層級 ( ConfidenceLevel )

對於 ML 比對，這是當 ML 識別相符的記錄集 AWS Entity Resolution 時，套用的可信度層級。這是將包含在輸出中的[相符工作流程中繼資料](#)的一部分。

## 解密

將加密資料轉換回原始格式的程序。只有在您可以存取秘密金鑰時，才能執行解密。

## 加密

將資料編碼為使用稱為金鑰的秘密值隨機顯示的形式的程序。無法在無法存取金鑰的情況下判斷原始純文字。

### Group name (群組名稱)

群組名稱會參考整個輸入欄位群組，並可協助您將剖析的資料分組在一起，以達成比對目的。

例如，如果有三個輸入欄位：**first\_name**、**middle\_name**和**last\_name**，您可以輸入群組名稱作為比對和輸出**full\_name**，將它們分組在一起。

## 雜湊

雜湊表示套用密碼編譯演算法，該演算法會產生固定大小的不可逆且唯一的字元字串，稱為雜湊。

AWS Entity Resolution 使用安全雜湊演算法 256 位元 (SHA256) 雜湊通訊協定，並將輸出 32 位元組字元字串。在中 AWS Entity Resolution，您可以選擇是否要在輸出中雜湊資料值。

### 雜湊通訊協定 ( HashingProtocol )

AWS Entity Resolution 使用 Secure Hash Algorithm 256 位元 (SHA256) 雜湊通訊協定，並將輸出 32 位元組字元字串。這是將包含在輸出中的[相符工作流程中繼資料](#)的一部分。

## ID 映射方法

您希望如何執行 ID 映射。

有兩種 ID 映射方法：

- 規則型 – 使用比對規則，將來源的第一方資料轉譯為 ID 映射工作流程中的目標的方法。
- 提供者服務 – 使用提供者服務將第三方編碼資料從來源轉譯至 ID 映射工作流程中目標的方法。

AWS Entity Resolution 目前支援 LiveRamp 作為提供者服務型 ID 映射方法。您必須擁有 LiveRamp 至的訂閱 AWS Data Exchange，才能使用此方法。如需詳細資訊，請參閱[步驟 1：訂閱提供者服務 AWS Data Exchange](#)。

## ID 映射工作流程

根據指定的 ID 映射方法，將資料從輸入資料來源映射到輸入資料目標的資料處理任務。它會產生 ID 映射表。此工作流程需要您指定 [ID 映射方法](#)，以及您要從來源轉譯到目標的輸入資料。

您可以設定 ID 映射工作流程，在您自己的 中 AWS 帳戶 或跨兩個 執行 AWS 帳戶。

## ID 命名空間

中的資源包含中繼資料 AWS Entity Resolution，解釋多個 AWS 帳戶 資料集，以及如何在 [ID 映射工作流程](#) 中使用這些資料集。

ID 命名空間有兩種類型：SOURCE 和 TARGET。SOURCE 包含將在 ID 映射工作流程中處理的來源資料的組態。TARGET 包含所有來源將解析的目標資料的組態。若要定義您要在兩個 之間解析的輸入資料 AWS 帳戶，請建立 ID 命名空間來源和 ID 命名空間目標，以將資料從一組 ( SOURCE ) 轉換為另一組 ( ) TARGET。

在您和其他成員建立 ID 命名空間並執行 ID 映射工作流程之後，您可以在 中加入協作 AWS Clean Rooms，以在 ID 映射資料表上執行多資料表聯結，並分析資料。

如需詳細資訊，請參閱《AWS Clean Rooms 使用者指南》<https://docs.aws.amazon.com/clean-rooms/latest/userguide/what-is.html>。

## 輸入欄位

輸入欄位對應於 AWS Glue 輸入資料表中的資料欄名稱。

## 輸入來源 ARN ( InputSourceARN )

為 AWS Glue 資料表輸入產生的 Amazon Resource Name ( ARN )。這是將包含在輸出中的[相符工作流程中繼資料](#)的一部分。

## 輸入類型

輸入資料的類型。您可以從預先設定的值清單中選取，例如名稱、地址、電話號碼或電子郵件地址。輸入類型會說明您要呈現的 AWS Entity Resolution 資料類型，以便正確分類和標準化資料。

## 機器學習型比對

機器學習型比對（ML 比對）會尋找可能不完整或看起來不完全相同的資料相符項目。ML 比對是預設程序，會嘗試比對您輸入所有資料的記錄。ML 比對會傳回每組相符資料的[比對 ID](#) 和[可信度](#)。

## 手動處理

比對工作流程任務的處理節奏選項，可視需要執行。

此選項預設為 `Manual`，且適用於[規則型比對](#)和[機器學習型比對](#)。

## Many-to-Many 比對

Many-to-many 比對會比較類似資料的多個執行個體。已指派相同相符金鑰的輸入欄位中的值會彼此比對，無論它們位於相同的輸入欄位還是不同的輸入欄位。

例如，您可能有多個電話號碼輸入欄位，例如 `mobile_phone` 和 `home_phone` 具有相同相符金鑰「電話」。使用 many-to-many 比對將 `mobile_phone` 輸入欄位中的資料與 `mobile_phone` 輸入欄位中的資料和 `home_phone` 輸入欄位中的資料進行比較。

比對規則會使用與（或）操作相同的比對索引鍵評估多個輸入欄位中的資料，比對 one-to-many 則會比較多個輸入欄位的值。這表示如果兩個記錄之間有任何 `mobile_phone` 或 `home_phone` 的組合相符，則「電話」相符金鑰會傳回相符項目。對於相符金鑰「電話」尋找相符項目，`Record One mobile_phone = Record Two mobile_phone` 或 `Record One mobile_phone = Record Two home_phone` OR `Record One home_phone = Record Two home_phone` 或 `Record One home_phone = Record Two mobile_phone`。

## 比對 ID MatchID )

對於規則型比對和 ML 比對，這是由產生 AWS Entity Resolution 並套用至每個比對記錄集的 ID。這是將包含在輸出中的[相符工作流程中繼資料](#)的一部分。

## 比對金鑰（ MatchKey ）

比對金鑰會指示要將 AWS Entity Resolution 哪些輸入欄位視為類似資料，以及要將哪些欄位視為不同資料。這有助於 AWS Entity Resolution 自動設定規則型比對規則，並比較儲存在不同輸入欄位中的類似資料。

如果資料中有多個電話號碼資訊類型，例如mobile\_phone輸入欄位和您要比較的home\_phone輸入欄位，您可以將相符金鑰“Phone”提供給他們。然後，可以設定規則型比對，使用「或」陳述式，在所有輸入欄位中使用「電話」比對金鑰來比較資料（請參閱[One-to-One 比對](#)工作流程中的比對與[Many-to-Many 比對](#)定義一節）。

如果您想要規則型比對完全分開考慮不同類型的電話號碼資訊，您可以建立更具體的比對金鑰，例如「Mobile\_Phone」和「Home\_Phone」。然後，在設定相符的工作流程時，您可以指定每個電話相符金鑰在規則型相符中使用的方式。

如果特定輸入欄位未指定 MatchKey 任何，則無法用於比對，但可透過比對工作流程程序進行，並在需要時進行輸出。

## 比對金鑰名稱

指派給 Match Key 的名稱。

## 比對規則（ MatchRule ）

對於規則型比對，這是產生相符記錄集的套用規則編號。這是將包含在輸出中的[相符工作流程中繼資料](#)的一部分。

## 相符

合併和比較不同輸入欄位、資料表或資料庫的資料，並根據滿足特定比對條件（例如，透過比對規則或模型）來判斷哪些資料相似或相符的程序。

## 比對工作流程

您設定以指定要比對的輸入資料，以及如何執行比對的程序。

## 比對工作流程描述

您可以選擇輸入的相符工作流程的選用描述。如果建立多個工作流程，描述可協助您區分相符的工作流程。

## 比對工作流程名稱

您指定的相符工作流程的名稱。

**Note**

相符的工作流程名稱必須是唯一的。它們不能具有相同的名稱，否則將會傳回錯誤。

## 比對工作流程中繼資料

比對工作流程任務 AWS Entity Resolution 期間由產生和輸出的資訊。輸出時需要此資訊。

## 標準化 ( ApplyNormalization )

選擇是否要標準化結構描述中定義的輸入資料。標準化會移除額外的空格和特殊字元，並將資料標準化為小寫格式。

例如，如果輸入欄位的輸入類型為 PHONE\_NUMBER，且輸入資料表中的值格式化為 (123) 456-7890，AWS Entity Resolution 會將值標準化為 1234567890。

下列各節說明我們的標準標準化規則。如需特定 ML 型比對，請參閱 [標準化 \( ApplyNormalization \) – 僅限 ML](#)。

### 主題

- [名稱](#)
- [電子郵件](#)
- [Phone](#)
- [Address](#)
- [雜湊](#)
- [Source\\_ID](#)

### 名稱

- TRIM = 修剪前後空白
- LOWERCASE = 小寫所有字母字元
- CONVERT\_ACCENT = 將重音字母轉換為一般字母
- REMOVE\_ALL\_NON\_ALPHA = 移除所有非字母字元 **【a-zA-Z】**

## 電子郵件

- TRIM = 修剪前後空格
- LOWERCASE = 小寫所有字母字元
- CONVERT\_ACCENT = 將重音字母轉換為一般字母
- EMAIL\_ADDRESS\_UTIL\_NORM = 從使用者名稱中移除任何點 ( . )、移除使用者名稱中加號 ( + ) 之後的任何內容，以及標準化常見的網域變化
- REMOVE\_ALL\_NON\_EMAIL\_CHARS = 移除所有 non-alpha-numeric字元 **【a-zA-Z0-9】** 和 **【.@-】**

## Phone

- TRIM = 修剪前後空白
- REMOVE\_ALL\_NON\_NUMERIC = 移除所有非數字字元 **【0-9】**
- REMOVE\_ALL\_LEADING\_ZEROES = 移除所有前導零
- ENSURE\_PREFIX\_WITH\_MAP, "phonePrefixMap" = 檢查每個電話號碼，並嘗試將其與 中的模式比對 phonePrefixMap。如果找到相符項目，則規則會新增或修改電話號碼的字首，以確保其符合地圖中指定的標準化格式。

## Address

- TRIM = 修剪前後空白
- LOWERCASE = 小寫所有字母字元
- CONVERT\_ACCENT = 將重音字母轉換為一般字母
- REMOVE\_ALL\_NON\_ALPHA = 移除所有非字母字元 **【a-zA-Z】**
- RENAME\_WORDS 使用 ADDRESS\_RENAME\_WORD\_MAP = 使用來自 [ADDRESS\\_RENAME\\_WORD\\_MAP](#) 的單字取代地址字串中的單字
- RENAME\_DELIMITERS 使用 ADDRESS\_RENAME\_DELIMITER\_MAP = 使用來自 [ADDRESS\\_RENAME\\_DELIMITER\\_MAP](#) 的字串取代地址字串中的分隔符號
- RENAME\_DIRECTIONS 使用 ADDRESS\_RENAME\_DIRECTION\_MAP = 將地址字串中的分隔符號取代為來自 [ADDRESS\\_RENAME\\_DIRECTION\\_MAP](#) 的字串
- RENAME\_NUMBERS 使用 ADDRESS\_RENAME\_NUMBER\_MAP = 將地址字串中的數字取代為來自 [ADDRESS\\_RENAME\\_NUMBER\\_MAP](#) 的字串

- `RENAME_SPECIAL_CHARS` 使用 `ADDRESS_RENAME_SPECIALCHAR_MAP` = 使用來自 [ADDRESS\\_RENAME\\_SPECIAL\\_](#) 的字串取代地址字串中的特殊字元 `CHARMAP`

## ADDRESS\_RENAME\_WORD\_MAP

這些是標準化地址字串時將重新命名的單字。

```
"avenue": "ave",
"bouled": "blvd",
"circle": "cir",
"circles": "cirs",
"court": "ct",
"centre": "ctr",
"center": "ctr",
"drive": "dr",
"freeway": "fwy",
"frwy": "fwy",
"highway": "hwy",
"lane": "ln",
"parks": "park",
"parkways": "pkwy",
"pky": "pkwy",
"pkway": "pkwy",
"pkwys": "pkwy",
"parkway": "pkwy",
"parkwy": "pkwy",
"place": "pl",
"plaza": "plz",
"plza": "plz",
"road": "rd",
"square": "sq",
"squ": "sq",
"sqr": "sq",
"street": "st",
"str": "st",
"str.": "strasse"
```

## ADDRESS\_RENAME\_DELIMITER\_MAP

這些是標準化地址字串時將重新命名的分隔符號。

```
",": " ",
```

```
".": " ",  
"[": " ",  
"]": " ",  
"/": " ",  
"-": " ",  
"#": " number "
```

## ADDRESS\_RENAME\_DIRECTION\_MAP

這些是標準化地址字串時將重新命名的方向識別符。

```
"east": "e",  
"north": "n",  
"south": "s",  
"west": "w",  
"northeast": "ne",  
"northwest": "nw",  
"southeast": "se",  
"southwest": "sw"
```

## ADDRESS\_RENAME\_NUMBER\_MAP

這些是在標準化地址字串時將重新命名的數字字串。

```
"número": "number",  
"numero": "number",  
"no": "number",  
"núm": "number",  
"num": "number"
```

## ADDRESS\_RENAME\_SPECIAL\_CHAR\_MAP

這些是特殊字元字串，會在標準化地址字串時重新命名。

```
"ß": "ss",  
"ä": "ae",  
"ö": "oe",  
"ü": "ue",  
"ø": "o",  
"æ": "ae"
```

## 雜湊

- TRIM = 修剪前後空白

## Source\_ID

- TRIM = 修剪前後空白

## 標準化 ( ApplyNormalization ) – 僅限 ML

選擇是否要標準化結構描述中定義的輸入資料。標準化會移除額外的空格和特殊字元，並將資料標準化為小寫格式。

例如，如果輸入欄位的輸入類型為 NAME，且輸入資料表中的值格式化為 Johns Smith，AWS Entity Resolution 會將值標準化為 john smith。

下列各節說明[以機器學習為基礎的相符工作流程](#)的標準化規則。

### 主題

- [名稱](#)
- [電子郵件](#)
- [Phone](#)

## 名稱

- TRIM = 修剪前後空格
- LOWERCASE = 小寫所有字母字元

## 電子郵件

- LOWERCASE = 小寫所有字母字元
- 僅 ( 以 表示 ) 使用 @ 符號取代 ( 區分大小寫 )
- 移除值中的任何位置的所有空格
- "< >" 如果存在，則移除在第一個 之外的所有項目

## Phone

- TRIM = 修剪前後空格
- REMOVE\_ALL\_NON\_NUMERIC = 移除所有非數字字元【0-9】
- REMOVE\_ALL\_LEADING\_ZEROES = 移除所有前導零
- ENSURE\_PREFIX\_WITH\_MAP, "phonePrefixMap" = 檢查每個電話號碼，並嘗試將其與 中的模式比對 phonePrefixMap。如果找到相符項目，則規則會新增或修改電話號碼的字首，以確保其符合地圖中指定的標準化格式。

## One-to-One 比對

One-to-one 比對會比較類似資料的單一執行個體。相同輸入欄位中具有相同相符索引鍵和值的輸入欄位會互相比對。

例如，您可能有多個電話號碼輸入欄位，例如 mobile\_phone 和 home\_phone，其具有相同的相符金鑰「電話」。使用 one-to-one 比對將 mobile\_phone 輸入欄位中的資料與 mobile\_phone 輸入欄位中的資料進行比較，並將 home\_phone 輸入欄位中的資料與 home\_phone 輸入欄位中的資料進行比較。mobile\_phone 輸入欄位中的資料不會與 home\_phone 輸入欄位中的資料進行比較。

比對規則會使用與（或）操作相同的比對索引鍵評估多個輸入欄位中的資料，比對 one-to-many 則會比較單一輸入欄位內的值。這表示如果兩個記錄之間有 mobile\_phone 或 home\_phone 相符，則「電話」相符金鑰會傳回相符項目。對於相符金鑰「電話」尋找相符項目，Record One mobile\_phone = Record Two mobile\_phone 或 Record One home\_phone = Record Two home\_phone。

比對規則會使用具有（和）操作的不同比對金鑰評估輸入欄位中的資料。如果您希望規則型比對完全分開考慮不同類型的電話號碼資訊，您可以建立更具體的比對金鑰，例如「mobile\_phone」和「home\_phone」。如果您想要在規則中使用兩個相符金鑰來尋找相符項目，Record One mobile\_phone = Record Two mobile\_phone AND Record One home\_phone = Record Two home\_phone。

## 輸出

物件清單，每個 OutputAttribute 物件都有欄位名稱和雜湊。這些物件都代表要包含在 AWS Glue 輸出資料表中的資料欄，以及您是否希望雜湊資料欄中的值。

## OutputS3Path

AWS Entity Resolution 將寫入輸出資料表的 S3 目的地。

## OutputSourceConfig

物件清單，每個 OutputSource 物件都有 OutputS3Path ApplyNormalization 和 Output 等欄位。

## 提供者服務型比對

提供者服務型比對是設計來比對、連結和增強您記錄的程序，其使用偏好的資料服務提供者和授權資料集。您必須透過 AWS Data Exchange 與提供者服務進行訂閱，才能使用此比對技術。

AWS Entity Resolution 目前與下列資料服務供應商整合：

- LiveRamp
- TransUnion
- UID 2.0

## 規則型比對

規則型比對是設計用來尋找確切比對的程序。規則型比對是一套階層式的瀑布比對規則，由根據您輸入的資料建議 AWS Entity Resolution，並完全由您設定。規則條件中提供的所有相符金鑰都必須完全相符，才能宣告相符的比較資料，以及要輸出的關聯中繼資料。規則型比對會傳回每個相符資料集的 [比對 ID](#) 和規則編號。

我們建議定義可唯一識別實體的規則。排序您的規則，先尋找更精確的相符項目。

例如，假設您有兩個規則：規則 1 和規則 2。

這些規則具有下列相符金鑰：

- 規則 1 包含全名和地址
- 規則 2 包括全名、地址和電話

由於規則 1 會先執行，因此規則 2 不會找到相符項目，因為規則 1 會找到這些相符項目。

若要尋找以電話區分的相符項目，請重新排序規則，如下所示：

- 規則 2 包括全名、地址和電話
- 規則 1 包含全名和地址

## 結構描述

用於定義資料集如何組織和連線的結構或配置的術語。

## 結構描述描述

您可以選擇輸入的結構描述的描述。如果您建立多個結構描述映射，描述可協助您區分。

## 結構描述名稱

結構描述的名稱。

### Note

結構描述名稱必須是唯一的。它們不能具有相同的名稱，否則將會傳回錯誤。

## 結構描述映射

中的結構描述映射 AWS Entity Resolution 是您告知 AWS Entity Resolution 如何解譯資料以進行比對的程序。您可以定義 AWS Entity Resolution 要讀取至相符工作流程的輸入資料表結構描述。

## 結構描述映射 ARN

為[結構描述映射](#)產生的 Amazon Resource Name ( ARN )。

## 唯一 ID

您指定且必須指派給讀取之每一列輸入資料的唯一識別碼 AWS Entity Resolution 。

Example

例如，**Primary\_key**、**Row\_ID** 或 **Record\_ID**。

唯一 ID 資料欄為必填。

唯一 ID 必須是單一資料表內的唯一識別符。

在不同資料表中，唯一 ID 可以具有重複值。

執行[相符的工作流程](#)時，如果唯一 ID：

- 未指定
- 在同一資料表中不是唯一的
- 跨來源的屬性名稱重疊。
- 超過 38 個字元（僅限規則型相符工作流程）

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。