aws

使用者指南

Amazon Fraud Detector

版本 latest

Amazon Fraud Detector: 使用者指南

Table of Contents

什麼是 Amazon Fraud Detector？

Amazon Fraud Detector 是全受管的詐騙偵測服務，可自動偵測線上潛在詐騙活動。這些活動包括未經授權的交易和建立虛假帳戶。Amazon Fraud Detector 的運作方式是使用機器學習來分析您的資料。它以一種基於 Amazon 20 多年欺詐檢測經驗豐富的專業知識來實現這一目標。

您可以使用 Amazon Fraud Detector 建立自訂的詐騙偵測模型、新增決策邏輯以解釋模型的詐騙評估，以及指派結果 (例如通過或傳送以供檢閱) 以進行每個可能的詐騙評估。使用 Amazon Fraud Detector，您不需要機器學習專業知識即可偵測詐騙活動。

要開始使用，請收集並準備您在組織中收集的欺詐數據。然後，Amazon Fraud Detector 會使用此資料代表您訓練、測試和部署自訂詐騙偵測模型。作為此程序的一部分，Amazon Fraud Detector 使用機器學習模型，這些模型已從 Amazon 自己學習詐騙模式，以AWS及 Amazon 自己的詐騙專業知識來評估您的詐騙資料，並產生模型分數和模型效能資料。您可以設定決策邏輯來解譯模型的分數，並指派如何處理每個詐騙評估的結果。

優勢

Amazon Fraud Detector 提供下列好處。這些好處使您可以快速檢測欺詐行為，而無需投入建立和維護欺詐管理系統所需的時間和資源。

自動建立詐騙模型

Amazon 詐騙偵測器的詐騙偵測模型是全自動化的機器學習模型，可根據您的特定業務需求進行客製化。您可以使用 Amazon Fraud Detector 模型來識別任何線上交易中的潛在詐騙行為，例如建立新帳戶、線上付款和訪客結帳。

由於詐騙模型是透過自動化程序建立的，因此您可以放棄許多與建立和訓練模型相關的步驟。這些步驟包括資料驗證和擴充、功能工程、演算法選擇、超參數調整和模型部署。

若要使用 Amazon Fraud Detector 建立詐騙偵測模型，您只需上傳公司的歷史詐騙資料集，然後選取模型類型。然後，Amazon Fraud Detector 會自動為您的使用案例尋找最適合的詐騙偵測演算法，並建立模型。您不需要了解編碼或具備機器學習專業知識即可建立詐騙偵測模型。

發展和學習的欺詐模式

欺詐檢測模型必須不斷發展，以跟上不斷變化的欺詐環境。Amazon Fraud Detector 會透過計算帳戶年齡、自上次活動以來的時間和活動計數等資訊來自動執行此動作。結果是，您的模型可以了解經常進行

交易的受信任客戶和欺詐者的持續嘗試之間的差異。這有助於在再訓練階段之間更長時間維持模型的效能。

詐騙模型效能視覺化

使用您提供的資料訓練模型之後，Amazon Fraud Detector 會驗證您的模型效能。它還為您提供了可視化工具來評估性能。對於您訓練的每個模型，您都可以查看模型效能分數、評分分佈圖表、混淆矩陣、臨界值表格，以及您提供的所有輸入，並根據它們對模型效能的影響進行排名。使用這些效能工具，您可以瞭解模型的執行方式，以及哪些輸入會驅動模型效能。如果需要，您可以調整模型以改善其整體效能。

詐騙預測

Amazon Fraud Detector 會為您組織的業務活動產生詐騙預測。欺詐預測是對商業活動的欺詐風險的評估。Amazon Fraud Detector 會使用預測邏輯與活動相關聯的資料來產生預測。您在建立詐騙偵測模型時提供此資料。您可以即時取得單一活動的詐騙預測，或離線取得一組活動的詐騙預測。

欺詐預測說明可視化

Amazon Fraud Detector 會產生預測說明，做為詐騙預測程序的一部分。預測說明可讓您深入瞭解用於訓練模型的每個資料元素如何影響模型的詐騙預測分數。使用可視化工具（例如表格和圖表）提供預測說明。您可以使用這些工具直觀地識別每個資料元素對預測分數的影響程度。然後，您可以使用此信息來分析數據集中的欺詐模式並檢測偏見（如果有）。最後，您還可以在手動欺詐調查過程中使用預測說明來識別主要風險指標。這有助於您縮小導致誤報預測的根本原因。

以規則為基礎的動作

在您的詐騙偵測模型經過訓練之後，您可以新增規則來對評估的資料採取動作，例如接受資料、傳送資料以供審核或收集更多資料。規則是告知 Amazon Fraud Detector 如何在詐騙預測期間解譯資料的條件。例如，您可以建立標記待審核的可疑客戶帳戶的規則。如果檢測到的模型分數大於預定的閾值，並且帳戶付款的授權碼（AUTH_CODE）無效，則可以將此規則設置為啟動。

核心概念與術語

以下是 Amazon Fraud Detector 中使用的核心概念和術語清單：

事件

活動是您組織的業務活動，經過欺詐風險評估。Amazon Fraud Detector 會針對事件產生詐騙預測。

標籤

標籤會將單一事件分類為詐騙或合法事件。標籤用於訓練 Amazon Fraud Detector 中的機器學習模型。

實體

實體代表誰正在執行事件。您提供實體 ID 作為公司欺詐數據的一部分，以指示執行該事件的特定實體。

事件類型

事件類型會定義傳送至 Amazon Fraud Detector 的事件結構。這包括作為事件一部分傳送的資料、執行事件的實體 (例如客戶)，以及將事件分類的標籤。事件類型範例包括線上付款交易、帳戶註冊和驗證。

實體類型

實體類型會將實體分類。範例分類包括客戶、商家或帳戶。

事件資料集

事件資料集是貴公司特定商業活動或事件的歷史資料。例如，您公司的活動可能是在線帳戶註冊。來自單一事件 (註冊) 的資料可能包括相關聯的 IP 位址、電子郵件地址、帳單地址和事件時間戳記。您可以將事件資料集提供給 Amazon Fraud Detector，以建立和訓練詐騙偵測模型。

模型

模型是機器學習演算法的輸出。這些演算法會在程式碼中實作，並在您提供的事件資料上執行。

模型類型

模型類型定義模型訓練期間使用的演算法、擴充和特徵轉換。它還定義了訓練模型的數據需求。這些定義可針對特定類型的詐騙最佳化您的模型。您可以指定建立模型時要使用的模型類型。

模型訓練

模型訓練是使用提供的事件資料集來建立可預測詐騙事件的模型的程序。模型訓練程序中的所有步驟都是完全自動化的。這些步驟包括資料驗證、資料轉換、特徵工程、演算法選擇和模型最佳化。

模型分數

模型分數是貴公司歷史詐騙資料的評估結果。在模型訓練過程中，Amazon Fraud Detector 會評估資料集的詐騙活動，並產生介於 0 到 1000 之間的分數。對於此分數，0 代表低欺詐風險，而 1000 代表最高的欺詐風險。分數本身與誤判率 (FPR) 有直接關係。

模型版本

模型版本是訓練模型的輸出。

模型部署

模型部署是啟用模型版本並使其可用於產生詐騙預測的程序。

Amazon SageMaker 模型端點

除了使用 Amazon Fraud Detector 建置模型之外，您還可以在 Amazon Fraud Detector 評估中選擇性地使用 SageMaker託管模型端點。

若要取得有關在中建置模型的更多資訊 SageMaker，請參閱〈使用訓練模型〉Amazon SageMaker。

偵測器

檢測器包含檢測邏輯，例如您要評估欺詐的特定事件的模型和規則。您可以使用模型版本建立偵測器。

偵測器版本

偵測器可以有多個版本，每個版本的狀態為`DraftActive`、或`Inactive`。一次只能有一個偵測器版本處於`Active`狀態。

變數

變數代表與您要在詐騙預測中使用的事件相關聯的資料元素。變數可以隨事件一起傳送，做為詐騙預測的一部分，也可以衍生變數，例如 Amazon Fraud Detector 模型的輸出或Amazon SageMaker.

規則

規則是告知 Amazon Fraud Detector 如何在詐騙預測期間解譯變數值的條件。規則由一或多個變數、邏輯運算式以及一或多個結果所組成。規則中使用的變數必須是偵測器評估之事件資料集的一部分。此外，每個檢測器必須至少有一個與其關聯的規則。

Outcome

這是來自欺詐預測的結果或輸出。在詐騙預測中使用的每個規則都必須指定一或多個結果。

詐騙預測

欺詐預測是對單個事件或一組事件的欺詐評估。Amazon Fraud Detector 會根據規則同步提供模型分數和結果，為單一線上事件即時產生詐騙預測。Amazon Fraud Detector 會針對一組離線事件產生詐騙預測。您可以使用這些預測來執行離線操作 proof-of-concept，或回溯評估每小時、每天或每週的欺詐風險。

詐騙預測說明

詐騙預測說明可讓您深入瞭解每個變數如何影響模型的詐騙預測分數。它提供了有關每個變量如何影響風險分數的信息，其中包括從 0 到 5，5 為最高）和方向（推高或更低）。

亞馬遜 Fraud Detector 的原理

Amazon Fraud Detector 會建立自訂的機器學習模型，以偵測您企業中潛在的詐騙線上活動。若要開始使用，您可以提供您的企業使用案例。根據您的商業使用案例，Amazon Fraud Detector 會建議用來為您建立詐騙偵測模型的模型類型。此外，它還提供了有關您需要提供的數據元素的見解，以作為業務歷史數據的一部分。Amazon Fraud Detector 使用歷史資料集為您自動建立和訓練自訂模型。

自動化模型訓練程序包括選擇機器學習演算法，以偵測特定商業使用案例的詐騙、驗證您提供的資料，以及執行資料操作以改善模型效能。訓練模型後，Amazon Fraud Detector 會產生模型分數和其他模型效能指標。您可以使用分數和效能指標來評估模型效能。如果需要，您可以從提供的資料集中新增或移除資料元素以進行訓練，並重新訓練模型以改善模型分數。

建立、訓練和啟動模型之後，您需要設定決策邏輯 (也稱為規則)，以告訴模型如何解譯您的業務所產生的資料，並指派結果，以便如何處理每個活動的解釋。結果可以代表諸如，批准或審查活動之類的操作，也可以代表活動的風險級別，例如高風險，中度風險和低風險。

檢測器是一個容納您的模型和相關規則的容器。您需要在生產環境中建立、測試及部署偵測器。

在生產環境中部署的偵測器可為您的業務應用程式提供詐騙偵測功能。為了執行欺詐評估，該模型將業務活動中的所有傳入數據與您的業務歷史數據進行比較，並使用其精密的機器學習算法與您創建的規則來分析結果並分配結果。使用 Amazon Fraud Detector，您可以即時評估單一商業活動中的資料，或離線評估來自多個商業活動的資料。

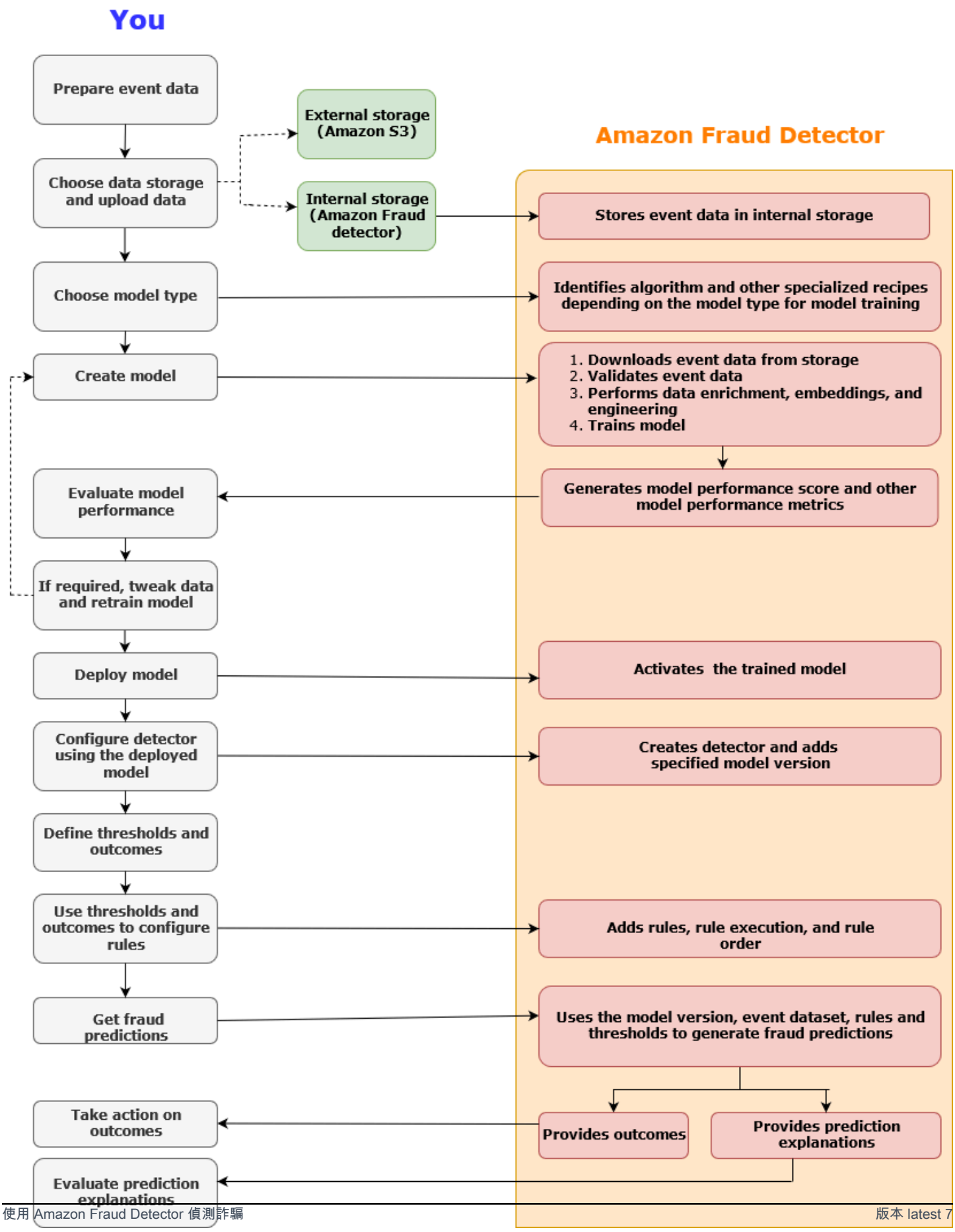
讓我們假設您的業務將在線資金轉移作為其活動之一。您想要使用 Amazon Fraud Detector 即時偵測詐騙資金轉移請求。若要開始使用，您必須先向 Amazon Fraud Detector 提供過去資金轉移請求的資料。Amazon Fraud Detector 使用此資料建立和訓練自訂模型，以偵測詐騙資金轉移請求。然後，您可以通過添加模型並配置模型的規則來解釋數據來創建檢測器。網上資金轉移活動的規則的一個例子可以是，如果資金轉移請求來自xyz@example.com電子郵件地址，發送審查請求。在您企業的生產環境中，當資金轉移請求出現時，模型會分析請求隨附的資料，並使用規則來指派結果。然後，您可以根據指派的結果對要求採取動作。

Amazon Fraud Detector 使用訓練資料集、模型、偵測器、規則和結果等元件，為您的企業提供詐騙評估邏輯。

如需使用 Amazon Fraud Detector 偵測詐騙的工作流程的相關資訊，請參閱使用 Amazon Fraud Detector 偵測詐騙

使用 Amazon Fraud Detector 偵測詐騙

本節說明使用 Amazon Fraud Detector 偵測詐騙的典型工作流程。它還總結了如何完成這些任務。下圖提供使用 Amazon Fraud Detector 偵測詐騙的工作流程的高階檢視。


You
Prepare event data
Choose data storage and upload data
External storage (Amazon S3)
Internal storage (Amazon Fraud detector)
Choose model type
Create model
Evaluate model performance
If required, tweak data and retrain model
Deploy model
Configure detector using the deployed model
Define thresholds and outcomes
Use thresholds and outcomes to configure rules
Get fraud predictions
Take action on outcomes
Evaluate prediction explanations
Amazon Fraud Detector
Stores event data in internal storage
Identifies algorithm and other specialized recipes depending on the model type for model training
1. Downloads event data from storage
2. Validates event data
3. Performs data enrichment, embeddings, and engineering
4. Trains model
Generates model performance score and other model performance metrics
Activates the trained model
Creates detector and adds specified model version
Adds rules, rule execution, and rule order
Uses the model version, event dataset, rules and thresholds to generate fraud predictions
Provides outcomes
Provides prediction explanations

欺詐檢測是一個持續的過程。部署模型之後，請務必根據預測說明評估其效能分數和指標。如此一來，您就可以識別最高風險指標、縮小導致誤報的根本原因，以及分析資料集中的詐騙模式，並偵測偏差(如果有的話)。為了提高預測的準確性，您可以調整數據集以包含新的或修訂的數據。然後，您可以使用更新的資料集重新訓練模型。隨著可用的資料越多，您可以繼續重新訓練模型以提高準確度。

訪問 Amazon Fraud Detector

Amazon Fraud Detector 有多種可用，AWS 區域並且可以使用AWS介面存取。

可用性

Amazon Fraud Detector 可在美國東部 (維吉尼亞北部)、美國東部 (俄亥俄)、美國西部 (奧勒岡)、歐洲 (愛爾蘭)、亞太區域 (新加坡) 和亞太區域 (雪梨) 使用AWS 區域。

介面

您可以使用下列任何介面建立、訓練、部署、測試、執行和管理詐騙偵測模型和偵測器：

AWS Management Console-Amazon Fraud Detector 提供基於 Web 的使用者界面，即 Amazon Fraud Detector 主控台。如果您已註冊AWS 帳戶，則可以存取 Amazon Fraud Detector 主控台。如需詳細資訊，請參閱設定 Amazon Fraud Detector。

AWS Command Line Interface(AWS CLI)-提供一個介面，您可以使用命令列殼層中的AWS 服務命令與包括 Amazon Fraud Detector 在內的廣泛集合互動。 AWS CLI適用於 Amazon Fraud Detector 的命令可實作與 Amazon Fraud Detector 主控台提供的功能相當。

AWSSDK-提供特定語言的 API 並管理許多連接詳細信息，例如簽名計算，請求重試處理和錯誤處理。有關更多信息，請轉到構建工具AWS頁面，向下滾動到 SDK 部分，然後選擇加號 (+) 以展開該部分。

AWS CloudFormation-提供可用於定義 Amazon Fraud Detector 資源和屬性的範本。如需詳細資訊，請參閱AWS CloudFormation使用者指南中的 Amazon Fraud Detector 資源類型參考。

定價

使用 Amazon Fraud Detector，您只需按使用量付費。沒有最低費用或者預付款項。我們會根據訓練和託管模型所使用的運算時數、使用的儲存空間量，以及您進行的詐騙預測數量向您收費。如需詳細資訊，請參閱 Amazon Fraud Detector 定價。

設置 Amazon Fraud Detector

若要使用 Amazon Fraud Detector，您首先需要一個 Amazon Web Services (AWS) 帳戶，然後必須設定許可以讓您 AWS 帳戶 存取所有界面。稍後，當您開始建立 Amazon Fraud Detector 資源時，您需要授與許可，以允許 Amazon Fraud Detector 存取您的帳戶，以代表您執行任務並存取您擁有的資源。

完成本節中的以下任務，以設定使用 Amazon Fraud Detector：

- 註冊 AWS.
- 設定允許您 AWS 帳戶 存取 Amazon Fraud Detector 界面的許可。
- 設定您要用來存取 Amazon Fraud Detector 的界面。

完成這些步驟後，請參閱開始使用 Amazon Fraud Detector繼續開始使用 Amazon Fraud Detector。

註冊成為 AWS

當您註冊 Amazon Web Services（AWS）時，您的所有服務 AWS 帳戶 都會自動註冊 AWS，包括 Amazon Fraud Detector。您只需針對所使用的服務付費。如果您已經擁有 AWS 帳戶，請跳至下一個工作。

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。
2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

設定存取 Amazon Fraud Detector 界面的權限

若要使用 Amazon Fraud Detector，請設定存取 Amazon Fraud Detector 主控台和 API 操作的許可。

遵循安全最佳實務，建立一個 AWS Identity and Access Management (IAM) 使用者，其存取權限僅限於 Amazon Fraud Detector 操作，並具有必要的許可。您可以視需要新增其他許可。

下列政策提供使用 Amazon Fraud Detector 所需的權限：

- `AmazonFraudDetectorFullAccessPolicy`

  您可使用此政策來執行下列動作：

  - 存取所有 Amazon Fraud Detector 資源
  - 列出並描述中的所有模型端點 SageMaker
  - 列出帳戶中的所有 IAM 角色
  - 列出所有 Amazon S3 存儲桶
  - 允許 IAM 通過角色將角色傳遞給 Amazon Fraud Detector
- `AmazonS3FullAccess`

  允許完整存取 Amazon Simple Storage Service。如果您需要將訓練資料集上傳到 Amazon S3，則必須執行此動作。

以下說明如何建立 IAM 使用者並指派所需的權限。

若要建立使用者並指派必要權限

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇 Users (使用者)，然後選擇 Add user (新增使用者)。
3. 在 User name (使用者名稱) 中輸入 **`AmazonFraudDetectorUser`**。
4. 選取 [AWS 管理主控台存取] 核取方塊，然後設定使用者密碼。

5. (選擇性) 根據預設， AWS 要求新使用者在第一次登入時建立新密碼。您可以清除 User must create a new password at next sign-in (使用者下次登入必須建立新的密碼) 旁的核取方塊，讓新使用者登入時可以重設密碼。
6. 選擇 Next: Permissions (下一步：許可)。
7. 選擇 Create group (建立群組)。
8. 對於群組名稱，輸入**`AmazonFraudDetectorGroup`**。
9. 在政策清單中，選取AmazonFraudDetectorFullAccessPolicy和 Amazon FullAccess S3 的核取方塊。選擇 Create group (建立群組)。
10. 在群組清單中，選取新群組的核取方塊。如果您在清單中看不到該群組，請選擇「重新整理」。
11. 選擇 Next: Tags (下一步：標籤)。
12. (選用) 藉由連接標籤做為索引鍵/值組，將中繼資料新增至使用者。如需如何在 IAM 中使用標籤的指示，請參閱標記 IAM 使用者和角色。
13. 選擇下一步：檢閱以查看新使用者的使用者詳細資料和權限摘要。當您準備好繼續時，請選擇 [建立使用者]。

設定介面以存取 Amazon Fraud Detector

您可以使用 Amazon Fraud Detector 主控台或 AWS SDK 存取 Amazon Fraud Detector。 AWS CLI在您可以使用它們之前，請先設置 AWS CLI 和 AWS SDK。

存取 Amazon Fraud Detector 主控台

您可以透過存取 Amazon Fraud Detector 主控台和其他 AWS 服務 AWS Management Console。您的 AWS 帳戶，授予您存取的 AWS Management Console.

若要存取 Amazon Fraud Detector 主控台，

1. 移至https://console.aws.amazon.com/並登入您的 AWS 帳戶.
2. 導航到 Amazon Fraud Detector。

使用 Amazon Fraud Detector 主控台，您可以建立和管理模型和詐騙偵測資源，例如偵測器、變數、事件、實體、標籤和結果。您可以產生預測並評估模型的效能和預測。

設定 AWS CLI

您可以在命令列殼層中執行命令，使用 AWS Command Line Interface (AWS CLI) 與 Amazon Fraud Detector 互動。透過最小組態，您可以使用 AWS CLI 來執行與 Amazon Fraud Detector 主控台提供的功能類似的命令，從終端機的命令提示字元執行命令。

若要設定 AWS CLI

下載和設定 AWS CLI。如需指示，請參閱《 AWS Command Line Interface 使用指南》中的下列主題：

- 使用 AWS 指令行介面進行設置
- 規劃指 AWS 令行介面

如需 Amazon Fraud Detector 命令的相關資訊，請參閱可用命令

設定 AWS 開發套件

您可以使用 AWS SDK 撰寫程式碼，以建立和管理詐騙偵測資源，以及取得詐騙預測。 AWS 開發套件支援 Amazon Fraud Detector JavaScript和 Python (Boto 3)。

若要設定 AWS SDK for Python (Boto3)

您可以用 AWS SDK for Python (Boto3) 來建立、設定和管理 AWS 服務。有關如何安裝博托的說明，請參閱AWS 開發套件 請確認您使用的是博多 3 SDK 版本 1.14.29 或更高版本。

安裝之後 AWS SDK for Python (Boto3)，請執行下列 Python 範例，以確認您的環境設定正確。如果設定正確，則回應會包含偵測器清單。如果未建立偵測器，則清單為空白。

```
import boto3
fraudDetector = boto3.client('frauddetector')

response = fraudDetector.get_detectors()
print(response)
```

若要為 Java 設定 AWS 開發套件

如需有關如何安裝和載入的指示 AWS SDK for JavaScript，請參閱設定 JavaScript.

開始使用 Amazon Fraud Detector

開始前，請確定您已閱讀使用 Amazon Fraud Detector 偵測詐騙並完成中的步驟設置 Amazon Fraud Detector。

使用本節中的實作教學課程，協助您如何使用 Amazon Fraud Detector 來建立、訓練和部署詐騙偵測模型。在本教學課程中，您將扮演詐騙分析師的角色，使用機器學習模型來預測新帳戶註冊是否為詐騙行為。模型必須使用來自帳戶註冊的資料進行訓練。Amazon Fraud Detector 為本教學提供帳戶註冊資料集範例。您必須先上傳範例資料集，才能開始使用教學課程。

您可以使用以下任一界面開始使用 Amazon Fraud Detector。開始使用本教學課程之前，請確定您遵循指示取得並上傳範例資料集

- 教學課程：開始使用 Amazon Fraud Detector 主控台
- 教學課程：開始使用AWS SDK for Python (Boto3)

取得並上傳範例資料集

您在本教學課程中使用的範例資料集提供線上帳戶註冊的詳細資訊。資料集位於使用 UTF-8 格式之逗號分隔值 (CSV) 的文字檔案中。CSV 資料集檔案的第一列包含標題。標題列後面接著多列資料。這些資料列都是由單一帳戶註冊的資料元素所組成。為方便起見，資料會標記為方便起見。資料集中的資料欄可識別帳戶註冊是否為詐騙行為。

若要取得並上傳範例資料集

1. 前往 [範例]。

   有兩個數據文件具有在線帳戶註冊數據-registration_data_20K_minimum.csv 和 registration_data_20K_full.csv。該文件只`registration_data_20K_minimum`包含兩個變量：IP 地址和電子郵件地址。該文件`registration_data_20K_full`包含其他變量。這些變量是針對每個事件，它們包括地址，電話號碼和用戶 _ 代理。這兩個數據文件還包含兩個必填字段：

   - 事件時間戳記 — 定義事件發生時的時間
   - 事件標籤 — 將事件分類為詐騙或合法

   您可以在本自學課程中使用兩個檔案的其中一個。下載您要使用的資料檔案。

2. 建立一個Amazon Simple Storage Service (Amazon S3) 儲存貯體。

   在此步驟中，您會建立外部儲存裝置來儲存資料集。此外部儲存貯體是 Amazon S3 儲存貯體。如需關於 Amazon S3 的詳細資訊，請參閱 Amazon S3？

   a. 登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/s3/ 的 Amazon S3 主控台。

   b. 在「值區」中選擇「建立值區」。

   c. 在 Bucket name (儲存貯體名稱) 中，輸入儲存貯體名稱。請務必遵循主控台中的值區命名規則，並提供全域唯一名稱。我們建議您使用描述值區用途的名稱。

   d. 在中 AWS 區域，選擇要在AWS 區域其中建立儲存貯體的位置。您選擇的區域必須支援 Amazon Fraud Detector。若要減少延遲，請選擇最AWS 區域接近您所在地理位置的延遲。如需支援 Amazon Fraud Detector 的區域清單，請參閱全球基礎設施指南中的區域表。

   e. 保留本教學課程的物件擁有權、區塊公開存取的值區設定、值區版本控制和標籤的預設設定。

   f. 對於預設加密，請在本教學課程中選擇停用。

   g. 檢閱值區組態，然後選擇 [建立值區]。

3. 將範例資料檔案上傳至 Amazon S3 儲存貯體。

   現在您已經擁有儲存貯體，請將先前下載的其中一個範例檔案上傳到剛建立的 Amazon S3 儲存貯體。

   a. 在「值區」中，會列出您的值區名稱。選擇您的儲存貯體。

   b. 選擇 Upload (上傳)。

   c. 在 [檔案和資料夾] 中選擇 [新增檔案]。

   d. 選擇您在電腦上下載的其中一個範例資料檔案，然後選擇 [開啟]。

   e. 保留 [目的地]、[權限] 和 [屬性] 的預設設定。

   f. 檢閱組態，然後選擇 [上傳]。

   g. 範例資料檔案會上傳至 Amazon S3 儲存貯體。請記下儲存貯體的位置。在 [物件] 中，選擇您剛上傳的範例資料檔案。

   h. 在物件概觀中，複製 S3 URI 下的位置。這是範例資料檔案的 Amazon S3 位置。供稍後使用。您可以另外複製 S3 儲存貯體的 Amazon Resource Name (SAN)，才能使用另外複製 S3 儲存貯體的 Amazon Resource Name (SAN

教學課程：開始使用 Amazon Fraud Detector 主控台

本自學課程由兩部分組成。第一部分說明如何建置、訓練和部署詐騙偵測模型。第二部分說明如何使用模型即時產生詐騙預測。模型是使用您上傳到 S3 儲存貯體的範例資料檔進行訓練。在本教學課程的結尾，您將完成下列動作：

- 建置和訓練 Amazon Fraud Detector 模型
- 產生即時詐騙預測

> **Important**
>
> 開始前，請確定您已按照指示取得並上傳範例資料集

A 部分：建置、訓練和部署 Amazon Fraud Detector 模型

在 A 部分中，您可以定義業務使用案例、定義事件、建立模型、訓練模型、評估模型的效能，以及部署模型。

步驟 1：選擇您的業務使用案例

- 在此步驟中，您可以使用資料模型總管將您的商業使用案例與 Amazon Fraud Detector 支援的詐騙偵測模型類型相符。資料模型總管是與 Amazon Fraud Detector 主控台整合的工具，可針對您的商業使用案例建立和訓練詐騙偵測模型，建議使用的模型類型。資料模型總管也會針對您需要包含在資料集中的強制性、建議和選用資料元素提供深入解析。該數據集將用於創建和訓練您的欺詐檢測模型。

  在本教學課程中，您的企業使用案例是新帳戶註冊。在您指定商業使用案例之後，資料模型總管會建議用於建立詐騙偵測模型的模型類型，並提供建立資料集所需的資料元素清單。由於您已經上傳包含新帳戶註冊資料的範例資料集，因此不需要建立新的資料集。

  a. 開啟AWS管理主控台並登入您的帳戶。導航到 Amazon Fraud Detector。
  b. 在左側導覽窗格中，選擇資料模型總管。
  c. 在 [資料模型總管] 頁面的 [商業使用案例] 下，選取 [新帳戶詐騙]。
  d. Amazon Fraud Detector 會顯示建議的模型類型，用於為選取的商業使用案例建立詐騙偵測模型。模型類型定義 Amazon Fraud Detector 將用來訓練您的詐騙偵測模型的演算法、擴充和轉換。

請記下建議的模型類型。稍後建立模型時，您將需要此功能。

e. [資料模型深入解析] 窗格提供建立和訓練詐騙偵測模型所需的強制性和建議資料元素的深入解析。

請查看您下載的範例資料集，並確定資料表中列出了所有必要資料元素和一些建議的資料元素。

稍後當您為特定商務使用案例建立模型時，您將使用提供的深入解析來建立資料集。

步驟 2：建立事件類型

- 在此步驟中，您會定義要評估詐騙的商業活動 (事件)。定義事件包括設定資料集中的變數、起始事件的實體，以及將事件分類的標籤。在本教學課程中，您會定義帳戶註冊事件。

a. 開啟AWS管理主控台並登入您的帳戶。導航到 Amazon Fraud Detector。

b. 在左側導覽窗格中，選擇事件。

c. 在 [事件類型] 頁面中，選擇 [建立]。

d. 在事件類型詳細資訊下`sample_registration`，輸入事件類型名稱，並選擇性地輸入事件的描述。

e. 針對「實體」，選擇建立實體。

f. 在 [建立實體] 頁面中`sample_customer`，輸入實體類型名稱。您可以選擇輸入實體類型的描述。

g. 選擇 Create entity (建立實體)。

h. 在事件變數下，對於選擇如何定義此事件的變數，選擇從訓練資料集選取變數。

i. 對於 IAM 角色，請選擇建立 IAM 角色。

j. 在 [建立 IAM 角色] 頁面中，輸入您上傳範例資料的 S3 儲存貯體名稱，然後選擇 [建立角色]。

k. 在資料位置中，輸入範例資料的路徑。這是您上傳範例資料後所儲存的`S3 URI`路徑。路徑類似於：`S3://your-bucket-name/example dataset filename.csv`。

l. 選擇 Upload (上傳)。

Amazon Fraud Detector 會從範例資料檔案中擷取標頭，並使用變數類型對應它們。對映會顯示於主控台中。

m. 在 [標示-可選] 下，對於 [標示]，選擇 [建立新標示]。

n. 在「建立標籤」頁面中fraud，輸入名稱。此標籤對應於範例資料集中代表詐騙帳戶註冊的值。

o. 選擇「建立標籤」。

p. 建立第二個標籤，然後輸入legit作為名稱。此標籤對應於範例資料集中代表合法帳戶註冊的值。

q. 選擇 [建立事件類型]。

步驟 3：建立模型

1. 在「模型」頁面上，選擇「新增模型」，然後選擇「建立模型」。
2. 對於步驟 1-定義模型詳細資訊sample_fraud_detection_model，請輸入模型名稱。您可以選擇新增模型的描述。
3. 針對「模型類型」，選擇「線上詐騙洞察」模型。
4. 對於事件類型，請選擇範例註冊。這是您在步驟 1 中建立的事件類型。
5. 在歷史事件數據中，

   a. 在事件資料來源中，選擇存放在 S3 中的事件資料。

   b. 針對 IAM 角色，選取您在步驟 1 中建立的角色。

   c. 在訓練資料位置中，輸入範例資料檔案的 S3 URI 路徑。
6. 選擇 下一步。

步驟 4：訓練模型

1. 在模型輸入中，保留勾選所有核取方塊。根據預設，Amazon Fraud Detector 會使用歷史事件資料集中的所有變數做為模型輸入。
2. 在「標籤」分類中，針對詐騙標籤選擇詐騙，因為此標籤對應於範例資料集中代表詐騙事件的值。對於合法標籤，請選擇合法，因為此標籤對應於範例資料集中代表合法事件的值。
3. 對於「未標籤的事件」處理方式，請保留預設選取「忽略此範例資料集的未標籤事件」。
4. 選擇 下一步。
5. 檢閱後，選擇 [建立並訓練模型]。Amazon Fraud Detector 會建立模型，並開始訓練新版本的模型。

   在模型版本中，狀態欄指示模型訓練的狀態。使用範例資料集的模型訓練大約需要 45 分鐘才能完成。模型訓練完成後，狀態會變更為 [準備部署]。

步驟 5：檢閱模型效能

使用 Amazon Fraud Detector 的重要步驟是使用模型分數和效能指標來評估模型的準確性。模型訓練完成後，Amazon Fraud Detector 會使用 15% 的資料來驗證模型效能，這些資料未用於訓練模型並產生模型效能分數和其他效能指標。

1. 若要檢視模型的效能，

   a. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇模型。

   b. 在「模型」頁面中，選擇您剛訓練的模型（模型），然後選擇 1.0。這是亞馬遜 Fraud Detector 為您的模型創建的版本。

2. 查看模型效能整體分數以及 Amazon Fraud Detector 為此模型產生的所有其他指標。

   若要深入瞭解此頁面上的模型效能分數和效能測量結果，請參閱模型分數和模型效能指標。

   您可以預期所有訓練有素的 Amazon Fraud Detector 模型都具有與您在本教學中看到的模型效能指標類似的真實世界詐騙偵測效能指標。

步驟 6：部署模型

在您檢閱訓練模型的效能指標，並準備好使用它產生詐騙預測之後，您就可以部署模型。

1. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇「型號」。
2. 在 [模型] 頁面中，選擇 [偵測模型]，然後選擇您要部署的特定模型版本。對於此自學課程，請選擇 1.0。
3. 在 [模型版本] 頁面上，選擇 [動作]，然後選擇 [部署模型版本]。
4. 在「模型」版本中，「狀態」 會顯示部署的狀態。部署完成後，狀態會變更為「作用中」。這表示模型版本已啟動並可用於產生詐騙預測。繼續完B 部分：產生詐騙預測成產生詐騙預測的步驟。

B 部分：產生詐騙預測

欺詐預測是對商業活動（事件）欺詐的評估。Amazon Fraud Detector 使用偵測器產生詐騙預測。偵測器包含您要評估詐騙之特定事件的偵測邏輯，例如模型和規則。偵測邏輯會使用規則告知 Amazon Fraud Detector 如何解譯與模型相關聯的資料。在本教學課程中，您會使用先前上傳的帳戶註冊範例資料集來評估帳戶註冊事件。

在零件 A 中，您已建立、訓練及部署模型。在 B 部分中，您可以為sample_registration事件類型建立偵測器、新增已部署的模型、建立規則和規則執行順序，然後建立並啟動用來產生詐騙預測的偵測器版本。

步驟 1：建立偵測

若要建立偵測器

1. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇 De tector。
2. 選擇創建檢測器。
3. 在 [定義偵測器詳細資訊] 頁面中，輸入sample_detector偵測器名稱。您可以選擇輸入偵測器的描述，例如my sample fraud detector。
4. 對於事件類型，選取範例註冊。這是您在本自學課程的第 A 部分中建立的事件。
5. 選擇 下一步。

步驟 2：新增模型

如果您完成本教學課程的 A 部分，那麼您可能已經擁有可新增至偵測器的 Amazon Fraud Detector 模型。如果您尚未建立模型，請移至「A 部分」並完成建立、訓練和部署模型的步驟，然後繼續執行 B 部分。

1. 在 [新增模型-選用] 中，選擇 [新增模型]。
2. 在「新增模型」頁面中，針對 「選取模型」，選擇您先前部署的 Amazon Fraud Detector 型號名稱。對於 「選取版本」，請選擇已部署模型的模型版本。
3. 選擇 Add model (新增模型)。
4. 選擇 下一步。

步驟 3：新增規則

規則是指示 Amazon Fraud Detector 如何在評估詐騙預測時解譯模型效能分數的條件。在本自學課程中，您將建立三個規則：high_fraud_riskmedium_fraud_risk、和low_fraud_risk。

1. 在 [新增規則] 頁面的 [定義規則] 下，輸入high_fraud_risk規則名稱，並在 [說明-選用性] 下輸入**This rule captures events with a high ML model score**規則的說明。
2. 在運算式中，使用 Amazon Fraud Detector 簡化的規則運算式語言輸入下列規則運算式：

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```

3. 在 [成果] 中，選擇 [建立新的結果]。結果是詐騙預測的結果，如果規則在評估期間符合，則會傳回結果。
4. 在建立新結果中，輸入verify_customer作為結果名稱。您可以選擇輸入描述。
5. 選擇 [儲存結果]。
6. 選擇新增規則以執行規則驗證檢查程式並儲存規則。建立後，Amazon Fraud Detector 會讓規則可用於您的偵測器。
7. 選擇 [新增其他規則]，然後選擇 [建立規則] 索引標籤。
8. 再重複此程序兩次，以使用下列low_fraud_risk規則詳細資訊建立您的medium_fraud_risk和規則：

   - 中等詐騙風險

     規則名稱：medium_fraud_risk

     成果：review

     表達式：

     ```
     $sample_fraud_detection_model_insightscore <= 900 and
     ```

     ```
     $sample_fraud_detection_model_insightscore > 700
     ```

   - 低欺詐風險

     規則名稱：low_fraud_risk

     成果：approve

     表達式：

     ```
     $sample_fraud_detection_model_insightscore <= 700
     ```

   這些值是用於此教學課程的範例。當您為自己的偵測器建立規則時，請使用適合您的模型和使用案例的值，

9. 建立全部三個規則之後，請選擇 [下一步]。

   如需建立和寫入規則的詳細資訊，請參閱規則和規則語言參考。

步驟 4：設定規則執行和規則順序

偵測器中包含之規則的規則執行模式會決定是否評估您定義的所有規則，或規則評估是否在第一個符合的規則停止。規則順序決定了您希望規則執行的順序。

預設規則執行模式為FIRST_MATCHED。

第一個匹配

第一個符合的規則執行模式會根據定義的規則順序傳回第一個相符規則的結果。若您指定FIRST_MATCHED，Amazon Fraud Detector 會從頭到尾依序評估規則，並在遇到第一個相符規則後停止評估。然後，Amazon Fraud Detector 會提供該單一規則的結果。

您執行規則的順序可能會影響產生的詐騙預測結果。建立規則之後，請依照下列步驟重新排序規則，以所需的順序執行規則：

如果您的high_fraud_risk規則尚未在規則清單頂端，請選擇 [順序]，然後選擇 [1]。這將移動high_fraud_risk到第一個位置。

重複此程序，以便您的medium_fraud_risk規則位於第二個位置，而您的low_fraud_risk規則位於第三個位置。

全部符合

無論規則順序為何，所有符合的規則執行模式都會傳回所有符合規則的結果。若您指定ALL_MATCHED，Amazon Fraud Detector 會評估所有規則，並傳回所有相符規則的結果。

選取FIRST_MATCHED此教學課程，然後選擇 [下一步]。

步驟 5：檢閱並建立偵測貯體版本

檢測器版本定義了用於生成欺詐預測的特定模型和規則。

1. 在「檢閱並建立」頁面中，檢閱您設定的偵測器詳細資訊、模型和規則。如果您需要進行任何變更，請選擇相應區段旁邊的 [編輯]。
2. 選擇創建檢測器。建立偵測器之後，偵測器的第一個版本會顯示在「偵測器版本」表格中，並顯示Draft狀態。

   您可以使用草稿版本來測試您的偵測器。

步驟 6：測試並啟用偵測器版本

在 Amazon Fraud Detector 主控台中，您可以使用具有執行測試功能的模擬資料來測試偵測器的邏輯。在本教學課程中，您可以使用範例資料集中的帳戶註冊資料。

1. 捲動至 [偵測器版本詳細資訊] 頁面底部的 [執行測試]。
2. 在事件中繼資料中，輸入事件發生時間的時間戳記，並為執行事件的實體輸入唯一識別碼。在本教學課程中，從日期選擇器中選取時間戳記的日期，然後輸入「1234」做為實體 ID。
3. 在事件變數中，輸入您要測試的變數值。在本教學課程中，您只需要`ip_address`和`email_address`欄位。這是因為它們是用於訓練 Amazon Fraud Detector 模型的輸入。您可使用以下範例值。這假設您使用了建議的變量名稱：

   - 位址 (_1)：`205.251.233.178`
   - 電子郵件地址：`johndoe@exampledomain.com`
4. 選擇運行測試。
5. Amazon Fraud Detector 會根據規則執行模式傳回詐騙預測結果。如果規則執行模式為`FIRST_MATCHED`，則傳回的結果會對應至符合的第一個規則。第一個規則是具有最高優先順序的規則。如果它被評估為 true，它是匹配的。如果規則執行模式為`ALL_MATCHED`，則傳回的結果會對應至符合的所有規則。這意味著它們都被評估為真實。Amazon Fraud Detector 也會傳回新增至偵測器之任何模型的模型分數。

   您可以更改輸入並運行幾個測試以查看不同的結果。您可以使用範例資料集中的 ip_address 和 email_ address 值進行測試，並檢查結果是否符合預期。
6. 當您對探測器的工作方式感到滿意時，請將其從推廣`Draft`到`Active`。這樣做使得檢測器可用於實時欺詐檢測。

   在偵測器版本詳細資料頁面上，選擇 [動作]、[發佈]、[發佈版本 這會將偵測器的狀態從「草稿」變更為「作用中」。

   此時，您的模型和相關的偵測器邏輯已準備好使用 Amazon Fraud Detector`GetEventPrediction` API 即時評估線上活動是否有詐騙。您也可以使用 CSV 輸入檔案和`CreateBatchPredictionJob` API 離線評估事件。如需有關詐騙預測的詳細資訊，請參閱詐騙預測

完成本教學課程後，您將執行下列作業：

- 將範例事件資料集上傳至 Amazon S3。

- 使用範例資料集建立並訓練 Amazon Fraud Detector 詐騙偵測模型。
- 檢視 Amazon Fraud Detector 產生的模型效能分數和其他效能指標。
- 部署了欺詐檢測模型。
- 創建了一個檢測器並添加了部署的模型。
- 在偵測器中新增規則、規則執行順序和結果。
- 通過提供不同的輸入並檢查規則和規則執行順序是否按預期工作來測試檢測器。
- 通過發布它激活檢測器。

教學課程：開始使用AWS SDK for Python (Boto3)

本教學說明如何建置和訓練 Amazon Fraud Detector 模型，然後使用此模型產生即時詐騙預測AWS SDK for Python (Boto3)。模型是使用您上傳到 Amazon S3 儲存貯體的帳戶註冊範例資料檔進行訓練。

在本教學的結尾，您將完成下列動作：

- 建置和訓練 Amazon Fraud Detector 模型
- 產生即時 Fraud Dete

先決條件

以下是本教學課程的先決條件步驟。

- 已完成設置 Amazon Fraud Detector。

  如果您已經使用了設定 AWS 開發套件，請確保您使用的是 Boto3 SDK 版本 1.14.29 或更高版本。
- 按照說明到本教程所需的取得並上傳範例資料集文件。

開始使用

步驟 1：設定及驗證您的 Python 環境

博托是 Amazon Web Services（AWS）軟件開發套件 Python。您可以使用它來建立、設定和管理 AWS 服務。如需如何安裝 Boto3 的相關指示，請參閱適用於 Python 的 AWS 開發套件。

安裝之後AWS SDK for Python (Boto3)，請執行下列 Python 範例命令，以確認您的環境設定正確。如果您的環境設定正確，則回應會包含偵測器清單。如果未建立偵測器，清單會是空的。

```
import boto3
fraudDetector = boto3.client('frauddetector')

response = fraudDetector.get_detectors()
print(response)
```

步驟 2：建立變數、實體類型和標籤

在此步驟中，您會建立用於定義模型、事件和規則的資源。

建立變數

變數是您要用來建立事件類型、模型和規則的資料集中的資料元素。

在下面的例子中，CreateVariableAPI 用於創建兩個變量。變量是email_address和ip_address。將它們分配給相應的變量類型：EMAIL_ADDRESS和IP_ADDRESS。這些變數是您上傳範例資料集的一部分。當您指定變數類型時，Amazon Fraud Detector 會在模型訓練期間和取得預測時解譯變數。只有具有關聯變數類型的變數才能用於模型訓練。

```
import boto3
fraudDetector = boto3.client('frauddetector')

 #Create variable email_address
fraudDetector.create_variable(
    name = 'email_address',
    variableType = 'EMAIL_ADDRESS',
    dataSource = 'EVENT',
    dataType = 'STRING',
    defaultValue = '<unknown>'
)

#Create variable ip_address
fraudDetector.create_variable(
    name = 'ip_address',
    variableType = 'IP_ADDRESS',
    dataSource = 'EVENT',
    dataType = 'STRING',
    defaultValue = '<unknown>'
)
```

建立實體類型

實體代表誰正在執行事件，實體類型會將實體分類。分類範例包括客戶、商家或帳戶。

在下面的例子中，PutEntityTypeAPI 用於創建一個`sample_customer`實體類型。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_entity_type(
   name = 'sample_customer',
   description = 'sample customer entity type'
)
```

建立標籤

標籤會將事件分類為詐騙或合法，並用來訓練 Fraud Detector。該模型學習使用這些標籤值對事件進行分類。

在下面的例子中，Putlabel API 用於創建兩個標籤，`fraud`和`legit`。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_label(
    name = 'fraud',
    description = 'label for fraud events'
)

fraudDetector.put_label(
    name = 'legit',
    description = 'label for legitimate events'
)
```

步驟 3：建立事件類型

使用 Amazon Fraud Detector，您可以建立可評估風險並為個別事件產生 Fraud Detector 的模型 事件類型會定義個別事件的結構。

在下列範例中，PutEventTypeAPI 是用來建立事件類型sample_registration。您可以透過指定在上一個步驟中建立的變數 (email_address,ip_addresssample_customer)、實體類型 (legit) 和標籤 (fraud,) 來定義事件類型。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_event_type (
     name = 'sample_registration',
     eventVariables = ['ip_address', 'email_address'],
     labels = ['legit', 'fraud'],
     entityTypes = ['sample_customer'])
```

步驟 4：建立、訓練和部署模型

Amazon Fraud Detector 會訓練模型以學習偵測特定事件類型的詐騙行為。在上一個步驟中，您建立了事件類型。在此步驟中，將會建立及訓練事件類型的模型。該模型充當模型版本的容器。每次訓練模型時，就會建立新的版本。

使用下列範例程式碼來建立和訓練線上詐騙洞察模型。這個模型被稱為sample_fraud_detection_model。它適用於sample_registration使用您上傳到 Amazon S3 的帳戶註冊範例資料集的事件類型。

如需 Amazon Fraud Detector 支援之不同模型類型的詳細資訊，請參閱選擇型號類型。

建立模型

在下面的例子中，CreateModelAPI 用於創建模型。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_model (
       modelId = 'sample_fraud_detection_model',
       eventTypeName = 'sample_registration',
       modelType = 'ONLINE_FRAUD_INSIGHTS')
```

訓練模型

在下列範例中，CreateModelVersionAPI 用於訓練模型。指定'EXTERNAL_EVENTS'您存放範例資料集RoleArn的trainingDataSource和 Amazon S3 位置，以及其 Amazon S3 儲存貯體的位置externalEventsDetail。對於trainingDataSchema參數，請指定 Amazon Fraud Detector 如何解譯範例資料。更具體地說，指定要包含哪些變數，以及如何分類事件標籤。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_model_version (
         modelId = 'sample_fraud_detection_model',
         modelType = 'ONLINE_FRAUD_INSIGHTS',
         trainingDataSource = 'EXTERNAL_EVENTS',
         trainingDataSchema = {
            'modelVariables' : ['ip_address', 'email_address'],
            'labelSchema' : {
               'labelMapper' : {
                   'FRAUD' : ['fraud'],
                   'LEGIT' : ['legit']
        }
    }
},
         externalEventsDetail = {
              'dataLocation' : 's3://your-S3-bucket-name/your-example-data-
filename.csv',
              'dataAccessRoleArn' : 'role_arn'
}
)
```

您可以多次訓練模型。每次訓練模型時，就會建立新的版本。模型訓練完成後，模型版本狀態會更新為TRAINING_COMPLETE。您可以檢閱模型效能分數和其他模型效能測量結果。

檢閱模型效能

使用 Amazon Fraud Detector 的重要步驟是使用模型分數和效能指標來評估模型的準確性。模型訓練完成後，Amazon Fraud Detector 會使用未用於訓練模型的 15% 資料來驗證模型效能。它會產生模型效能分數和其他效能指標。

使用 DescribeModelVersionsAPI 來檢閱模型效能。查看模型效能整體分數以及 Amazon Fraud Detector 針對此模型產生的所有其他指標。

若要深入瞭解模型效能分數和效能指標，請參閱模型分數和模型效能指標。

您可以預期所有訓練有素的 Amazon Fraud Detector 模型都具有真實世界的詐騙偵測效能指標，這些指標與本教學中的指標類似。

部署模型

檢閱訓練模型的效能指標後，請部署模型並將其提供給 Amazon Fraud Detector 以產生詐騙預測。若要部署訓練過的模型，請使用 UpdateModelVersionStatusAPI。在下面的例子中，它用於將模型版本狀態更新為 ACTIVE。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.update_model_version_status (
     modelId = 'sample_fraud_detection_model',
     modelType = 'ONLINE_FRAUD_INSIGHTS',
     modelVersionNumber = '1.00',
     status = 'ACTIVE'
)
```

步驟 5：建立偵測器、結果、規則和偵測器版本

檢測器包含檢測邏輯，例如模型和規則。此邏輯適用於您要評估詐騙的特定事件。規則是您指定的條件，以告訴 Amazon Fraud Detector 如何在預測期間解譯變數值。結果是欺詐預測的結果。檢測器可以有多個版本，每個版本的狀態為草稿，活動或非活動狀態。偵測器版本必須至少有一個規則與之建立關聯。

使用下列範例程式碼建立偵測器、規則、結果，以及發佈偵測器。

建立偵測器

在下面的例子中，PutDetectorAPI 用於創建`sample_registration`事件類型的`sample_detector`檢測器。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_detector (
     detectorId = 'sample_detector',
     eventTypeName = 'sample_registration'
)
```

創造成果

為每個可能的欺詐預測結果創建結果。在下列範例中，PutOutcomeAPI 用於建立三個結果-verify_customerreview、和approve。這些結果稍後會指派給規則。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_outcome(
     name = 'verify_customer',
     description = 'this outcome initiates a verification workflow'
    )

fraudDetector.put_outcome(
     name = 'review',
     description = 'this outcome sidelines event for review'
    )

fraudDetector.put_outcome(
     name = 'approve',
     description = 'this outcome approves the event'
)
```

建立規則

規則由資料集中的一或多個變數、邏輯運算式以及一或多個結果所組成。

在下列範例中，CreateRuleAPI 用於建立三個不同的規則：high_riskmedium_risk、和low_risk。建立規則運算式，將模型效能分數sample_fraud_detection_model_insightscore值與各種臨界值進行比較。這是為了確定事件的風險級別，並指派在上一個步驟中定義的結果。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_rule(
     ruleId = 'high_fraud_risk',
     detectorId = 'sample_detector',
```

```
     expression = '$sample_fraud_detection_model_insightscore > 900',
     language = 'DETECTORPL',
     outcomes = ['verify_customer']
     )

fraudDetector.create_rule(
     ruleId = 'medium_fraud_risk',
     detectorId = 'sample_detector',
     expression = '$sample_fraud_detection_model_insightscore <= 900 and
 $sample_fraud_detection_model_insightscore > 700',
     language = 'DETECTORPL',
     outcomes = ['review']
     )

fraudDetector.create_rule(
     ruleId = 'low_fraud_risk',
     detectorId = 'sample_detector',
     expression = '$sample_fraud_detection_model_insightscore <= 700',
     language = 'DETECTORPL',
     outcomes = ['approve']
     )
```

建立偵測器版本

偵測器版本會定義用來取得詐騙預測的模型和規則。

在下面的例子中，CreateDetectorVersionAPI 用於創建一個檢測器版本。它通過提供模型版本詳細信息，規則和規則執行模式 FIRST_MATCHED 來完成此操作。規則執行模式指定評估規則的順序。規則執行模式 FIRST_MATCHED 會從頭到尾依序評估規則，並在遇到第一個相符規則後停止評估。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_detector_version(
      detectorId = 'sample_detector',
      rules = [{
          'detectorId' : 'sample_detector',
          'ruleId' : 'high_fraud_risk',
          'ruleVersion' : '1'
},
{
```

```
          'detectorId' : 'sample_detector',
          'ruleId' : 'medium_fraud_risk',
          'ruleVersion' : '1'
},
{
          'detectorId' : 'sample_detector',
          'ruleId' : 'low_fraud_risk',
          'ruleVersion' : '1'
}
],
      modelVersions = [{
          'modelId' : 'sample_fraud_detection_model',
          'modelType': 'ONLINE_FRAUD_INSIGHTS',
          'modelVersionNumber' : '1.00'
}      ],
      ruleExecutionMode = 'FIRST_MATCHED'
)
```

步驟 6：產生 Fraud Detector

本教學課程的最後一個步驟使用在上一個步驟中sample_detector建立的偵測器，即時產生sample_registration事件類型的詐騙預測。偵測器會評估上傳至 Amazon S3 的範例資料。回應包括模型績效分數，以及與相符規則相關聯的任何結果。

在下列範例中，GetEventPredictionAPI 用於在每個請求中提供單一帳戶註冊的資料。在本教程中，請從帳戶註冊示例數據文件中獲取數據（電子郵件地址和 ip_address）。頂端標題行之後的每一行 (列) 代表來自單一帳戶註冊事件的資料。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.get_event_prediction(
      detectorId = 'sample_detector',
      eventId = '802454d3-f7d8-482d-97e8-c4b6db9a0428',
      eventTypeName = 'sample_registration',
      eventTimestamp = '2020-07-13T23:18:21Z',
      entities = [{'entityType':'sample_customer', 'entityId':'12345'}],
 eventVariables = {
      'email_address': 'johndoe@exampledomain.com',
      'ip_address': '1.2.3.4'
}
```

```
)
```

完成本教學後，您將執行下列作業：

- 將事件資料集範例上傳到 Amazon S3。
- 建立用於建立和訓練模型的變數、實體和標籤。
- 使用範例資料集建立並訓練模型。
- 檢視 Amazon Fraud Detector 產生的模型效能分數和其他效能指標。
- 部署了欺詐檢測模型。
- 創建了一個檢測器並添加了部署的模型。
- 在偵測器中新增規則、規則執行順序和結果。
- 已建立偵測器版本。
- 通過提供不同的輸入並檢查規則和規則執行順序是否按預期工作來測試檢測器。

（可選）使用木普特（IPython）筆記本探索亞馬遜 Fraud Detector API

如需有關如何使用 Amazon Fraud Detector API 的更多範例，請參閱aws-fraud-detector-samples GitHub 儲存庫。筆記型電腦涵蓋的主題包括使用 Amazon Fraud Detector API 的建置模型和偵測器，以及使用`GetEventPrediction` API 提出批次詐騙預測請求。

後續步驟

現在，您已經建立了模型和偵測器，您可以進行更深入的研究，並開始建立模型和偵測器，並產生詐騙預測。

Amazon Fraud Detector 使用者指南中的以下各節說明您的企業或組織如何使用 Amazon Fraud Detector 偵測詐騙。

- 準備並建立事件資料集以訓練模型。
- 建立事件類型
- 建立模型
- 建立偵測器
- 取得詐騙預測
- 管理您的 Amazon Fraud Detector 資源 (特別是變數、實體、結果和標籤)

- 設定 Amazon Fraud Detector 以符合您的安全性和合規目標
- 監控亞馬遜 Fraud Detector 並記錄 Amazon Fraud Detector API 呼叫
- 使用 Amazon Fraud Detector 的問題

事件資料集

事件資料集是貴公司的歷史詐騙資料。您將此資料提供給 Amazon Fraud Detector，以建立詐騙偵測模型。

Amazon Fraud Detector 使用機器學習模型來產生詐騙預測。每個模型都使用模型類型進行訓練。模型類型指定用於訓練模型的演算法和轉換。模型訓練是使用您提供的資料集來建立可預測詐騙事件的模型的程序。如需詳細資訊，請參閱 Amazon FraFraud Detector 的運作方式

用於創建欺詐檢測模型的數據集提供了事件的詳細信息。事件是評估詐騙風險的商業活動。例如，帳戶註冊可以是一個事件。與帳戶註冊事件相關聯的資料可以是事件資料集。Amazon Fraud Detector 會使用此資料集來評估帳戶註冊詐騙。

在將資料集提供給 Amazon Fraud Detector 以建立模型之前，請務必定義建立模型的目標。您還需要確定如何使用模型，並定義指標，以根據您的特定需求評估模型是否正在執行。

例如，您建立評估帳戶註冊詐騙的詐騙偵測模型的目標如下：

- 自動核准合法註冊。
- 捕獲欺詐性註冊以供日後調查。

確定目標後，下一步就是決定要如何使用模型。以下是使用欺詐檢測模型評估註冊欺詐的一些示例：

- 用於每個帳戶註冊的實時欺詐檢測。
- 每小時離線評估所有帳戶註冊。

以下是一些可用來測量模型效能的量度範例：

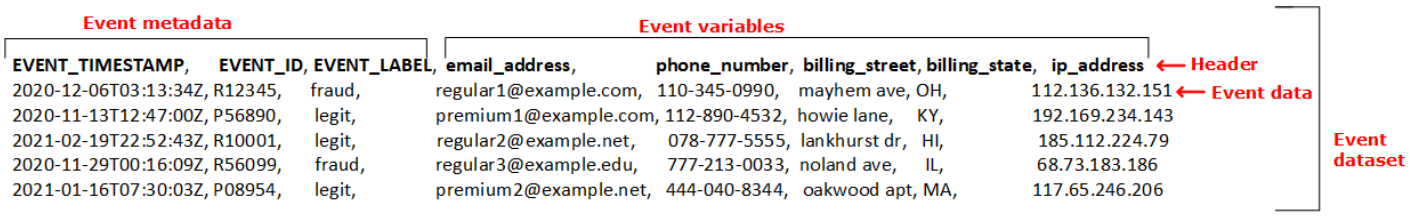
- 在生產環境中的執行效能一致優於目前的基準。
- 以 Y% 誤判率擷取 X% 詐騙註冊。
- 接受多達 5% 的自動核准註冊是詐騙的。

事件資料集結構

Amazon Fraud Detector 要求您使用 UTF-8 格式的逗號分隔值 (CSV) 以文字檔案提供事件資料集。CSV 資料集檔案的第一行必須包含檔案標頭。文件頭由事件元數據和事件變量組成，這些變量描述了與事件相關聯的每個數據元素。標頭後跟事件資料。每一行都包含來自單一事件的資料元素。

- 事件中繼資料-提供有關事件的資訊。例如，EVENT_TIMESTAMP 是一個事件中繼資料，用於指定事件發生的時間。根據您的業務使用案例和用於建立和訓練詐騙偵測模型的模型類型，Amazon Fraud Detector 會要求您提供特定的事件中繼資料。在 CSV 檔案標頭中指定事件中繼資料時，請使用 Amazon Fraud Detector 指定的相同事件中繼資料名稱，並僅使用大寫字母。
- 事件變數-代表您要用來建立和訓練詐騙偵測模型的事件特定資料元素。根據您的業務使用案例以及用於建立和訓練詐騙偵測模型的模型類型，Amazon Fraud Detector 可能會要求或建議您提供特定的事件變數。您也可以選擇性地提供事件中要包含在訓練模型中的其他事件變數。線上註冊事件的一些事件變數範例可以是電子郵件地址、IP 位址和電話號碼。在 CSV 檔案標頭中指定事件變數名稱時，請使用您選擇的任何變數名稱，並僅使用小寫字母。
- 事件數據-表示從實際事件收集的數據。在 CSV 檔案中，檔案標頭後面的每一列都包含單一事件中的資料元素。例如，在線上註冊事件資料檔案中，每一列都包含來自單一註冊的資料。列中的每個資料元素都必須符合對應的事件中繼資料或事件變數。

下列範例是 CSV 檔案範例，其中包含來自帳戶註冊事件的資料。標頭列包含大寫的事件中繼資料，以及小寫後跟事件資料的事件變數。資料集中的每一列都包含與單一帳戶註冊相關聯的資料元素，以及與標頭對應的每個資料元素。



使用資料模型總管取得事件資料集需求

您選擇建立模型的模型類型會定義資料集的需求。Amazon Fraud Detector 會使用您提供的資料集來建立和訓練詐騙偵測模型。Amazon Fraud Detector 開始建立模型之前，它會檢查資料集是否符合大小、格式和其他需求。如果資料集不符合需求，則模型建立和訓練會失敗。您可以使用資料模型總管來識別要用於商業使用案例的模型類型，並深入瞭解已識別之模型類型的資料集需求。

資料模型總管

資料模型總管是 Amazon Fraud Detector 主控台中的工具，可將您的商業使用案例與 Amazon Fraud Detector 支援的模型類型保持一致。資料模型總管也提供 Amazon Fraud Detector 建立詐騙偵測模型所需資料元素的深入解析。在開始準備事件資料集之前，請使用資料模型總管找出 Amazon Fraud Detector 為您的業務用途建議的模型類型，並查看建立資料集所需的強制性、建議和選用資料元素清單。

要使用數據模型資源管理器，

1. 開啟AWS管理主控台並登入您的帳戶。導航 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇資料模型總管。
3. 在 [資料模型總管] 頁面的 [商業使用案例] 下，選取您要評估詐騙風險的商業使用案例。
4. Amazon Fraud Detector 會顯示與您的商業使用案例相符的建議模型類型。模型類型定義 Amazon Fraud Detector 將用來訓練您的詐騙偵測模型的演算法、擴充和轉換。

   請記下建議的模型類型。稍後建立模型時，您將需要此功能。

   > **Note**
   >
   > 如果您找不到您的業務使用案例，請使用說明中的「聯繫我們」鏈接向我們提供您的業務用例的詳細信息。我們會針對您的企業使用案例建立詐騙偵測模型時，建議使用的模型類型。

5. 「資料模型深入解析」窗格可提供針對企業使用案例建立和訓練詐騙偵測模型所需的強制性、建議和選用資料元素的深入解析。使用深入解析窗格中的資訊來收集事件資料並建立資料集。

收集事件資料

收集事件資料是建立模型的重要步驟。這是因為模型在預測詐騙時的效能取決於資料集的品質。當您開始收集事件資料時，請記住資料模型總管為您建立資料集所提供的資料元素清單。您需要收集所有強制性 (事件中繼資料) 資料，並根據建立模型的目標決定要包含哪些建議和選用的資料元素 (事件變數)。決定要包含的每個事件變數的格式以及資料集的總大小也很重要。

事件資料集品質

若要為您的模型收集高品質資料集，我們建議下列作法：

- 收集成熟的數據- 使用最新的數據有助於識別最新的欺詐模式。但是，為了檢測欺詐用例，請允許數據成熟。到期期限取決於您的業務，並且可能需要從兩週到三個月的任何地方。例如，如果您的事件包括信用卡交易，則資料的到期日可能會由信用卡的借項沖回期間或調查員決定所花費的時間來決定。

  確保用於訓練模型的數據集有足夠的時間根據您的業務成熟。
- 確保資料分佈不會顯著漂移- Amazon Fraud Detector 模型訓練程序會根據 EVENT_TIMESTAMP 為您的資料集進行樣本和分割。例如，如果您的資料集包含從過去 6 個月擷取的詐騙事件，但只包含

最後一個月的合法事件，則資料分佈會被視為漂移且不穩定。不穩定的資料集可能會導致模型效能評估出現偏差。如果您發現資料分佈顯著漂移，請考慮收集與目前資料分佈類似的資料來平衡資料集。

- 確保數據集代表實現/測試模型的用例- 否則，估計的性能可能會有偏差。假設您正在使用模型來自動拒絕所有門戶申請人，但是您的模型是使用具有先前批准的歷史數據/標籤的數據集進行培訓。然後，您的模型評估可能不正確，因為評估是基於沒有拒絕申請人表示的資料集。

事件資料格式

Amazon Fraud Detector 會將您的大部分資料轉換為所需的格式，做為模型訓練程序的一部分。不過，您可以輕鬆使用一些標準格式來提供資料，以協助避免 Amazon Fraud Detector 驗證資料集時發生問題。下表提供提供建議事件中繼資料之格式的指引。

> **Note**
>
> 建立 CSV 檔案時，請務必以大寫字母輸入如下所列的事件中繼資料名稱。

元數據名稱	格式	必要
事件識別碼	如有提供，它必須符合下列需求： • 這對於該事件來說是獨一無二的。 • 它代表了對您的業務有意義的信息。 • 它遵循正則表達式模式（例如，`^[0-9a-z_-]+$`.） • 除了上述要求之外，我們建議您不要在 EVENT_ID 附加時間戳記。這樣做可能會導致更新事件時出現問題。這是因為如果你這樣做，你必須提供完全相同的 EVENT_ID。	取決於型號類型

元數據名稱	格式	必要
事件時間戳	• 必須採用下列其中一種格式指定： • %YY-%mm-%Dt%HH:%mm: %ssz (ISO 8601 標準在世界標準時間內只有在世界標準時間，沒有毫秒) 範例：2019-11-30T13：凌晨 1 時 • %yyyy/%mm/%dd %hh:%公釐:% ss (上午/下午) 例子：下午一時三十一分或十一月三十一日 • %mm/%dd/%yyyy %hh:%毫米:% 例子：十一月三十日下午一時零一分，十一月三十日 • % 毫米 /%dd/%yy %hh:%毫米:% 例子：十一月三十一日下午一時零一分 • Amazon Fraud Detector 在剖析事件時間戳記的日期/時間戳記格式時，會進行下列假設： • 如果您使用的是 ISO 8601 標準，它必須完全符合上述規格	是

元數據名稱	格式	必要

	• 如果您使用的是其他格式之一，還有額外的靈活性：
	  • 對於月份和日期，您可以提供單一或兩位數字。例如，2019 年 1 月 12 日是一個有效的日期。
	  • 如果你沒有它們，你不需要包含 hh：mm：ss（也就是說，你可以簡單地提供一個日期）。您也可以提供小時和分鐘的子集 (例如 hh:mm)。不支持只提供小時。毫秒也不受支援。
	  • 如果您提供 AM/PM 標籤，則假設為 12 小時制。如果沒有 AM/PM 資訊，則假設為 24 小時制。
	  • 您可以使用「/」或「-」作為日期元素的分隔符。假定為時間戳元素「：」。	

實體識別碼	• 它必須遵循正則表達式模式：`^[0-9A-Za-z_.@+-]+$` 。 • 如果實體 ID 在評估時無法使用，請將實體 ID 指定為未知。	取決於型號類型
實體類型	您可以使用任何字符串	取決於型號類型

元數據名稱	格式	必要
事件標籤	您可以使用任何標籤，例如「欺詐」，「合法」，「1」或「0」。	如果包含標籤 _ 時間戳記，則需要
標籤時間戳記	它必須遵循時間戳記格式。	如果包含事件標籤，則需要

如需事件變數的相關資訊，請參閱變數。

> **Important**
>
> 如果您要建立帳戶接管見解 (ATI) 模型，請參閱準備資料以取得準備和選取資料的詳細資訊。

空值或缺少值

事件時間戳記和事件 _ 標籤變數不得包含任何空值或遺漏值。您可以為其他變數設定 null 或缺少值。但是，建議您對這些變數只使用少量空值。如果 Amazon Fraud Detector 判斷事件變數有太多空值或遺漏值，它會自動省略模型中的變數。

最小变量

建立模型時，除了必要的事件中繼資料之外，資料集還必須包含至少兩個事件變數。這兩個事件變數必須通過驗證檢查。

事件資料集大小

必要

您的資料集必須符合下列基本需求，才能成功進行模型訓練。

- 來自至少 100 個事件的數據。
- 資料集必須包含至少 50 個被歸類為詐騙的事件 (列)。

建議

我們建議您的資料集包含下列項目，以便成功進行模型訓練和良好的模型效能。

- 包括至少三週的歷史數據，但最多六個月的數據。

- 包含至少 10K 總事件資料。
- 包括至少 400 個分類為詐騙的事件 (列)，以及 400 個分類為合法的事件 (列)。
- 如果您的模型類型需要 ENTITY_ID，請包括 100 個以上的唯一實體。

資料集驗證

在 Amazon Fraud Detector 開始建立模型之前，它會檢查用於訓練模型的資料集中包含的變數是否符合大小、格式和其他需求。如果資料集未通過驗證，則不會建立模型。在建立模型之前，您必須先修正未通過驗證的變數。Amazon Fraud Detector 為您提供資料剖析工具，可在開始訓練模型之前，協助您識別並修正資料集的問題

資料剖析工具

Amazon Fraud Detector 提供開放原始碼工具，用於分析和準備資料以進行模型訓練。此自動化資料分析工具可協助您避免常見的資料準備錯誤，並識別潛在問題，例如錯誤對應的變數類型，這些問題會對模型效能造成負面影響。效能分析工具會產生直覺且全面的資料集報告，包括變數統計資料、標籤分佈、分類和數值分析，以及變數和標籤關聯性。它提供有關變數類型的指導，以及將資料集轉換為 Amazon Fraud Detector 所需格式的選項。

使用資料分析工具

自動化資料分析工具是使用AWS CloudFormation堆疊建置的，只要按幾下滑鼠即可輕鬆啟動。所有代碼都可以在 Github 上找到。如需如何使用資料剖析工具的相關資訊，請遵循我們部落格中的指示使用 Amazon Fraud Detector 的自動資料剖析工具更快訓練模型

常見事件資料集錯誤

以下是 Amazon Fraud Detector 在驗證事件資料集時遇到的一些常見問題。執行資料分析工具之後，請在建立模型之前，使用此清單檢查資料集是否有錯誤。

- CSV 檔案不是 UTF-8 格式的檔案。
- 資料集中的事件數目小於 100。
- 識別為欺詐或合法事件的數量少於 50。
- 與詐騙事件相關聯的唯一實體數量少於 100 個。
- EVENT_TIMESTAMP 中超過 0.1% 的值包含空值或受支持的日期/時間戳記格式以外的值。
- EVENT_LABEL 中超過 1% 的值包含事件類型中定義的空值或值以外的值。
- 小於兩個變數可用於模型訓練。

資料集儲存

收集資料集後，您可以使用 Amazon Fraud Detector 或 Amazon Simple Storage Service (Amazon S3) 將資料集存放在外部。建議您根據用於產生詐騙預測的模型，選擇儲存資料集的位置。有關模型類型的詳細資訊，請參閱選擇模型類型。如需儲存資料集的詳細資訊，請參閱事件資料儲存體。

事件類型

使用 Amazon 詐騙偵測器，您可以針對事件產生詐騙預測。事件類型定義傳送至 Amazon 詐騙偵測器之個別事件的結構。定義之後，您可以建立模型和偵測器，以評估特定事件類型的風險。

事件的結構包括下列項目：

- 實體類型：分類執行事件的人員。在預測期間，請指定實體類型和實體 ID，以定義執行事件的人員。
- 變數：定義可以作為事件一部分傳送的變數。模型和規則會使用變數來評估詐騙風險。新增之後，就無法從事件類型中移除變數。
- 標籤：將事件分類為欺詐或合法事件。在模型訓練期間使用。一旦新增，標籤就無法從事件類型中移除。

建立事件類型

在建立詐騙偵測模型之前，您必須先建立事件類型。創建事件類型涉及定義您的業務活動（事件）以評估欺詐行為。定義事件包括識別資料集中要包含用於詐騙評估的事件變數、指定起始事件的實體，以及將事件分類的標籤。

建立事件類型的先決條件

在開始建立事件類型之前，請確定您已完成下列項目：

- 使用此資料模型總管工具深入瞭解 Amazon 詐騙偵測器建立詐騙偵測模型所需的資料元素。
- 使用您從資料模型總管取得的深入解析來建立事件資料集，並將資料集上傳到 Amazon S3 儲存貯體。
- 已建立 Variables實體，且標籤您希望 Amazon 詐騙偵測器用於為此事件建立詐騙偵測模型。請確定您建立的變數、實體類型和標籤都包含在事件資料集中。

您可以使用 API，或使用 AWS SDK，在 Amazon 詐騙偵測器主控台中AWS CLI建立事件類型。

在 Amazon 詐騙偵測器主控台中建立事件類型

若要建立事件類型，

1. 開啟AWS管理主控台並登入您的帳戶。導航到亞馬遜欺詐檢測器。

2. 在左側導覽窗格中，選擇 [事件]。
3. 在 [事件類型] 頁面中，選擇 [建立]。
4. 在事件類型詳細信息下，
   a. 在名稱中，輸入活動的名稱。
   b. 在「描述」中，選擇性地輸入描述。
   c. 在「實體」中，選取您為事件建立的實體類型。
5. 在事件變量下，
   - 在 [選擇如何定義此事件的變數] 中，
     - 如果您已經為此事件建立了事件變數，請從變數清單中選取「選取變數」，然後在「變數」中選取您為此事件建立的變數。
     - 如果您尚未為此事件建立變數，請選取 [從訓練資料集選取變數]
       - 在 IAM 角色中，選取您希望 Amazon 詐騙偵測器用來存取包含資料集的 Amazon S3 儲存貯體的 IAM 角色
       - 在「資料」位置中，輸入資料集位置的路徑。使用類似於這樣的S3 URI路徑：`S3://your-bucket-name/example dataset filename.csv`。
       - 選擇 Upload (上傳)。
       - 在「變數」下，會顯示 Amazon 詐騙偵測器從資料集檔案擷取的所有事件變數名稱。

         如果您想要包含變數以偵測詐騙，請在「變數」類型中選取變數類型。選擇 [移除] 以移除包含在詐騙偵測中的變數。對清單中的每個變數重複此步驟。
6. 在 [標籤 (選用)] 下的 [標籤] 中，選取您為此事件建立的標籤。請務必針對詐騙和合法事件分別選取一個標籤。
7. 如果您想要為此事件設定自動下游處理，請在使用 Amazon 的事件協調 EventBridge-選用下，開啟啟用 Amazon 事件協調流程。EventBridge如需事件協調流程的詳細資訊，請參閱活動編排。

   > **Note**
   >
   > 您也可以在稍後建立事件類型之後啟用事件協調流程。

8. 選擇 [建立事件類型]。

使用建立事件類型 AWS SDK for Python (Boto3)

下列範例顯示 PutEventType API 的範例要求。此範例假設您已建立變數ip_addressemail_address、標籤legit和fraud和實體類型sample_customer。若要取得有關如何建立這些資源的資訊，請參閱資源。

> **Note**
>
> 在將變數、實體類型和標籤新增至事件類型之前，您必須先建立變數、實體類型和標籤。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_event_type (
name = 'sample_registration',
eventVariables = ['ip_address', 'email_address'],
labels = ['legit', 'fraud'],
entityTypes = ['sample_customer'])
```

刪除事件或事件類型

當您刪除事件時，Amazon 詐騙偵測器會永久刪除該事件，且與該事件相關的資料將不再儲存在 Amazon 詐騙偵測器中。

刪除 Amazon 詐騙偵測器已透過 **GetEventPrediction** API 評估的事件

1. 登入AWS Management Console並開啟亞馬遜詐騙偵測器主控台，網址為 https://console.aws.amazon.com/frauddetector。
2. 在主控台的左側導覽窗格中，選擇 [搜尋過去的預測]。
3. 選擇您要刪除的事件。
4. 選擇「動作」，然後選擇「刪除事件」。
5. 輸入**delete**，然後選擇 [刪除事件]。

> **Note**
>
> 這會刪除與該事件 ID 相關聯的所有記錄，包括傳送至作業的任何事件資料，以及透過SendEvent作業產生的任何預測資料。GetEventPrediction

若要刪除儲存在 Amazon 詐騙偵測器中但尚未評估的事件 (亦即透過SendEvent作業儲存) 的事件，您必須提出DeleteEvent請求並指定事件 ID 和事件類型 ID。如果要同時刪除事件和與事件相關聯的任何預測歷史記錄，請將deleteAuditHistory參數的值設置為「true」。將deleteAuditHistory參數設定為「true」時，事件資料在刪除作業完成後最多可透過搜尋取得 30 秒。

若要刪除與某個事件類型相關聯的所有事件

1. 在主控台的左側導覽窗格中，選擇 [事件類型]
2. 選擇您要刪除所有事件的事件類型。
3. 瀏覽至 [儲存的事件] 索引標籤，並選擇 [刪除

視事件類型的儲存事件數目而定，刪除所有儲存的事件可能需要一些時間。例如，一個 1 GB 的資料集 (一般客戶約為 1-2 百萬個事件) 需要大約 2 小時才能刪除。在此期間，不會儲存您傳送至 Amazon 詐騙偵測器此事件類型的新事件，但您可以繼續透過GetEventPrediction作業產生詐騙預測。

若要刪除事件類型

您無法刪除偵測器或模型中使用的事件類型，或具有相關聯的已儲存事件。刪除事件類型之前，您必須刪除與該事件類型相關聯的所有事件。

刪除事件類型時，Amazon 詐騙偵測器會永久刪除該事件類型，且資料不會再儲存在 Amazon 詐騙偵測器中。

1. 在 Amazon 詐騙偵測器主控台的左側導覽窗格中，選擇 [資源]，然後選擇 [事件]。
2. 選擇您要刪除的事件類型。
3. 選擇 [動作]，然後選擇 [刪除事件類型]。
4. 輸入事件類型名稱，然後選擇 [刪除事件類型]。

事件資料儲存體

收集資料集之後，您可以使用 Amazon Storage Service (Amazon S3) Fraud Detector 資料集存放在內部。建議您根據用於產生詐騙預測的模型，選擇儲存資料集的位置。以下是這兩個儲存選項的詳細說明。

- 內部儲存- 您的資料集會與 Amazon Fraud Detector 一起儲存。與事件相關聯的所有事件資料都會儲存在一起。您可以隨時上傳透過 Amazon Fraud Detector 儲存的事件資料集。您可以一次將事件串流至 Amazon Fraud Detector API，或使用批次匯入功能匯入大型資料集 (最多 1GB)。使用 Amazon Fraud Detector 儲存的資料集訓練模型時，您可以指定時間範圍來限制資料集的大小。
- 外部儲存- 您的資料集儲存在 Amazon Fraud Detector 以外的外部資料來源中。目前 Amazon Fraud Detector 支援使用 Amazon Storage Service (Amazon S3)。如果您的模型位於已上傳至 Amazon S3 的檔案上，則該檔案的未壓縮資料不得超過 5GB。如果不止於此，請務必縮短資料集的時間範圍。

下表提供有關模型類型及其支援的資料來源的詳細資訊。

模型類型	相容的訓練資料來源
線上詐騙詳情的	外接儲存裝置、內部儲存
交易詐騙詳情的	內部儲存體
帳戶接管詳情的	內部儲存體

如需使用 Amazon 簡單儲存服務在外部存放資料集的相關資訊，請參閱透過 Amazon S3 在外部存放您的事件資料 。如需使用 Amazon Fraud Detector 在內部儲存資料集的資訊，請參閱使用 Amazon Fraud Detector 在內部存放您的事件資料。

透過 Amazon S3 在外部存放您的事件資料

如果您正在訓練線上詐騙洞見模型，您可以選擇將事件資料存放在 Amazon S3 外部。若要將事件資料存放在 Amazon S3，您必須先建立 CSV 格式的文字檔案、新增事件資料，然後將 CSV 檔案上傳到 Amazon S3 儲存貯體。

> **Note**
>
> 交易詐騙洞見和帳戶接管洞察模型類型不支援透過 Amazon S3 外部存放的資料集

建立 CSV 檔案

Amazon Fraud Detector 要求 CSV 檔案的第一列包含欄標題。CSV 檔案中的欄標題必須對應至事件類型中定義的變數。如需資料集範例，請參閱取得並上傳範例資料集

線上詐騙深入分析模型需要具有至少 2 個變數和 100 個變數的訓練資料集。除了事件變數之外，訓練資料集還必須包含下列標題：

- 事件 _ 時間戳記-定義事件發生時的時間戳記
- 事件標籤-將事件分類為詐騙或合法。欄中的值必須與事件類型中定義的值相對應。

下列 CSV 資料範例代表來自線上商家的歷史註冊事件：

```
EVENT_TIMESTAMP,EVENT_LABEL,ip_address,email_address
4/10/2019 11:05,fraud,209.146.137.48,fake_burtonlinda@example.net
12/20/2018 20:04,legit,203.0.112.189,fake_davidbutler@example.org
3/14/2019 10:56,legit,169.255.33.54,fake_shelby76@example.net
1/3/2019 8:38,legit,192.119.44.26,fake_curtis40@example.com
9/25/2019 3:12,legit,192.169.85.29,fake_rmiranda@example.org
```

> **Note**
>
> CSV 資料檔案可以包含雙引號和逗號做為資料的一部分。

對應事件類型的簡化版本如下所示。事件變數對應於 CSV 檔案中的標頭，中的值EVENT_LABEL對應於標籤清單中的值。

```
(
name = 'sample_registration',
eventVariables = ['ip_address', 'email_address'],
labels = ['legit', 'fraud'],
entityTypes = ['sample_customer']
)
```

事件時戳記格式

請確定您的事件時間戳記是必要的格式。作為模型構建過程的一部分，在線欺詐洞察模型類型會根據事件時間戳記對您的數據進行排序，並將您的數據分割用於培訓和測試目的。為了獲得公平的效能估計，模型會先在訓練資料集上進行訓練，然後在測試資料集上測試此模型。

Amazon Fraud Detector 支援模型訓練期間值的下列日期/時`EVENT_TIMESTAMP`間戳記格式：

- %YY-%MM-%Dt%HH: %mm: %ssz (國際標準時間僅在世界標準時間內使用 ISO 8601 標準，沒有毫秒)

  範例：2019-11-30T13：凌晨 1 時
- %yyyy/%mm/%dd %hh:% 公釐:% ss (上午/下午)

  例子：下午一時三十一分或十一月三十一日
- %mm/%dd/%yyyy %hh:% 毫米:%

  例子：11 月 30 日下午 1 時 1 分 1 分，十一月三十日
- % 毫米 /%dd/%yy %hh:% 毫米:% ss

  例子：十一月三十一日下午一時零一分，十一月三十一日

Amazon Fraud Detector 在剖析事件時間戳記的日期/時間戳記格式時，會進行下列假設：

- 如果您使用的是 ISO 8601 標準，它必須完全符合上述規格
- 如果您使用的是其他格式之一，還有額外的靈活性：
  - 對於月份和日期，您可以提供單一或兩位數字。例如，2019 年 1 月 12 日為有效日期。
  - 你不需要包括 hh: mm: ss，如果你沒有他們 (所以, 你可以簡單地提供一個日期). 您也可以提供小時和分鐘的子集 (例如 hh: mm)。不支持只提供小時。毫秒也不受支援。
  - 如果您提供 AM/PM 標籤，則假設為 12 小時制。如果沒有 AM/PM 資訊，則假設為 24 小時制。
  - 您可以使用「/」或「-」作為日期元素的分隔符。假定為時間戳元素「：」。

跨時間取樣資料集

我們建議您提供相同時間範圍內的欺詐和合法樣本的示例。例如，如果您提供過去 6 個月的詐騙事件，您也應該提供平均跨越相同時段的合法事件。如果您的資料集包含高度不均勻的詐騙和合法事件分佈，您可能會收到下列錯誤訊息：「不同時間的詐騙散佈情形不可接受。無法正確分割資料集。」 通

常，此錯誤最簡單的解決方法是確保在相同的時間範圍內均勻地採樣欺詐事件和合法事件。如果您在短時間內遭遇大量欺詐，則可能還需要刪除數據。

如果您無法生成足夠的數據來創建均勻分佈的數據集，則一種方法是隨機化事件的 EVENT_TIMESTAMP，使其均勻分佈。不過，這通常會導致效能指標不切實際，因為 Amazon Fraud Detector 使用 EVENT_TIMESTAMP 來評估資料集中適當事件子集的模型。

空值和缺少值

亞馬遜 Fraud Detector 處理空值和缺失值。但是，變量的空值百分比應該受到限制。「事件時間戳記」和「事件 _ 標籤」欄不應包含任何遺漏的值。

檔案驗證

如果觸發下列任何一種條件，Amazon Fraud Detector 將無法訓練模型：

- 如果無法剖析 CSV
- 如果資料行的資料類型不正確

將事件資料上傳事件資料至 Amazon S3 儲存貯體

使用事件資料建立 CSV 檔案之後，將檔案上傳檔案上傳檔案上傳檔案上傳檔案至 Amazon S3 儲存貯體。

將上傳至 Amazon S3 儲存貯體

1. 登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/s3/ 的 Amazon S3 主控台。
2. 選擇 Create bucket (建立儲存貯體)。

   Create bucket (建立儲存貯體) 精靈會開啟。
3. 在 Bucket name (儲存貯體名稱) 中，為儲存貯體輸入符合 DNS 規範的名稱。

   儲存貯體名稱必須；

   - 在所有 Amazon S3 中都為唯一。
   - 長度必須介於 3 與 63 個字元之間。
   - 不含大寫字元。

- 以小寫字母或數字開頭。

建立儲存貯體後，便無法變更其名稱。如需有關命名儲存貯體的詳細資訊，請參閱《Amazon SStorage Service 使用者指南》中的儲存貯體

> ⚠ Important
>
> 避免在儲存貯體名稱中包含敏感資訊，例如帳戶號碼。在指向儲存貯體中之物件的 URL 中，會顯示儲存貯體名稱。

4. 針對 Region (區域)，選擇希望存放儲存貯體的 AWS 區域。您必須選擇使用 Amazon East (N. Virginia) Fraud Detector 國東部 (俄亥俄)、美國東部 (俄亥俄)、美國西部 (奧勒岡)、歐洲 (愛爾蘭)、亞太區域 (新加坡) 或亞太區域 (雪梨)。
5. 在 Bucket settings for Block Public Access (封鎖公開存取的儲存貯體設定) 中，選擇要套用至儲存貯體的封鎖公開存取設定。

   建議您將所有設定保持啟用的狀態。如需有關封鎖封鎖封鎖封鎖封鎖封鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖 Amazon Storage Service
6. 選擇 建立儲存貯體 。
7. 將訓練資料檔案上傳訓練檔案上 Amazon S3 資料檔案 請記下訓練檔案的 Amazon S3 位置路徑 (例如 s3://bucketname/object.csv)。

使用 Amazon Fraud Detector 在內部存放您的事件資料

您可以選擇在 Amazon Fraud Detector 中存放事件資料，稍後再使用儲存的資料來訓練模型。透過將事件資料存放在 Amazon Fraud Detector 中，您可以訓練使用自動計算變數的模型來提升效能、簡化模型再訓練，以及更新詐騙標籤以關閉機器學習回饋迴圈。事件會儲存在 Event Type 資源層級，因此相同事件類型的所有事件都會一起儲存在單一事件類型資料集中。在定義事件類型時，您可以選擇性地指定是否要儲存該事件類型的事件，方法是切換 Amazon Fraud Detector 主控台中的「事件擷取」設定。

您可以在 Amazon Fraud Detector 中存放單一事件或匯入大量事件資料集。單一事件可以使用 GetEventPredictionAPI 或 API 進行串流處SendEvent理。您可以使用 Amazon Fraud Detector 主控台中的批次匯入功能或使用 CreateBatchImportJobAPI，快速輕鬆地將大型資料集匯入 Amazon Fraud Detector。

您可以隨時使用 Amazon Fraud Detector 主控台來檢查每個事件類型已存放的事件數量。

準備事件資料以進行儲存

使用 Amazon Fraud Detector 在內部儲存的事件資料會儲存在Event Type資源層級。因此，來自相同事件的所有事件資料都會儲存在單一事件中Event Type。儲存的事件稍後可用來訓練新模型或重新訓練現有模型。使用預存的事件資料訓練模型時，您可以選擇性地指定事件的時間範圍，以限制訓練資料集的大小。

每次您使用 Amazon Fraud Detector 主控台、API 或SendEvent API 將資料存放在 Amazon Fraud Detector 時，Amazon Fraud Detector 都會在存放之前驗證您的資料。CreateBatchImportJob如果您的資料驗證失敗，則不會儲存事件資料。

使用 Amazon Fraud Detector 在內部存放資料的先決條

- 為了確保您的事件資料通過驗證並成功儲存資料集，請確定您已使用資料模型總管提供的深入解析來準備資料集。
- 為您要使用 Amazon Fraud Detector 存放的事件資料建立事件類型。如果你還沒有，請按照 intstructions 創建一個事件類型。

智慧資料驗證

當您在 Amazon Fraud Detector 主控台上傳資料集以進行批次匯入時，Amazon Fraud Detector 會使用智慧資料驗證 (SDV) 在匯入資料之前驗證您的資料集。SDV 會掃描上傳的資料檔案，並識別資料遺失、格式不正確或資料類型等問題。除了驗證資料集之外，SDV 還提供驗證報告，列出所有已識別的問題，並建議修正最具影響力的問題的動作。SDV 識別出的某些問題可能很重要，必須先解決，Amazon Fraud Detector 才能成功匯入您的資料集。如需詳細資訊，請參閱智能數據驗證報告。

SDV 會在檔案層級和資料 (列) 層級驗證您的資料集。在檔案層級，SDV 會掃描您的資料檔案，並識別存取檔案的權限不足、不正確的檔案大小、檔案格式和標頭 (事件中繼資料和事件變數) 等問題。在資料層級，SDV 會掃描每個事件資料 (列)，並識別不正確的資料格式、資料長度、時間戳記格式和 Null 值等問題。

智慧資料驗證目前僅在 Amazon Fraud Detector 主控台提供，且驗證預設為開啟。如果您不希望 Amazon Fraud Detector 在匯入資料集之前使用智慧型資料驗證，請在上傳資料集時關閉 Amazon Fraud Detector 主控台中的驗證。

使用 API 或AWS SDK 時驗證儲存的資料

透過、或CreateBatchImportJob API 操作上傳事件
時SendEventGetEventPrediction，Amazon Fraud Detector 會驗證下列項目：

- 該事件類型的 EventIngestion 設定為「已啟用」。
- 事件時間戳記無法更新。具有重複事件 ID 和不同 EVENT_TIMESTAMP 的事件將被視為錯誤。
- 變數名稱和值符合預期的格式。如需詳細資訊，請參閱 創建一個變量
- 必要的變數會填入值。
- 所有活動時間戳記不超過 18 個月，而且 future 也不會出現。

使用批次匯入儲存事件資料

透過批次匯入功能，您可以使用主控台、API 或 AWS 開發套件，在 Amazon Fraud Detector 中快速輕鬆地上傳大型歷史事件資料集。若要使用批次匯入，請建立包含所有事件資料的 CSV 格式的輸入檔案，將 CSV 檔案上傳到 Amazon S3 儲存貯體，然後開始匯入任務。Amazon Fraud Detector 會先根據事件類型驗證資料，然後自動匯入整個資料集。匯入資料之後，就可以用於訓練新模型或重新訓練現有模型。

輸入和輸出檔案

輸入 CSV 檔案必須包含符合關聯事件類型中定義之變數的標頭，以及四個強制變數。如需詳細資訊，請參閱 準備事件資料以進行儲存。輸入資料檔案的大小上限為 20 GB，或約 5000 萬個事件。活動數量將根據您的活動規模而有所不同。如果匯入工作成功，則輸出檔案為空。如果匯入失敗，輸出檔案會包含錯誤記錄檔。

建立 CSV 檔案

Amazon Fraud Detector 只會從逗號分隔值 (CSV) 格式的檔案匯入資料。CSV 檔案的第一列必須包含與相關事件類型中定義之變數完全相符的欄標題，以及四個強制變數：EVENT_ID、事件時間戳記、ENTTY_ID 和 ENTITY_TYPE。您還可以選擇包括事件 _ 標籤和標籤 _ 時間戳記（如果包含事件 _ 標籤，則需要標籤 _ 時間戳記）。

定義強制性變數

強制性變數會被視為事件中繼資料，而且必須以大寫字母指定。會自動包含事件中繼資料以進行模型訓練。下表列出了強制性變量，每個變量的描述以及變量所需的格式。

名稱	描述	請求
事件識別碼	事件的識別碼。例如，如果您的活動是線上交易，EVENT	• 批次匯入工作需要使用 EVENT_ID。

名稱	描述	請求
	_ID 可能是提供給客戶的交易參考編號。	• 該事件必須獨一無二。 • 它應該代表對您的業務有意義的信息。 • 它必須滿足規則表達式模式（例如，^[0-9a-z_-]+$.） • 我們不建議您將時間戳記附加到 EVENT_ID。這樣做可能會導致更新事件時出現問題。這是因為如果你這樣做，你必須提供完全相同的 EVENT_ID。

名稱	描述	請求
事件時間戳	事件發生時的時間戳記。時間戳記必須採用 ISO 8601 標準 (世界標準時間)。	• 批次匯入工作需要事件時間戳記。 • 該名稱必須以下其中一種格式指定： • %YY-%MM-%Dt%HH: %mm: %ssz (國際標準時間僅在世界標準時間內使用 ISO 8601 標準，沒有毫秒) 範例：2019-11-30T13：凌晨 1 時 • %yyyy/%mm/%dd %hh:% 公釐:% ss (上午/下午) 例子：下午一時三十一分或十一月三十一日 • %mm/%dd/%yyyy %hh:% 毫米:% 例子：11 月 30 日下午 1 時 1 分 1 分，十一月三十日 • % 毫米 /%dd/%yy %hh:% 毫米:% ss 例子：十一月三十一日下午一時零一分，十一月三十一日 • Amazon Fraud Detector 在剖析事件時間戳記的日期/時間戳記格式時，會進行下列假設：

名稱	描述	請求

		• 如果您使用的是 ISO 8601 標準，它必須完全符合上述規格
		• 如果您使用的是其他格式之一，還有額外的靈活性：
		  • 對於月份和日期，您可以提供單一或兩位數字。例如，2019 年 1 月 12 日為有效日期。
		  • 如果你沒有它們，你不需要包含 hh：mm：ss（也就是說，你可以簡單地提供一個日期）。您也可以提供小時和分鐘的子集 (例如 hh:mm)。不支持只提供小時。毫秒也不受支援。
		  • 如果您提供 AM/PM 標籤，則假設為 12 小時制。如果沒有 AM/PM 資訊，則假設為 24 小時制。
		  • 您可以使用「/」或「-」作為日期元素的分隔符。假定為時間戳元素「：」。

名稱	描述	請求
實體識別碼	執行事件之實體的識別碼。	• 批次匯入工作需要 ENTTY_ID • 它必須遵循正則表達式模式：`^[0-9A-Za-z_.@+-]+$` 。 • 如果實體 ID 在評估時無法使用，請將實體 ID 指定為未知。
實體類型	執行事件的實體，例如商家或客戶	批次匯入工作需要實體類型
事件標籤	將事件分類為`fraudulent` 或`legitimate`	如果包含標籤 _ 時間戳記，則需要事件 _ 標籤
標籤時間戳記	上次填入或更新事件標籤時的時間戳記	• 如果包含事件標籤，則需要標籤 _ 時間戳記。 • 它必須遵循時間戳記格式。

將 CSV 檔案上傳 CSV 檔案上 Amazon S3 案上傳 CSV 檔案

使用資料建立 CSV 檔案之後，將檔案上傳檔案上傳檔案上傳檔案至 Amazon Storage Service (Amazon S3) 儲存貯體。

將事件資料上傳事件資料至 Amazon S3 儲存貯體

1. 登入 AWS Management Console，並開啟位於 https://console.aws.amazon.com/s3/ 的 Amazon S3 主控台。
2. 選擇 Create bucket (建立儲存貯體)。

   Create bucket (建立儲存貯體) 精靈會開啟。
3. 在 Bucket name (儲存貯體名稱) 中，為儲存貯體輸入符合 DNS 規範的名稱。

   儲存貯體名稱必須；

   - 在所有 Amazon S3 中都為唯一。

- 長度必須介於 3 與 63 個字元之間。
- 不含大寫字元。
- 以小寫字母或數字開頭。

建立儲存貯體後，便無法變更其名稱。如需有關命名儲存貯體的詳細資訊，請參閱《Amazon SStorage Service 使用者指南》中的儲存貯體

> ⚠ Important
>
> 避免在儲存貯體名稱中包含敏感資訊，例如帳戶號碼。在指向儲存貯體中之物件的 URL 中，會顯示儲存貯體名稱。

4. 針對 Region (區域)，選擇希望存放儲存貯體的 AWS 區域。您必須選擇使用 Amazon East (N. Virginia) Fraud Detector 國東部 (俄亥俄)、美國東部 (俄亥俄)、美國西部 (奧勒岡)、歐洲 (愛爾蘭)、亞太區域 (新加坡) 或亞太區域 (雪梨)。
5. 在 Bucket settings for Block Public Access (封鎖公開存取的儲存貯體設定) 中，選擇要套用至儲存貯體的封鎖公開存取設定。

   建議您將所有設定保持啟用的狀態。如需有關封鎖封鎖封鎖封鎖封鎖封鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖鎖 Amazon Storage Service
6. 選擇 建立儲存貯體 。
7. 將訓練資料檔案上傳訓練檔案上 Amazon S3 資料檔案 請記下訓練檔案的 Amazon S3 位置路徑 (例如 s3://bucketname/object.csv)。

在 Amazon Fraud Detector 主控台中 Batch 匯入事件資料

您可以使用`CreateBatchImportJob` API 或使用 AWS 開發套件，在 Amazon Fraud Detector 主控台輕鬆匯入大量事件資料集。在繼續之前，請確定您已遵循指示將資料集準備為 CSV 檔案。確定您也將 CSV 檔案上傳至 Amazon S3 儲存貯體。

使用 Amazon Fraud Detector 主控台

若要在主控台中批次匯入事件資料

1. 開啟 AWS 主控台並登入您的帳戶，然後瀏覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇事件。

3. 選擇事件類型。
4. 選擇存儲的事件選項卡。
5. 在 [已儲存的事件詳細資料] 窗格中，確定 [事件擷取] 為 [開啟]。
6. 在 [匯入事件資料] 窗格中，選擇 [新增匯入]。
7. 在 [新事件匯入] 頁面中，提供下列資訊：

   - [建議] 將啟用此資料集的智慧資料驗證-新的設定保留為預設設定。
   - 對於資料的 IAM 角色，請選取您為包含您計劃匯入的 CSV 檔案的 Amazon S3 儲存貯體建立的 IAM 角色。
   - 在輸入資料位置中，輸入您擁有 CSV 檔案的 S3 位置。
   - 如果要指定單獨的位置來存放匯入結果，請按一下輸入和結果分隔資料位置按鈕，並提供有效的 Amazon S3 儲存貯體位置。

   > **Important**
   >
   > 請確定您選取的 IAM 角色具有輸入 Amazon S3 儲存貯體的讀取許可，以及對輸出 Amazon S3 儲存貯體寫入許可。

8. 選擇 Start (啟動)。
9. [匯入事件] 資料窗格中的 [狀態] 欄會顯示驗證和匯入工作的狀態。頂端的橫幅提供資料集首先經過驗證，然後匯入時，狀態的高階描述。
10. 請遵循提供給的指導監控資料集驗證和匯入任務的進度。

監控資料集驗證和匯入任務的進度

如果您使用 Amazon Fraud Detector 主控台執行批次匯入任務，Amazon Fraud Detector 預設會在匯入前驗證您的資料集。您可以在 Amazon Fraud Detector 主控台的 [新事件匯入] 頁面中監控驗證和匯入任務的進度和狀態。頁面頂端的橫幅會提供驗證發現項目的簡短說明，以及匯入任務的狀態。根據驗證發現項目和匯入工作的狀態，您可能需要採取動作，以確保資料集的驗證和匯入成功。

下表根據驗證和匯入作業的結果，提供您必須採取之動作的詳細資訊。

橫幅訊息	狀態	代表什麼意思	我該怎麼辦
驗證已開始	驗證中	SDV 已開始驗證您的資料集	等待狀態變更
由於資料集發生錯誤，資料驗證無法繼續進行。修正資料檔案中的錯誤，並開始新的匯入工作。如需詳細資訊，請參閱驗證報告	驗證失敗	SDV 在您的資料檔案中識別出問題。必須解決這些問題才能成功匯入資料集。	在匯入事件資料窗格中，選取 Job ID 並檢視驗證報告。遵循報告中的「建議」，以解決列出的所有錯誤。如需詳細資訊，請參閱使用驗證報告。
已開始匯入資料。驗證已成功完成	匯入中	您的資料集已通過驗證。漁農處已開始匯入您的資料集	等待狀態變更
驗證已完成，但有警告。已開始匯入資料	匯入中	資料集中的某些資料驗證失敗。但是，通過驗證的資料符合匯入的最小資料大小需求。	監視橫幅中的訊息，並等待狀態變更
您的資料已部分匯入。有些資料驗證失敗且未匯入。請參閱驗證報告以取得更多資訊。	已匯入。狀態會顯示警告圖示。	未匯入資料檔案中驗證失敗的某些資料。已匯入通過驗	在匯入事件資料窗格中，選取 Job ID 並檢視驗證報告。遵循「資料層級警告」表格中的「建議」來處理列出的警告。您無需解決所有警告。不過，請確定您的資料集擁有 50%

橫幅訊息	狀態	代表什麼意思	我該怎麼辦
		證的其餘資料。	以上的資料，這些資料通過驗證，才能成功匯入。處理完警告之後，請啟動新的匯入工作。如需詳細資訊，請參閱使用驗證報告。
資料匯入失敗，因為處理錯誤。開始新資料匯入任務	匯入失敗	由於暫時性執行階段錯誤，匯入失敗	開始新匯入任務
已成功匯入資料	已匯入	驗證和匯入都順利完成	選取匯入 Job 的工作 ID 以檢視詳細資料，然後繼續進行模型訓練

> **Note**
>
> 建議您在資料集成功匯入 Amazon Fraud Detector 後等候 10 分鐘，以確保系統完全擷取這些資料集。

智能數據驗證報告

智慧資料驗證會在驗證完成後建立驗證報告。驗證報表提供 SDV 在資料集中識別的所有問題的詳細資料，並提供修正最具影響力問題的建議動作。您可以使用驗證報表來判斷問題所在、問題在資料集中的位置、問題的嚴重性，以及如何修正問題。即使驗證成功完成，也會建立驗證報告。在這種情況下，您可以查看報告以查看是否列出任何問題，以及是否存在，請決定是否要修復任何問題。

> **Note**
>
> SDV 的目前版本會掃描您的資料集，找出可能導致批次匯入失敗的問題。如果驗證和批次匯入成功，您的資料集仍可能存在可能導致模型訓練失敗的問題。我們建議您檢視驗證報告，即使驗證和匯入成功，並解決報告中列出的任何問題，以便成功進行模型訓練。解決問題之後，請建立新的批次匯入工作。

存取驗證報告

您可以使用下列其中一個選項，在驗證完成後隨時存取驗證報表：

1. 驗證完成後，匯入工作正在進行時，在頂端橫幅中，選擇 [檢視驗證報告]。
2. 匯入 Job 完成後，在 [匯入事件] 資料窗格中，選擇剛完成之匯入工作的 [工作 ID]。

使用驗證報告

匯入工作的驗證報表頁面會提供此匯入工作的詳細資訊、如果找到的嚴重錯誤清單、有關資料集中特定事件 (資料列) 的警告清單 (如果找到)，以及資料集的簡短摘要，其中包括無效值，以及每個變數的遺漏值。

- 匯入工作詳情

  提供匯入任務的詳細資訊。如果匯入工作失敗或資料集已部分匯入，請選擇 [前往結果檔案] 以檢視匯入失敗之事件的錯誤記錄。

- 嚴重錯誤

  提供 SDV 識別資料集中最具影響力問題的詳細資訊。此窗格中列出的所有問題都很重要，您必須先解決這些問題，然後再繼續匯入。如果您嘗試匯入資料集而未解決重大問題，則匯入工作可能會失敗。

  若要解決嚴重問題，請遵循針對每個警告提供的建議。解決「嚴重錯誤」窗格中列出的所有問題後，請建立新的批次匯入工作。

- 資料層級警告

  提供資料集中特定事件 (資料列) 警告的摘要。如果已填入 [資料層級警告] 窗格，則資料集中的某些事件驗證失敗且未匯入。

  對於每個警告，「描述」欄會顯示發生問題的事件數目。範例事件 ID 會提供範例事件 ID 的部分清單，您可以用來做為起點，以尋找發生問題的其餘事件。使用針對警告提供的建議來修正此問題。另外，請使用輸出檔案中的錯誤記錄檔，以取得有關此問題的其他資訊。會針對批次匯入失敗的所有事件產生錯誤記錄。若要存取錯誤記錄，請在 [匯入工作詳細資料] 窗格中，選擇 [移至結果檔案]。

> **Note**
>
> 如果資料集中超過 50% 的事件 (資料列) 驗證失敗，匯入工作也會失敗。在此情況下，您必須先修正資料，然後再開始新的匯入工作。

- 資料集摘要

  提供資料集驗證報表的摘要。如果警告數目欄顯示的警告數目超過 0，請決定是否需要修正這些警告。如果警告數目欄顯示 0，請繼續訓練您的模型。

使用 AWS 開發套件 (Boto3) Batch 匯入事件資料

以下範例會顯示 CreateBatchImportJobAPI 的範例請求。批次匯入工作必須包含 Jobid、輸入路徑、輸出路徑eventTypeName和iamRoleArn。Jobid 不能包含過去工作的相同 ID，除非該工作存在於 CREATE_FAILED 狀態。輸入路徑和輸出路徑必須是有效的 S3 路徑。您可以選擇不在 OutputPath 中指定檔案名稱，但仍需提供有效的 S3 儲存貯體位置。 eventTypeName 和 iamRoleArn 必須存在。IAM 角色必須授與讀取許可才能輸入 Amazon S3 儲存貯體和寫入許可才能輸出 Amazon S3 儲存貯體。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_batch_import_job (
jobId = 'sample_batch_import',
inputPath = 's3://bucket_name/input_file_name.csv',
outputPath = 's3://bucket_name/',
eventTypeName = 'sample_registration',
iamRoleArn: 'arn:aws:iam::************:role/service-role/AmazonFraudDetector-
DataAccessRole-************'
)
```

取消批次匯入工作

您可以隨時在 Amazon Fraud Detector 主控台中使用CancelBatchImportJob API 或 AWS 開發套件取消進行中的批次匯入任務。

若要在 Console 中取消批次匯入任務，

1. 開啟 AWS 主控台並登入您的帳戶，然後瀏覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇事件。
3. 選擇事件類型。
4. 選擇存儲的事件選項卡。
5. 在 [匯入事件] 資料窗格中，選擇您要取消的進行中匯入工作的工作 ID。
6. 在事件工作頁面中，按一下動作，然後選取取消事件匯入。
7. 選擇「停止事件匯入」以取消批次匯入工作。

使用 AWS 開發套件 (Boto3) 取消批次匯入任務

以下範例會顯示`CancelBatchImportJob` API 的範例請求。取消匯入工作必須包含進行中批次匯入工作的工作 ID。

```
import boto3
fraudDetector = boto3.client('frauddetector')
fraudDetector.cancel_batch_import_job (
    jobId = 'sample_batch'
)
```

使用 GetEventPredictions API 作業儲存事件資料

根據預設，傳送至`GetEventPrediction` API 進行評估的所有事件都會儲存在 Amazon Fraud Detector 中。這表示 Amazon Fraud Detector 會在您產生預測時自動存放事件資料，並使用該資料以近乎即時的方式更新計算的變數。您可以在 Amazon Fraud Detector 主控台中導覽至事件類型，然後將事件擷取設定為關閉，或使用`PutEventType` API 操作將 EventIngestion 值更新為已停用，以停用資料儲存。如需關於`GetEventPrediction` API 操作的更多資訊，請參閱詐騙預測。

> **Important**
>
> 我們強烈建議您在啟用事件類型的事件擷取之後，將其保持啟用狀態。停用相同事件類型的事件擷取，然後產生預測可能會導致行為不一致。

使用 SendEvent API 作業儲存事件資料

您可以使用SendEvent API 操作將事件存放在 Amazon Fraud Detector 中，而無需針對這些事件產生詐騙預測。例如，您可以使用SendEvent作業上傳歷史資料集，稍後可用來訓練模型。

SendEvent API 的事件時間戳記格式

使用SendEvent API 儲存事件資料時，您必須確定事件時間戳記是必要的格式。Amazon Fraud Detector 支援下列日期/時間戳記格式：

- %YY-%MM-%Dt%HH: %mm: %ssz (國際標準時間僅在世界標準時間內使用 ISO 8601 標準，沒有毫秒)

  範例：2019-11-30T13：凌晨 1 時
- %yyyy/%mm/%dd %hh:% 公釐:% ss (上午/下午)

  例子：下午一時三十一分或十一月三十一日
- %mm/%dd/%yyyy %hh:% 毫米:%

  例子：11 月 30 日下午 1 時 1 分 1 分，十一月三十日
- % 毫米 /%dd/%yy %hh:% 毫米:% ss

  例子：十一月三十一日下午一時零一分，十一月三十一日

Amazon Fraud Detector 在剖析事件時間戳記的日期/時間戳記格式時，會進行下列假設：

- 如果您使用的是 ISO 8601 標準，它必須完全符合上述規格
- 如果您使用的是其他格式之一，還有額外的靈活性：
  - 對於月份和日期，您可以提供單一或兩位數字。例如，2019 年 1 月 12 日為有效日期。
  - 如果你沒有它們，你不需要包含 hh：mm：ss（也就是說，你可以簡單地提供一個日期）。您也可以提供小時和分鐘的子集 (例如 hh: mm)。不支持只提供小時。毫秒也不受支援。
  - 如果您提供 AM/PM 標籤，則假設為 12 小時制。如果沒有 AM/PM 資訊，則假設為 24 小時制。
  - 您可以使用「/」或「-」作為日期元素的分隔符。假定為時間戳元素「：」。

以下是SendEvent API 呼叫範例。

```
import boto3
```

```
fraudDetector = boto3.client('frauddetector')

fraudDetector.send_event(
            eventId        = '802454d3-f7d8-482d-97e8-c4b6db9a0428',
            eventTypeName  = 'sample_registration',
            eventTimestamp = '2020-07-13T23:18:21Z',
            eventVariables =  {
       'email_address' : 'johndoe@exampledomain.com',
       'ip_address' : '1.2.3.4'},
            assignedLabel  = 'legit',
            labelTimestamp = '2020-07-13T23:18:21Z',
            entities       = [{'entityType':'sample_customer', 'entityId':'12345'}],

)
```

取得已儲存事件資料的詳細資訊

在 Amazon Fraud Detector 中存放事件資料後，您可以使用 GetEventAPI 檢查針對事件存放的最新資料。下列範例程式碼會檢查針對`sample_registration`事件儲存的最新資料。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.get_event(
            eventId        = '802454d3-f7d8-482d-97e8-c4b6db9a0428',
            eventTypeName  = 'sample_registration'
)
```

檢視已儲存事件資料集的量度

對於每個事件類型，您可以在 Amazon Fraud Detector 主控台中檢視指標，例如存放的事件數量、存放的事件總大小，以及最早和最新存放事件的時間戳記。

若要檢視某個事件類型的已儲存事件指標，

1. 開啟主AWS控台並登入您的帳戶。導航至 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇事件。

3. 選擇事件類型。
4. 選擇存儲的事件選項卡。
5. [儲存的事件] 詳細資料窗格會顯示量度。這些指標每天會自動更新一次。
6. 選擇性地按一下「重新整理事件量度」，以手動更新

> **Note**
>
> 如果您剛匯入資料，建議您在匯入資料完成後等待 5-10 分鐘，以重新整理和檢視指標。

活動編排

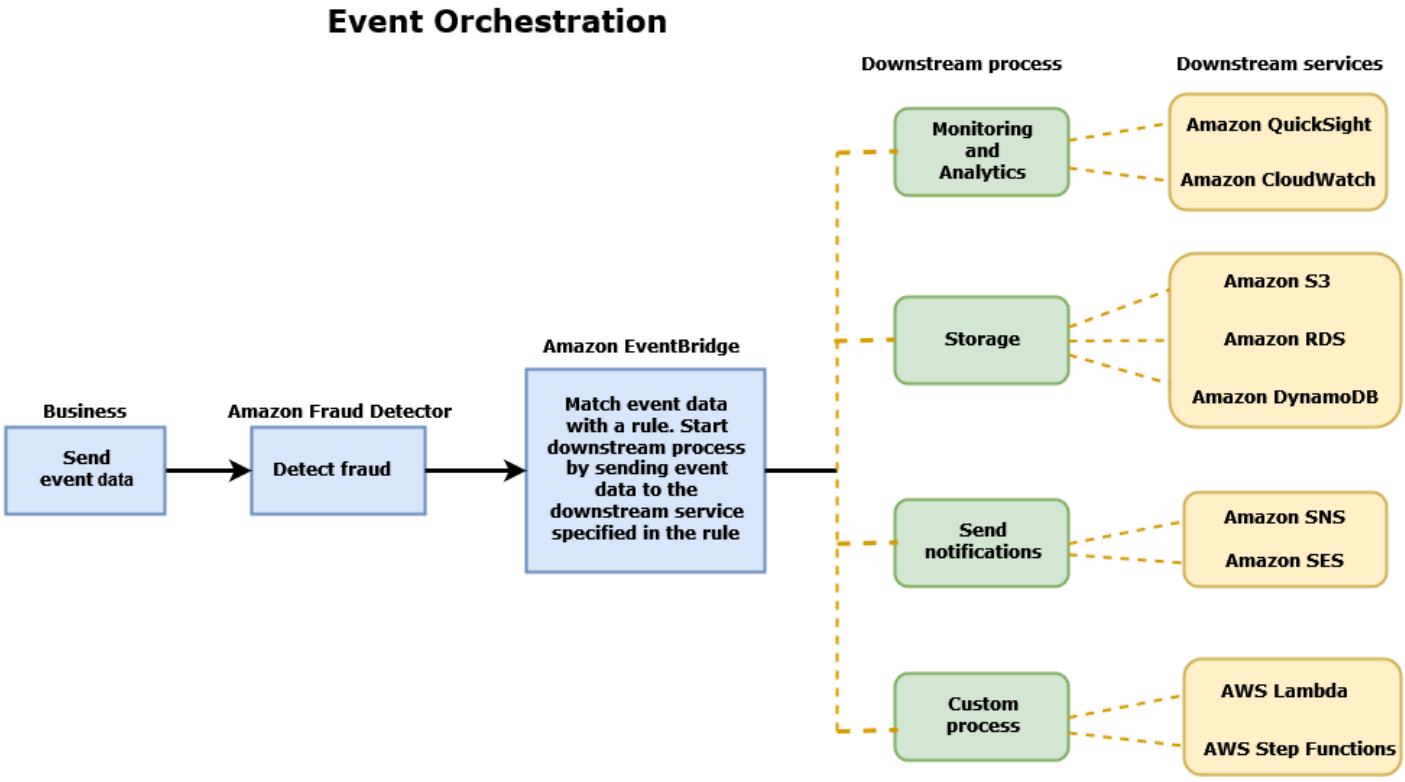
事件協調可讓您使用 Amazon EventBridge 輕鬆將事件傳送至AWS 服務下游處理。Amazon Fraud Detector 提供簡單的規則，可讓您在偵測到詐騙後自動處理事件。透過事件協調流程，您可以自動化下游事件流程，例如，將事件傳送至儀表板以從事件資料取得見解、根據詐騙偵測結果產生通知，以及根據詐騙偵測所學到的資訊，使用標籤更新事件。

事件編排可讓您透過 Amazon EventBridge 輕鬆存取AWS環境中的服務。您可以 EventBridge 將 Amazon 設定為使用 API 目的地直接AWS 服務或間接傳送事件。AWS 服務您用來協調下游流程的也稱為目標。您可以用來協調下游處理的一些目標如下：

- 用於監控和分析-Amazon QuickSight，Amazon CloudWatch
- 適用於儲存 — Amazon S3、Amazon RDS、亞馬遜動態
- 用於發送通知 — Amazon SNS，Amazon SES
- 對於自訂處理 — AWS Lambda、AWS Step Functions

如需 Amazon 支援的協調流程目標的詳細資訊 EventBridge，請參閱 Amazon EventBridge 目標。

下圖提供事件協調流程運作方式的高階檢視。



設定事件協調

為事件設定事件協調流程需要在目標服務中設定程序、設定 Amazon 以 EventBridge 接收和傳送事件資料，以及在 Amazon 中建立規則 EventBridge 以指定啟動下游程序的條件。完成下列步驟以設定事件協調流程：

若要設定事件協調

1. 轉到 Amazon 用 EventBridge 戶指南並了解如何使用 Amazon EventBridge。請務必學習如何在 Amazon 中 EventBridge 為您的使用案例建立規則。
2. 按照說明進行操作在 Amazon Fraud Detector 中啟用事件協調。

> **Note**
>
> 依預設，會停用事件的事件協調流程。

3. 設定目標服務以接收和處理事件資料。例如，如果您的下游程序涉及傳送通知，而您想要使用 Amazon SNS，請前往 Amazon SNS 主控台，建立 SNS 主題，然後訂閱該主題的端點。
4. 按照說明創建 Amazon EventBridge 規則。

> **Important**
>
> 在 Amazon 中構建事件模式時 EventBridge，請確保提`aws.frauddetector`供源字段和`Event Prediction Result Returned`詳細信息類型字段。

在 Amazon Fraud Detector 中啟用事件協調

您可以在建立事件類型時或在建立事件類型之後啟用事件協調作業。您可以在 Amazon Fraud Detector 主控台中啟用事件協調、使用`put-event-type`命令、`PutEventType` API 或使用AWS SDK for Python (Boto3).

在 Amazon Fraud Detector 主控台中啟用事件協調

此範例會針對已建立的事件類型啟用事件協調作業。如果您要建立新的事件類型並想要啟用協調流程，請依照指示執行建立事件類型。

啟用事件協調

1. 開啟AWS管理主控台並登入您的帳戶。導航到 Amazon Fraud Detector。
2. 在左側導覽窗格中，選擇 [事件]。
3. 在「事件類型」頁面中，選擇您的事件類型。
4. 開啟使用 Amazon EventBridge 啟用事件協調流程。
5. 繼續執行的步驟 3 指示設定事件協調。

使用啟用事件協調 AWS SDK for Python (Boto3)

下列範例顯示更新事件類型`sample_registration`以啟用事件協調流程的範例要求。此範例使用 `PutEventType` API，並假設您已建立變數`ip_address`、`email_address`、標籤`legit`和`fraud`和實體類型`sample_customer`。如需如何建立這些資源的詳細資訊，請參閱資源。

```
import boto3
fraudDetector = boto3.client('frauddetector')
fraud_detector.put_event_type(
  name = 'sample_registration',
  eventVariables = ['ip_address', 'email_address'],
  eventOrchestration = {'eventBridgeEnabled': True},
  labels = ['legit', 'fraud'],
  entityTypes = ['sample_customer'])
```

停用 Amazon Fraud Detector 中的事件協調

您可以隨時在 Amazon Fraud Detector 主控台中停用事件的事件協調流程、使用`put-event-type`命令、`PutEventType` API 或使用AWS SDK for Python (Boto3).

在 Amazon Fraud Detector 主控台中停用事件協調

若要停用事件協調

1. 開啟AWS管理主控台並登入您的帳戶。導航到 Amazon Fraud Detector。
2. 在左側導覽窗格中，選擇 [事件]。
3. 在「事件類型」頁面中，選擇您的事件類型。
4. 關閉使用 Amazon EventBridge 啟用事件協調流程。

使用停用事件協調流程 AWS SDK for Python (Boto3)

下列範例顯示更新事件類型以使用 PutEventType API 停sample_registration用事件協調流程的範例要求。

```
import boto3
fraudDetector = boto3.client('frauddetector')
fraud_detector.put_event_type(
  name = 'sample_registration',
  eventVariables = ['ip_address', 'email_address'],
  eventOrchestration = {'eventBridgeEnabled': False},
  entityTypes = ['sample_customer'])
```

模型

Amazon Fraud Detector 使用機器學習模型來產生詐騙預測。每個模型都使用模型類型進行訓練。模型類型指定用於訓練模型的演算法和轉換。模型訓練是使用您提供的資料集來建立可預測詐騙事件的模型的程序。

若要建立模型，您必須先選擇模型類型，然後準備並提供用於訓練模型的資料。

選擇型號類型

Amazon Fraud Detector 提供以下型號類型。選擇適合您使用案例的模型類型。

- 網上詐騙洞察

  「線上詐騙見解」模型類型經過最佳化，可在有關評估實體的歷史資料很少時偵測詐騙，例如線上註冊新帳戶的新客戶。

- 交易詐騙洞察

  「交易詐騙洞見」模型類型最適合偵測詐騙使用案例，其中正在評估的實體可能具有互動歷史記錄，該模型可以分析以提高預測準確性（例如，具有過去購買歷史記錄的現有客戶）。

- 帳戶接管洞察

  帳戶接管見解模型類型會偵測帳戶是否遭到網路釣魚或其他類型的攻擊入侵。遭入侵帳戶的登入資料 (例如登入時使用的瀏覽器和裝置) 與帳戶相關聯的歷史登入資料不同。

網上詐騙洞察

線上詐騙洞見是一種受監管的機器學習模型，這表示它使用詐騙和合法交易的歷史範例來訓練模型。在線欺詐洞察模型可以根據很少的歷史數據檢測欺詐。該模型的輸入非常靈活，因此您可以對其進行調整以檢測各種欺詐風險，包括虛假評論，促銷濫用和訪客結帳欺詐。

線上詐騙洞察模型使用一系列機器學習演算法來進行資料豐富、轉型和詐騙分類。作為模型訓練程序的一部分，「線上詐騙洞察」會透過第三方資料 (例如 IP 位址的地理位置或信用卡的發卡銀行) 來豐富原始資料元素，例如 IP 位址和 BIN 號碼。除了第三方資料之外，線上詐騙洞見還使用深度學習演算法來考量 Amazon 和AWS. 這些詐騙模式會使用漸層樹增強演算法，成為模型的輸入特徵。

為了提高性能，在線欺詐洞察通過貝葉斯優化過程優化梯度樹增強算法的超參數。它依序訓練具有不同模型參數的數十種不同模型（例如樹木數量，樹木的深度和每片葉子的樣本數量）。它還使用不同的優化策略，例如增加少數欺詐人群的權重，以照顧非常低的欺詐率。

選取資料來源

訓練線上詐騙洞見模型時，您可以選擇針對存放在外部 (Amazon Fraud Detector 外部) 或存放在 Amazon Fraud Detector 中的事件資料來訓練模型。Amazon Fraud Detector 目前支持的外部存儲是 Amazon Simple Storage Service (Amazon S3)。如果您使用外部儲存，您的事件資料集必須以逗號分隔值 (CSV) 格式上傳到 Amazon S3 儲存貯體。這些資料儲存選項在模型訓練組態中稱為 EXTERNAL_EVENTS (用於外部儲存裝置) 和 INGESTED_EVENTS (用於內部儲存裝置)。如需有關可用資料來源以及如何在其中儲存資料的詳細資訊，請參閱事件資料儲存體。

準備資料

無論您選擇將事件資料存放在何處 (Amazon S3 或 Amazon Fraud Detector)，線上詐騙洞見模型類型的要求都相同。

您的資料集必須包含資料欄標題 EVENT_LABEL。此變數會將事件分類為詐騙或合法事件。使用 CSV 檔案 (外部儲存) 時，您必須在檔案中包含每個事件的 EVENT_LABEL。對於內部存儲，EVENT_LABEL 字段是可選的，但所有事件都必須標記才能包含在訓練數據集中。設定模型訓練時，您可以選擇是否要忽略未標籤的事件、為未標籤的事件採用合法標籤，或為所有未標籤的事件採用欺詐性標籤。

選取資料

請參閱收集事件資料，瞭解如何選擇資料以訓練您的線上詐騙見解模型。

線上詐騙洞察訓練會根據 EVENT_TIMESTAMP 來進行範例和分割歷史資料。無需手動取樣資料，這樣做可能會對模型結果產生負面影響。

事件變數

除了必要的事件中繼資料外，線上詐騙洞見模型至少需要兩個變數，這些變數已通過模型訓練的資料驗證，並允許每個模型最多允許 100 個變數。一般而言，您提供的變數越多，模型就越能區分詐騙和合法事件。雖然線上詐騙見解模型可支援數十個變數 (包括自訂變數)，但我們建議您加入 IP 位址和電子郵件地址，因為這些變數通常最有效地識別要評估的實體。

驗證資料

在訓練過程中，線上詐騙洞見將驗證資料集是否存在可能影響模型訓練的資料品質問題。驗證資料後，Amazon Fraud Detector 將採取適當的行動來建立最佳的模型。這包括針對潛在的資料品質問題發出警告、自動移除有資料品質問題的變數，或者發出錯誤並停止模型訓練程序。如需詳細資訊，請參閱資料集驗證。

交易詐騙洞察

「交易詐騙見解」模型類型旨在偵測線上或 card-not-present交易詐騙。交易詐騙洞見是一種受監管的機器學習模型，這表示它使用詐騙和合法交易的歷史範例來訓練模型。

交易詐騙見解模型使用一系列機器學習演算法來進行資料豐富、轉換和詐騙分類。它利用功能工程引擎來建立實體層級和事件層級彙總。作為模型訓練程序的一部分，「交易詐騙洞察」會使用第三方資料 (例如 IP 位址的地理位置或信用卡的發卡銀行) 來豐富原始資料元素 (例如 IP 位址和 BIN 號碼)。除了第三方資料之外，交易詐騙洞見還使用深度學習演算法，這些演算法會考慮 Amazon 上看到的詐騙模式，而AWS這些詐騙模式會使用漸層樹增強演算法成為您模型的輸入功能。

為了提高性能，交易欺詐洞察通過貝葉斯優化過程優化梯度樹增強算法的超參數，依次培訓具有不同模型參數的數十種不同模型（例如樹的數量，樹的深度，每葉的樣本數量）以及不同的優化策略（例如增加少數族群欺詐人群）以照顧非常低的欺詐率。

作為模型訓練程序的一部分，交易詐騙模型的功能工程引擎會計算訓練資料集中每個唯一實體的值，以協助改善詐騙預測。例如，在訓練過程中，Amazon Fraud Detector 會計算並儲存實體上次購買的時間，並在您每次呼叫`GetEventPrediction`或 `SendEvent` API 時動態更新此值。在詐騙預測期間，事件變數會與其他實體和事件中繼資料結合，以預測交易是否為詐騙行為。

選取資料來源

交易詐騙洞見模型僅針對使用 Amazon Fraud Detector (INGESTED_EVENTS) 內部儲存的資料集進行訓練。這可讓 Amazon Fraud Detector 持續更新您正在評估之實體的計算值。如需有關可用資料來源的詳細資訊，請參閱 事件資料儲存體

準備資料

在訓練交易詐騙洞見模型之前，請確定您的資料檔案包含準備事件資料集中所述的所有標頭。「交易詐騙洞見」模型會將收到的新實體與資料集中詐騙和合法實體的範例進行比較，因此為每個實體提供許多範例會很有幫助。

Amazon Fraud Detector 會自動將儲存的事件資料集轉換成正確的訓練格式。模型完成訓練後，您可以檢閱效能指標，並決定是否應將實體新增至訓練資料集。

選取資料

根據預設，交易詐騙洞見會針對您選取的事件類型，根據您的整個儲存資料集進行訓練。您可以選擇性地設定時間範圍，以減少用於訓練模型的事件。設定時間範圍時，請確保用於訓練模型的記錄有足夠的時間來成熟。也就是說，已經過了足夠的時間來確保正確識別合法和欺詐記錄。例如，對於退款欺詐，通常需要 60 天或更長時間才能正確識別欺詐事件。為了獲得最佳模型效能，請確定訓練資料集中的所有記錄都已成熟。

無需選擇代表理想欺詐率的時間範圍。Amazon Fraud Detector 會自動取樣您的資料，以在詐騙率、時間範圍和實體計數之間取得平衡。

如果您選取的時間範圍沒有足夠的事件無法成功訓練模型，Amazon Fraud Detector 會在模型訓練期間傳回驗證錯誤。對於儲存的資料集，EVENT_LABEL 欄位是選擇性的，但事件必須標記才能包含在訓練資料集中。設定模型訓練時，您可以選擇是否要忽略未標籤的事件、假設未標籤事件採用合法標籤，還是假設未標記事件的欺詐性標籤。

事件變數

用於訓練模型的事件類型必須包含至少 2 個變數，除了必要的事件中繼資料之外，這些變數已通過資料驗證且最多可包含 100 個變數。一般而言，您提供的變數越多，模型就越能區分詐騙和合法事件。雖然交易詐騙洞察模型可支援數十個變數，包括自訂變數，但我們建議您包括 IP 位址、電子郵件地址、付款工具類型、訂單價格和信用卡 BIN。

驗證資料

在訓練過程中，交易詐騙洞見會驗證訓練資料集，找出可能影響模型訓練的資料品質問題。驗證資料後，Amazon Fraud Detector 會採取適當的動作來建立最佳的模型。這包括針對潛在的資料品質問題發出警告、自動移除有資料品質問題的變數，或者發出錯誤並停止模型訓練程序。如需詳細資訊，請參閱資料集驗證。

如果唯一實體數量少於 1,500 個，Amazon Fraud Detector 將發出警告，但會繼續訓練模型，因為這會影響訓練資料的品質。如果您收到警告，請複查效能測量結果。

帳戶接管洞察

帳戶接管洞察 (ATI) 模型類型會偵測帳戶是否因惡意接管、網路釣魚或憑證遭竊而遭到入侵，藉此識別詐騙線上活動。帳戶接管見解是一種機器學習模型，它使用來自線上業務的登入事件來訓練模型。

您可以在即時登入流程中內嵌訓練有素的「帳戶接管見解」模型，以偵測帳戶是否遭到入侵。該模型評估了各種身份驗證和登錄類型。其中包括 Web 應用程式登入、API 型驗證和 (SSO)。 single-sign-on

若要使用帳戶接管見解模型，請在出現有效的登入認證後呼叫 GetEventPredictionAPI。API 會產生一個分數，以量化帳戶遭到入侵的風險。Amazon Fraud Detector 會使用您定義的分數和規則，為登入事件傳回一或多個結果。結果是您設定的結果。根據您收到的結果，您可以針對每次登入採取適當的動作。也就是說，您可以批准或挑戰為登錄提供的憑據。例如，您可以通過要求提供帳戶 PIN 作為其他驗證來挑戰憑據。

您也可以使用帳戶接管見解模型以非同步方式評估帳戶登入，並對高風險帳戶採取動作。例如，可將高風險帳戶新增至調查佇列，供人工審核者使用，以判斷是否需要採取進一步的動作，例如暫停帳號。

帳戶接管見解模型是使用包含您企業歷史登入事件的資料集進行訓練。您提供此資料。您可以選擇將帳戶標記為合法或欺詐性帳戶。但是，訓練模型並不需要這樣做。帳戶接管見解模型會根據成功登入帳戶的歷史記錄來偵測異常情況。它也會學習如何偵測使用者行為中的異常情況，進而增加惡意帳戶接管事件的風險。例如，通常從同一組裝置和 IP 位址登入的使用者。欺詐者通常從不同的設備和地理位置登錄。此技術會產生異常活動的風險評分，這通常是惡意帳戶接管的主要特徵。

在訓練帳戶接管洞察模型之前，Amazon Fraud Detector 使用機器學習技術的組合來執行資料豐富、資料彙總和資料轉換。然後，在訓練過程中，Amazon Fraud Detector 會豐富您提供的原始資料元素。原始資料元素的範例包括 IP 位址和使用者代理程式。Amazon Fraud Detector 使用這些元素來建立描述登入資料的其他輸入。這些輸入包括裝置、瀏覽器和地理位置輸入。Amazon Fraud Detector 也會使用您提供的登入資料，持續運算描述過去使用者行為的彙總變數。使用者行為的範例包括使用者從特定 IP 位址登入的次數。使用這些額外的擴充和彙總，Amazon Fraud Detector 可以從您的登入事件中的一小組輸入產生強大的模型效能。

「帳戶接管見解」模型會偵測不良行為者存取合法帳戶的執行個體，無論不良行為者是人類還是機器人。此模型會產生單一分數，指出帳戶遭到入侵的相對風險。可能已遭入侵的帳戶會標示為高風險帳戶。您可以通過以下兩種方式之一處理高風險帳戶。或者，您可以強制執行其他身份驗證。或者，您可以將帳號傳送至佇列以進行手動調查。

選取資料來源

帳戶接管洞察模型是根據內部儲存在 Amazon Fraud Detector 中的資料集進行訓練。若要使用 Amazon Fraud Detector 儲存您的登入事件資料，請建立包含使用者登入事件的 CSV 檔案。針對每個事件，包括登入資料，例如事件時間戳記、使用者 ID、IP 位址、使用者代理程式，以及登入資料是否有效。建立 CSV 檔案後，請先將檔案上傳到 Amazon Fraud Detector，然後使用匯入功能來存放資料。然後，您可以使用儲存的資料來訓練模型。如需使用 Amazon Fraud Detector 儲存事件資料集的詳細資訊，請參閱 使用 Amazon Fraud Detector 在內部存放您的事件資料

準備資料

Amazon Fraud Detector 要求您以逗號分隔值 (CSV) 檔案 (以 UTF-8 格式編碼) 提供使用者帳戶登入資料。CSV 檔案的第一行必須包含檔案標頭。文件頭由描述每個數據元素的事件元數據和事件變量組成。事件數據跟隨標題。事件資料中的每一行都包含來自單一登入事件的資料。

對於帳戶接管見解模型，您必須在 CSV 檔案的標題行中提供下列事件中繼資料和事件變數。

事件元數據

建議您在 CSV 檔案標頭中提供下列中繼資料。事件中繼資料必須是大寫字母。

- EVENT_ID-登入事件的唯一識別碼。
- ENTITY_TYPE-執行登入事件的實體，例如商家或客戶。
- ENTITY_ID-執行登入事件之實體的識別碼。
- 事件時間戳記-發生登錄事件時的時間戳。時間戳記必須採用 ISO 8601 標準 (世界標準時間)。
- EVENT_LABEL（建議使用）-將事件分類為欺詐或合法的標籤。您可以使用任何標籤，例如「欺詐」，「合法」，「1」或「0」。

> **Note**
>
> - 事件中繼資料必須是大寫字母。它是區分大小寫的。
> - 登入事件不需要標籤。不過，我們建議您加入 EVENT_LABEL 中繼資料，並為您的登入事件提供標籤。如果標籤不完整或零星，這很好。如果您提供標籤，Amazon Fraud Detector 會使用這些標籤來自動計算帳戶接管探索率，並將其顯示在模型效能圖表和表格中。

事件變數

對於帳戶接管見解模型，您必須提供必要 (強制) 變數和選用變數。建立變數時，請務必將變數指派給正確的變數類型。做為模型訓練程序的一部分，Amazon Fraud Detector 會使用與變數相關聯的變數類型來執行變數擴充和功能工程。

> **Note**
>
> 事件變數名稱必須是小寫字母。它們是區分大小寫的。

強制性變數

訓練「帳戶接管見解」模型時，需要下列變數。

類別	變數類型	描述
IP 地址	IP_ADDRESS	登入事件中使用的 IP 位址
瀏覽器和設備	用戶代理	登入事件中使用的瀏覽器、裝置和作業系統
有效的憑證	有效	指出用於登入的認證是否有效

選擇性變數

下列變數是用於訓練「帳戶接管見解」模型的選用變數。

類別	Type	描述
瀏覽器和設備	指紋	瀏覽器或裝置指紋的唯一識別碼
階段作業 ID	SESSION_ID	驗證工作階段的識別碼
標籤	事件標籤	將事件歸類為詐騙或合法的標籤。您可以使用任何標籤，例如「欺詐」，「合法」，「1」或「0」。
時間戳記	標籤時間戳記	上次更新標籤時的時間戳記。如果提供了事件 _ 標籤，這是必需的。

Note

- 您可以為這兩個強制性變量可選變量提供任何變量名稱。重要的是，每個強制性和可選變量分配給正確的變量類型。

- 您可以提供其他變數。但是，Amazon Fraud Detector 不會包含這些變數來訓練帳戶接管洞察模型。

選取資料

收集資料是建立帳戶接管見解模型的重要步驟。開始收集登入資料時，請考慮下列需求和建議：

必要

- 提供至少 1,500 個使用者帳戶範例，每個範例至少有兩個相關的登入事件。
- 您的資料集必須涵蓋至少 30 天的登入事件。您稍後可以指定用於訓練模型的事件的特定時間範圍。

建議

- 您的資料集包含不成功的登入事件範例。您可以選擇將這些失敗的登入標籤為「詐騙」或「合法」。
- 使用超過六個月的登入事件準備歷史資料，並包含 10 萬個實體。

如果您沒有符合最低需求的資料集，請考慮透過呼叫 SendEventAPI 操作將事件資料串流至 Amazon Fraud Detector。

驗證資料

在建立帳戶接管洞察模型之前，Amazon Fraud Detector 會檢查您在資料集中用於訓練模型的中繼資料和變數是否符合大小和格式要求。如需詳細資訊，請參閱資料集驗證。它還檢查其他要求。如果資料集未通過驗證，則不會建立模型。為了成功創建模型，請確保在再次訓練之前修復未通過驗證的數據。

常見資料集錯誤

在驗證資料集以訓練帳戶接管洞察模型時，Amazon Fraud Detector 會掃描這些問題和其他問題，並在遇到一或多個問題時擲回錯誤。

- CSV 檔案不是使用 UTF-8 格式的檔案。
- CSV 檔案標頭不包含下列至少一個中繼資料：EVENT_IDENTITY_ID、或EVENT_TIMESTAMP。
- CSV 檔案標頭不包含下列變數類型的至少一個變數：IP_ADDRESSUSERAGENT、或VALIDCRED。
- 有一個以上的變量是與相同的變量類型相關聯。
- 中超過 0.1% 的值EVENT_TIMESTAMP包含空值或受支援的日期和時間戳記格式以外的值。

- 第一個事件和最後一個事件之間的天數少於 30 天。
- 變數類型的IP_ADDRESS變數有 10% 以上為無效或空值。
- 超過 50% 的變量類型的USERAGENT變量包含空值。
- 變數類型的所有VALIDCRED變數都設定為false。

建立模型

Amazon Fraud Detector 模型可學習偵測特定事件類型的詐騙行為。在 Amazon Fraud Detector 中，您首先建立模型，該模型可做為模型版本的容器。每次訓練模型時，都會建立新版本。如需如何使用AWS主控台建立和訓練模型的詳細資訊，請參閱步驟 3：建立模型。

每個模型都有對應的模型分數變數。Amazon Fraud Detector 會在您建立模型時代表您建立此變數。您可以在規則運算式中使用此變數，在詐騙評估期間解譯您的模型分數。

使用訓練和部署模型 AWS SDK for Python (Boto3)

透過呼叫CreateModel和CreateModelVersion作業建立模型版本。 CreateModel啟動模型，該模型充當模型版本的容器。 CreateModelVersion會啟動訓練程序，這會產生特定版本的模型。每次呼叫 CreateModelVersion 都會建立新的解決方案版本。

下列範例顯示 CreateModel API 的範例要求。此範例會建立「線上詐騙洞察」模型類型，並假設您已建立事件類型sample_registration。如需有關建立事件類型的其他詳細資訊，請參閱建立事件類型。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_model (
modelId = 'sample_fraud_detection_model',
eventTypeName = 'sample_registration',
modelType = 'ONLINE_FRAUD_INSIGHTS')
```

使用 CreateModelVersionAPI 訓練您的第一個版本。針對TrainingDataSource並ExternalEventsDetail指定訓練資料集的來源和 Amazon S3 位置。對於TrainingDataSchema指定 Amazon Fraud Detector 應如何解譯訓練資料，特別是要包含哪些事件變數，以及如何對事件標籤進行分類。根據預設，Amazon Fraud Detector 會忽略未標籤的事件。此範例程式碼用AUTO於指unlabeledEventsTreatment定 Amazon Fraud Detector 決定如何使用未標籤的事件。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_model_version (
modelId = 'sample_fraud_detection_model',
modelType = 'ONLINE_FRAUD_INSIGHTS',
trainingDataSource = 'EXTERNAL_EVENTS',
trainingDataSchema = {
    'modelVariables' : ['ip_address', 'email_address'],
    'labelSchema' : {
        'labelMapper' : {
            'FRAUD' : ['fraud'],
            'LEGIT' : ['legit']
        }
       unlabeledEventsTreatment = 'AUTO'
    }
},
externalEventsDetail = {
    'dataLocation' : 's3://bucket/file.csv',
    'dataAccessRoleArn' : 'role_arn'
}
)
```

成功的請求將導致具有狀態的新模型版本TRAINING_IN_PROGRESS。在訓練期間的任何時候，您都可以透過呼叫UpdateModelVersionStatus並將狀態更新為來取消訓練TRAINING_CANCELLED。訓練完成後，模型版本狀態將更新為TRAINING_COMPLETE。您可以使用 Amazon Fraud Detector 主控台或撥打電話來檢閱模型效能DescribeModelVersions。如需如何解譯模型分數和效能的詳細資訊，請參閱模型分數和模型效能指標。

檢閱模型效能後，啟動模型，讓偵測器可用於即時詐騙預測。Amazon Fraud Detector 會在多個可用區域中部署模型，以便在開啟 auto-scaling 的情況下進行備援，以確保模型隨著您進行的詐騙預測數量進行擴展。若要啟用模型，請呼叫 UpdateModelVersionStatus API 並將狀態更新為ACTIVE。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.update_model_version_status (
modelId = 'sample_fraud_detection_model',
modelType = 'ONLINE_FRAUD_INSIGHTS',
modelVersionNumber = '1.00',
status = 'ACTIVE'
```

)

模型分數

Amazon Fraud Detector 針對不同的模型類型產生不同的模型分數。

對於帳戶接管洞察 (ATI) 模型，Amazon Fraud Detector 僅使用彙總值 (結合一組原始變數計算的值) 來產生模型分數。新實體的第一個事件會產生 -1 的分數，表示風險不明。這是因為對於新實體而言，用於計算彙總的值將為零或 null。帳戶接管見解 (ATI) 模型會針對相同實體和現有實體的所有後續事件產生 0 到 1000 之間的模型分數，其中 0 表示詐騙風險低，1000 表示高詐騙風險。對於 ATI 模型，模型分數與挑戰率 (CR) 直接相關。例如，分數 500 對應於估計的 5% 挑戰率，而 900 分則對應於估計 0.1% 的挑戰率。

針對線上詐騙洞見 (OFI) 和交易詐騙洞見 (TFI) 模型，Amazon Fraud Detector 會同時使用彙總值 (結合一組原始變數計算的值) 和原始值 (為變數提供的值) 產生模型分數。模型分數可以介於 0 到 1000 之間，其中 0 表示低欺詐風險，1000 表示高欺詐風險。對於 OFI 和 TFI 模型，模型分數與誤判率（FPR）直接相關。例如，評分 600 對應於估計的 10% 誤判率，而 900 分則對應於估計的 2% 誤判率。下表提供特定模型分數與估計誤判率之間如何關聯的詳細資訊。

模型分數	估計人口普及性
975	0.50%
950	1%
900	2%
860	3%
775	5%
700	7%
600	10%

模型效能指標

模型訓練完成後，Amazon Fraud Detector 會使用未用於訓練模型的 15% 資料來驗證模型效能。您可以期待訓練有素的 Amazon Fraud Detector 模型具有與驗證效能指標類似的真實世界詐騙偵測效能。

作為一家企業，您必須在檢測更多欺詐行為和向合法客戶增加更多摩擦之間取得平衡。為了協助選擇適當的平衡，Amazon Fraud Detector 提供下列工具來評估模型效能：

- 分數分佈圖 — 模型評分分佈的直方圖假設範例人口為 100,000 個事件。左 Y 軸代表合法事件，右 Y 軸代表欺詐事件。您可以按一下圖表區域來選取特定的模型臨界值。這將更新混淆矩陣和 ROC 圖表中的對應視圖。
- 混淆矩陣 — 透過比較模型預測與實際結果來摘要指定評分臨界值的模型準確度。Amazon Fraud Detector 假設範例人口為 100,000 個事件。欺詐和合法事件的分佈模擬了您企業的欺詐率。
  - 真正的陽性 — 該模型預測欺詐行為，事件實際上是欺詐。
  - 誤報 — 該模型預測欺詐，但事件實際上是合法的。
  - 真正的負面因素 — 模型預測是合法的，事件實際上是合法的。
  - 假陰性 — 該模型預測是合法的，但事件實際上是欺詐。
  - 真正利率 (TPR) — 模型偵測到的總詐騙百分比。也稱為擷取速率。
  - 誤判率 (FPR) — 錯誤預測為詐騙的合法事件總數的百分比。
- 接收器運算子曲線 (ROC) — 將真正率繪製為所有可能模型評分閾值的誤判率函數。選擇進階測量結果來檢視此圖表。
- 曲線下方區域 (AUC) — 彙總所有可能的模型評分閾值的 TPR 和 FPR。沒有預測功率的模型 AUC 為 0.5，而完美模型的分數為 1.0。
- 不確定性範圍 — 它顯示了從模型預期的 AUC 範圍。較大的範圍（AUC 的上限和下限差異 > 0.1）意味著更高的模型不確定性。如果不確定性範圍很大 (>0.1)，請考慮提供更多標籤的事件並重新訓練模型。

使用模型效能測量結果

1. 從分數分佈圖開始，查看您的欺詐和合法事件的模型分數分佈。理想情況下，您將在欺詐和合法事件之間有明確的分離。這表示模型可以準確識別哪些事件是欺詐性的，哪些是合法的。按一下圖表區域以選取模型臨界值。您可以看到調整模型評分閾值如何影響您的真正和誤判率。

   > **Note**
   >
   > 分數分佈圖繪製兩個不同 Y 軸上的欺詐和合法事件。左 Y 軸代表合法事件，右 Y 軸代表欺詐事件。

2. 檢閱混淆矩陣。根據您選取的模型評分閾值，您可以根據 100,000 個事件的樣本查看模擬影響。欺詐和合法事件的分佈模擬了您企業的欺詐率。使用此資訊找出真正率與誤判率之間的適當平衡。

3. 如需其他詳細資訊，請選擇進階量度。使用 ROC 圖表瞭解任何模型評分閾值的真正率與誤判率之間的關係。ROC 曲線可以幫助您微調真正率和誤判率之間的權衡。

> **Note**
>
> 您也可以選擇「表格」，以表格形式檢閱量度。
> 表格檢視也會顯示測量結果精確度。與預測為欺詐的所有事件相比，Precision 是正確預測為欺詐事件的百分比。

4. 使用效能指標，根據您的目標和詐騙偵測使用案例，決定企業的最佳模型閾值。例如，如果您計劃使用模型將新帳戶註冊分類為高、中或低風險，則需要識別兩個臨界值評分，以便草擬三個規則條件，如下所示：

   - 分數 > X 是高風險
   - 分數 < X but > Y 為中等風險
   - 分數 < Y 是低風險

模型變數重要性

模型變數重要性是 Amazon Fraud Detector 的一項功能，可在模型版本中對模型變數進行排名。每個模型變數都會根據其對模型整體效能的相對重要性來提供一個值。與該模型版本的資料集中的其他模型變數相比，具有最高值的模型變數對模型來說更為重要，預設會列在頂端。同樣地，預設情況下，具有最低值的模型變數會列在底部，而且與其他模型變數相比最不重要。使用模型變數重要性值，您可以深入瞭解哪些輸入會驅動模型效能。

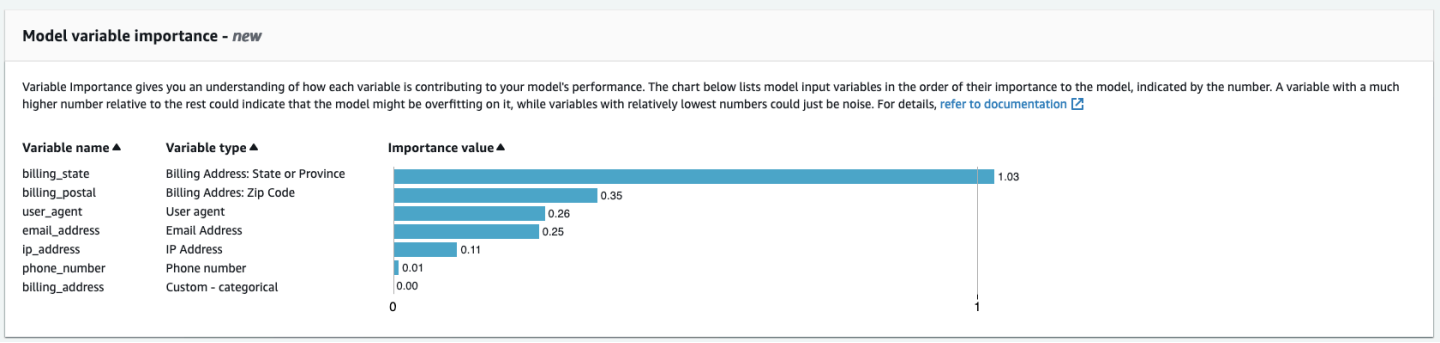
您可以在 Amazon Fraud Detector 主控台或使用 DescribeModelVersionAPI，檢視訓練模型版本的模型變數重要性值。

模型變數重要性為用於訓練模型版本的每個變數提供下列一組值。

- 變數類型：變數類型 (例如 IP 位址或電子郵件)。如需詳細資訊，請參閱變數類型。對於帳戶接管洞察 (ATI) 模型，Amazon Fraud Detector 為原始和彙總變數類型提供可變重要性值。原始變數類型會指派給您提供的變數。彙總變數類型會指派給 Amazon Fraud Detector 結合以計算彙總重要性值的一組原始變數。
- 變數名稱：用來訓練模型版本的事件變數名稱 (例如`ip_address`、`email_address`、`are_creadentials_valid`)。如果是彙總變數類型，則會列出用來計算彙總變數重要性值的所有變數名稱。

- 變數重要性值：代表原始或彙總變數對模型效能的相對重要性的數字。典型範圍：0 到 10

在 Amazon Fraud Detector 主控台中，線上詐騙洞見 (OFI) 或交易詐騙洞見 (TFI) 模型的模型變數重要性值顯示如下。帳戶接管洞察 (ATI) 模型除了原始變數的重要性值之外，還會提供彙總變數重要性值。視覺化圖表可讓您輕鬆查看變數之間的相對重要性，並使用垂直虛線來參考排名最高變數的重要性。



Amazon Fraud Detector 會為每個 Fraud Detector 模型版本產生可變重要性值，無需額外費用。

> **Important**
>
> 在 2021 年 7 月 9 日之前建立的模型版本沒有變數重要性值。您必須訓練模型的新版本，以產生模型變數重要性值。

使用模型變數重要性值

您可以使用模型變數重要性值，深入瞭解模型的提升或下降效能，以及哪些變數的貢獻最大。然後調整您的模型以提高整體性能。

更具體地說，為了提高模型效能，請根據您的領域知識檢查變數重要性值，並對訓練資料中的問題進行除錯。例如，如果帳戶 ID 被用作模型的輸入，並且它列在頂部，請查看其變量重要性值。如果變數重要性值明顯高於其餘值，則您的模型可能會過度擬合特定詐騙模式 (例如，所有詐騙事件都來自相同的帳戶 ID)。但是，如果變量取決於欺詐標籤，則也可能出現標籤洩漏的情況。根據您的領域知識分析的結果，您可能想要刪除變量並使用更多樣化的數據集進行訓練，或保持模型原樣。

同樣，看看最後排名的變量。如果變數重要性值明顯低於其餘值，則此模型變數在訓練模型時可能沒有任何重要性。您可以考慮刪除變量來訓練更簡單的模型版本。如果您的模型有很少的變數 (例如只有兩個變數)，Amazon Fraud Detector 仍會提供變數重要性值並對變數進行排序。但是，在這種情況下，見解將受到限制。

Important

1. 如果您發現 Model 變數重要性圖表中遺失了變數，可能是下列其中一個原因所造成的。請考慮修改資料集中的變數，然後重新訓練模型。
   - 訓練資料集中變數的唯一值計數低於 100。
   - 訓練資料集遺失大於 0.9 的變數值。
2. 每次要調整模型的輸入變數時，都需要訓練新的模型版本。

評估模型變數重要性值

我們建議您在評估模型變數重要性值時考慮下列事項：

- 變數重要性值必須始終與領域知識結合進行評估。
- 檢查變數的變數重要性值，相對於模型版本中其他變數的變數重要性值。請勿獨立考慮單一變數的變數重要性值。
- 比較相同模型版本內變數的變數重要性值。請勿在模型版本中比較相同變數的變數重要性值，因為模型版本中變數的變數重要性值可能與不同模型版本中相同變數的值不同。如果您使用相同的變數和資料集來訓練不同的模型版本，這不一定會產生相同的變數重要性值。

檢視模型變數重要性等級

模型訓練完成後，您可以在 Amazon Fraud Detector 主控台或使用 DescribeModelVersionAPI 檢視訓練模型版本的模型變數重要性排名。

若要使用主控台檢視模型變數重要性排名，

1. 開啟主AWS控台並登入您的帳戶。導航到 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇 Models (模型)。
3. 選擇您的型號，然後選擇模型版本。
4. 確定已選取 [概觀] 索引標籤。
5. 向下捲動以檢視「模型」變數重要性窗格。

瞭解如何計算模型變數重要性值

完成每個模型版本訓練後，Amazon Fraud Detector 會自動產生模型變數重要性值和模型的效能指標。為此，Amazon Fraud Detector 使用沙普利添加劑解釋（SHAP）。在考慮了所有模型變量的所有可能組合之後，SHAP 基本上是模型變量的平均預期貢獻。

SHAP 首先為事件的預測分配每個模型變量的貢獻。然後，它彙總這些預測，以在模型層級建立變數的排名。為了分配預測的每個模型變量的貢獻，SHAP 考慮所有可能的變量組合之間的模型輸出差異。通過包括包含或刪除特定變量集以生成模型輸出的所有可能性，SHAP 可以準確地訪問每個模型變量的重要性。當模型變量彼此之間高度相關時，這一點尤其重要。

在大多數情況下，ML 模型不允許您移除變數。您可以改用一或多個基準線 (例如，非詐騙事件) 中的對應變數值來取代模型中移除或遺失的變數。選擇適當的基準執行個體可能很困難，但 Amazon Fraud Detector 會將此基準設定為您的平均人口，從而簡化這項工作。

匯入 SageMaker 模型

您可以選擇將 SageMaker託管模型匯入 Amazon Fraud Detector。與模型類似，可以將 SageMaker 模型新增至偵測器，並使用 `GetEventPrediction` API 產生詐騙預測。作為`GetEventPrediction`請求的一部分，Amazon Fraud Detector 會叫用您的 SageMaker 端點，並將結果傳遞給您的規則。

您可以將 Amazon Fraud Detector 設定為使用作為`GetEventPrediction`請求一部分傳送的事件變數。如果您選擇使用事件變數，則必須提供輸入範本。Amazon Fraud Detector 會使用此範本將您的事件變數轉換為所需的輸入承載，以呼叫 SageMaker 端點。或者，您可以將 SageMaker 模型配置為使用作為請求一部分發送的 ByteBuffer。`GetEventPrediction`

Amazon Fraud Detector 支援匯入使用 JSON 或 CSV 輸入格式以及 JSON 或 CSV 輸出格式的 SageMaker 演算法。支援的 SageMaker 演算法範例包括 XGBoost、線性學習器和隨機切割森林。

使用匯入 SageMaker 模型 AWS SDK for Python (Boto3)

若要匯入 SageMaker 模型，請使用 `PutExternalModel` API。下列範例假設 SageMaker 端點`sagemaker-transaction-model`已部署、為`InService`狀態，並使用 XGBoost 演算法。

輸入配置指定將使用事件變量來構造模型輸入（`useEventVariables`設置為`TRUE`）。輸入格式是文字 CSV，因為 XGBoost 需要一個 CSV 輸入。 csvInputTemplate 指定如何從作為`GetEventPrediction`要求一部分傳送的變數建構 CSV 輸入。此範例假設您已建立變數`order_amt`、`prev_amt`、`hist_amt`和`payment_type`。

輸出組態會指定 SageMaker 模型的回應格式，並將適當的 CSV 索引對應至 Amazon Fraud Detector 變數`sagemaker_output_score`。設定完成後，您可以在規則中使用輸出變數。

> **Note**
>
> 來自 SageMaker 模型的輸出必須映射到帶有源的變量`EXTERNAL_MODEL_SCORE`。您無法使用「變數」在主控台中建立這些變數。當您設定模型匯入時，您必須改為建立它們。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_external_model (
modelSource = 'SAGEMAKER',
modelEndpoint = 'sagemaker-transaction-model',
invokeModelEndpointRoleArn = 'your_SagemakerExecutionRole_arn',
inputConfiguration = {
    'useEventVariables' : True,
    'eventTypeName' : 'sample_transaction',
    'format' : 'TEXT_CSV',
    'csvInputTemplate' : '{{order_amt}}, {{prev_amt}}, {{hist_amt}}, {{payment_type}}'
},

outputConfiguration = {
    'format' : 'TEXT_CSV',
    'csvIndexToVariableMap' : {
        '0' : 'sagemaker_output_score'
    }
},

modelEndpointStatus = 'ASSOCIATED'
)
```

刪除模型或模型版本

您可以刪除 Amazon Fraud Detector 中的模型和模型版本，前提是其與偵測器版本沒有關聯。刪除模型時，Amazon Fraud Detector 會永久刪除該模型，且資料不會再儲存在 Amazon Fraud Detector 中。

如果 Amazon SageMaker Fraud Detector 沒有與偵測器版本關聯，您也可以將其移除。移除 SageMaker 模型會中斷其與 Amazon Fraud Detector 的連線，但該模型仍然可在中使用 SageMaker。

刪除模型版本

您只能刪除Ready to deploy狀態中的模型版本。若要將模型版本從變更ACTIVE為Ready to deploy狀態，請取消部署模型版本。

1. 登入，開啟位於 https://console.aws.amazon.com/frauddetector 的AWS Management Console Amazon Fraud Detector 主控台台台台台台台台台台
2. 在 Amazon Fraud Detector 主控台台台台台台台台台台台台台台台台台台台台台台台台
3. 選擇包含想要刪除之模型版本的模型型型型型型型型型型號。
4. 選擇想要刪除的模型版本。
5. 選擇 動作，然後選擇 刪除。
6. 輸入模型版本名稱，然後選擇 [刪除模型版本]。

若要取消部署模型版本

您無法取消部署任何偵測器版本 (ACTIVE、、INACTIVEDRAFT) 正在使用的模型版本。因此，若要取消部署偵測器版本正在使用的模型版本，請先從偵測器版本中移除模型版本。

1. 在 Amazon Fraud Detector 主控台台台台台台台台台台台台台台台台台台台台台台台台
2. 選擇包含您要取消部署之模型版本的模型。
3. 選擇想要刪除的模型版本。
4. 選擇 [動作]，然後選擇 [取消部署模型版本]。

刪除模型型型

刪除模型之前，您必須先刪除所有模型版本，其與模型版本關聯。

1. 在 Amazon Fraud Detector 主控台台台台台台台台台台台台台台台台台台台台台台台台
2. 選擇想要刪除的模型型型型型型型型型。
3. 選擇 動作，然後選擇 刪除。
4. 輸入模型名稱，然後選擇「刪除模型」。

要刪除亞馬遜 SageMaker 模型

1. 在 Amazon Fraud Detector 主控台台台台台台台台台台台台台台台台台台台台台台台台
2. 選擇想要移除的 SageMaker 模型型型型型型型號。

3. 選擇「動作」，然後選擇「移除模型」。
4. 輸入模型名稱，然後選擇「移除 SageMaker模型」。

偵測器

偵測器是一種容器，其中包含您要評估詐騙的特定商業事件的詐騙偵測邏輯，例如模型和規則。首先，您可以透過指定已定義的事件來建立偵測器，然後選擇性地新增由 Amazon 詐騙偵測器為該事件建立和訓練的模型版本。

然後，您可以將規則和規則執行順序新增至偵測器，以建立偵測器的版本。偵測器版本會定義規則，並選擇性地將作為產生詐騙預測請求的一部分執行的模型。您可以將偵測器內定義的任何規則新增至偵測器版本。您也可以將在評估的事件類型上訓練的任何模型添加到檢測器版本中。偵測器可以有多個版本，每個版本都有不同的規則和規則執行順序，以滿足多種使用案例。

每個偵測器版本的狀態必須為DRAFT,ACTIVE，或INACTIVE。只有一個檢測器版本可以在ACTIVE一次的狀態。亞馬遜欺詐檢測器使用檢測器版本ACTIVE狀態以產生欺詐預測。

建立偵測器

您可以透過指定已定義的事件類型來建立偵測器。您可以選擇性地新增已由 Amazon 詐騙偵測器訓練和部署的模型。如果您新增模型，則可以在建立規則時，在規則運算式中使用 Amazon 詐騙偵測器產生的模型分數 (例如，`$model score < 90`).

您可以在 Amazon 詐騙偵測器主控台中建立偵測器，使用PutDetector應用程式介面，使用放入檢測器指令，或使用AWSSDK。如果您使用 API，命令或 SDK 來創建檢測器，則在創建檢測器後，請按照說明進行操作建立偵測器版本。

在 Amazon 詐騙偵測器主控台中建立偵測器

此範例假設您已建立事件類型，並且已建立並部署要用於詐騙預測的模型版本。

步驟 1：構建檢測器

1. 在 Amazon 詐騙偵測器主控台的左側導覽窗格中，選擇探測器。
2. 選擇建立偵測器。
3. 在定義偵測器細節頁面上，輸入`sample_detector`用於檢測器名稱。選擇性地輸入偵測器的描述，例如`my sample fraud detector`。
4. 對於事件類型」下方，選取您為詐騙預測建立的事件類型。
5. 選擇 下一步。

步驟 2：新增部署的模型版本

1. 請注意，這是一個可選步驟。您不需要將模型添加到檢測器中。要略過此步驟，請選擇 Next (下一步)。
2. 在新增模型-選擇性，選擇新增模型。
3. 在新增模型頁面，用於選擇型號，選擇您之前部署的 Amazon 詐騙偵測器型號名稱。對於選擇版本，選擇已部署模型的模型版本。
4. 選擇 Add model (新增模型)。
5. 選擇 下一步。

步驟 3：新增規則

規則是告知 Amazon 詐騙偵測器在評估詐騙預測時如何解譯變數值的條件。此範例會使用模型分數作為變數值來建立三個規則：high_fraud_risk,medium_fraud_risk，以及low_fraud_risk。若要建立您自己的規則、規則運算式、規則執行順序和結果，請使用適合您模型和使用案例的值。

1. 在新增規則頁面，下方定義規則，輸入high_fraud_risk對於規則名稱和下描述-可選，輸入**This rule captures events with a high ML model score**作為規則的描述。
2. 在表達中，使用 Amazon 詐騙偵測器簡化的規則運算式語言輸入下列規則運算式：

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```
3. 在成果，選擇創建一個新的結果。結果是詐騙預測的結果，如果規則在評估期間符合，則會傳回結果。
4. 在創建一個新的結果，輸入verify_customer作為結果名稱。您可以選擇性地輸入描述。
5. 選擇儲存結果。
6. 選擇新增規則以執行規則驗證檢查程式並儲存規則。建立後，Amazon 詐騙偵測器會讓規則可用於您的偵測器。
7. 選擇新增其他規則，然後選擇建立規則標籤。
8. 重複此過程兩次以創建medium_fraud_risk和low_fraud_risk使用下列規則詳細資訊的規則：

   - 中等詐騙風險

     規則名稱：medium_fraud_risk

     成果：review

表示式：

```
$sample_fraud_detection_model_insightscore <= 900 and

$sample_fraud_detection_model_insightscore > 700
```

- 低欺詐風險

  規則名稱：`low_fraud_risk`

  成果：`approve`

  表示式：

  ```
  $sample_fraud_detection_model_insightscore <= 700
  ```

9. 為您的使用案例建立所有規則之後，請選擇下一步。

   如需建立和寫入規則的詳細資訊，請參閱規則和規則語言參考。

步驟 4：設定規則執行和規則順序

偵測器中包含之規則的規則執行模式會決定是否評估您定義的所有規則，或規則評估是否在第一個符合的規則停止。規則順序決定了您希望規則執行的順序。

預設規則執行模式為`FIRST_MATCHED`。

第一個匹配

第一個符合的規則執行模式會根據定義的規則順序傳回第一個相符規則的結果。若您指定 `FIRST_MATCHED`，Amazon Fraud Detector 會從頭到尾依序評估規則，並在遇到第一個相符規則後停止評估。然後，Amazon 詐騙偵測器會為該單一規則提供結果。

您執行規則的順序可能會影響產生的詐騙預測結果。建立規則之後，請依照下列步驟重新排序規則，以所需的順序執行規則：

如果您的`high_fraud_risk`規則不在規則清單的頂端，請選擇訂單，然後選擇1。這會移動`high_fraud_risk`到第一個位置。

重複此過程，以便`medium_fraud_risk`規則處於第二個位置，並且您的`low_fraud_risk`規則位於第三個位置。

全部符合

無論規則順序為何，所有符合的規則執行模式都會傳回所有符合規則的結果。如果您指定ALL_MATCHED，Amazon 詐騙偵測器會評估所有規則，並傳回所有符合規則的結果。

选择FIRST_MATCHED對於本教程，然後選擇下一步。

步驟 5：查看並創建檢測器版本

檢測器版本定義了用於生成欺詐預測的特定模型和規則。

1. 在檢閱和建立頁面上，檢閱您設定的偵測器詳細資訊、模型和規則。如果您需要進行任何變更，請選擇編輯旁邊的相應部分。
2. 選擇建立偵測器。建立之後，您的偵測器的第一個版本會顯示在 [偵測器版本] 表格中Draft狀態。

   您使用草案版本來測試您的檢測器。

使用建立偵測器AWS SDK for Python (Boto3)

下列範例顯示的範例要求PutDetectorAPI。檢測器充當您的檢測器版本的容器。該PutDetectorAPI 指定檢測器將評估什麼事件類型。下列範例假設您已建立事件類型sample_registration。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_detector (
detectorId = 'sample_detector',
eventTypeName = 'sample_registration'
)
```

建立偵測器版本

偵測器版本會定義規則、規則執行順序以及選擇性的模型版本，這些版本將用作產生詐騙預測請求的一部分。您可以將偵測器內定義的任何規則新增至偵測器版本。您還可以添加對評估事件類型進行培訓的任何模型。

每個偵測器版本的狀態為DRAFT,ACTIVE，或INACTIVE。只有一個檢測器版本可以在ACTIVE一次的狀態。期間GetEventPrediction請求，亞馬遜欺詐檢測器將使用ACTIVE檢測器如果沒有DetectorVersion已指定。

規則執行模式

Amazon 詐騙偵測器支援兩種不同的規則執行模式：FIRST_MATCHED和ALL_MATCHED。

- 如果規則執行模式為FIRST_MATCHED，Amazon 詐騙偵測器會依序評估規則，先到最後，在第一個符合的規則停止。然後，Amazon 詐騙偵測器會為該單一規則提供結果。如果規則評估為 false (不符合)，則會評估清單中的下一個規則。
- 如果規則執行模式為ALL_MATCHED，則評估中的所有規則都會平行執行，無論其順序為何。Amazon 詐騙偵測器會執行所有規則，並針對每個符合的規則傳回定義的結果。

使用建立偵測器版本AWS SDK for Python (Boto3)

下列範例顯示的範例要求CreateDetectorVersionAPI。規則執行模式設定為FIRST_MATCHED因此，Amazon 詐騙偵測器會依序評估規則，先到最後，在第一個符合的規則處停止。然後，Amazon 詐騙偵測器會在下列期間提供該單一規則的結果GetEventPrediction response。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_detector_version(
detectorId = 'sample_detector',
rules = [{
    'detectorId' : 'sample_detector',
    'ruleId' : 'high_fraud_risk',
    'ruleVersion' : '1'
},
{
    'detectorId' : 'sample_detector',
    'ruleId' : 'medium_fraud_risk',
    'ruleVersion' : '1'
},
{
    'detectorId' : 'sample_detector',
    'ruleId' : 'low_fraud_risk',
    'ruleVersion' : '1'
}
```

```
],
modelVersions = [{
    'modelId' : 'sample_fraud_detection_model',
    'modelType': 'ONLINE_FRAUD_INSIGHTS',
    'modelVersionNumber' : '1.00'
}],
ruleExecutionMode = 'FIRST_MATCHED'
)
```

若要更新偵測器版本的狀態，請使用UpdateDetectorVersionStatusAPI。下列範例會更新偵測器版本狀態DRAFT至ACTIVE。在一個GetEventPrediction請求，如果未指定偵測器 ID，Amazon 詐騙偵測器將使用ACTIVE檢測器的版本。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.update_detector_version_status(
detectorId = 'sample_detector',
detectorVersionId = '1',
status = 'ACTIVE'
)
```

刪除偵測器、偵測器版本或規則版本

刪除 Amazon Fraud Detector 中的偵測器之前，必須先刪除所有與該偵測器相關聯的偵測器版本和規則版本。

當您刪除偵測器、偵測器版本或規則版本時，Amazon Fraud Detector 會永久刪除該資源，且資料不會再儲存在 Amazon Fraud Detector 中。

刪除偵測器版本

您只能刪除處於DRAFT或INACTIVE狀態的偵測器版本。

1. 登入，開啟位於 https://console.aws.amazon.com/frauddetector 的 Amazon Fraud Detector 主控台。AWS Management Console
2. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇偵測器。
3. 選擇包含要刪除的檢測器版本的檢測器。
4. 選擇您要刪除的偵測器版本。

5. 選擇 動作，然後選擇 刪除。
6. 輸入**delete**，然後選擇 [刪除偵測器]。

刪除規則版本

只有在任何ACTIVE或INACTIVE偵測器版本未使用規則版本時，您才可以刪除該版本。如有必要，在刪除規則版本之前，請先將ACTIVE偵測器版本移至INACTIVE，然後刪除INACTIVE偵測器版本。

1. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇偵測器。
2. 選擇包含您要刪除之規則版本的偵測器。
3. 選擇相關聯的規則標籤，選擇您要刪除的規則。
4. 選擇您要刪除的規則版本。
5. 選擇「動作」，然後選擇「刪除規則版本」。
6. 輸入**delete**，然後選擇 [刪除版本]。

刪除偵測器

刪除偵測器之前，必須先刪除所有與該偵測器相關聯的偵測器版本和規則版本。

1. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇偵測器。
2. 選擇您要刪除的偵測器。
3. 選擇 [動作]，然後選擇 [刪除偵測器]。
4. 輸入**delete**，然後選擇 [刪除偵測器]。

資源

模型、規則和偵測器會使用變數、結果、標籤、清單和實體等資源來評估事件是否存在詐騙風險。本節提供建立和管理資源主的相關資訊。

主題

Variables

變數代表您要在詐騙預測中使用的資料元素。這些變數可從您為訓練模型準備的事件資料集、Amazon 詐騙偵測器模型的風險分數輸出或 Amazon 模SageMaker型中擷取。如需有關從事件資料集取得之變數的詳細資訊，請參閱使用資料模型總管取得事件資料集需求。

您必須先建立您要用於詐騙預測的變數，然後在建立事件類型時新增至事件中。您建立的每個變數都必須指派資料類型、預設值，以及選擇性的變數類型。Amazon 詐騙偵測器會豐富您提供的某些變數，例如 IP 位址、銀行識別號碼 (BIN) 和電話號碼，以建立其他輸入並提升使用這些變數的模型效能。

資料類型

變數必須具有變數所代表之資料元素的資料類型，並且可以選擇性地指派其中一個預先定義的變數變數類型。對於指派給變數類型的變數，會預先選取資料類型。可能的資料類型包括下列類型：

資料類型	描述	預設值	範例值
字串	字母、整數或兩者的任意組合	<empty>	ABC, 123, 1 日
整數	正整數或負數	0	1, -1

資料類型	描述	預設值	範例值
Boolean	真或假	False	真假
DateTime	僅以 ISO 8601 標準世界標準格式指定的日期和時間	<empty>	2019-11-30T13:01:01Z
Float	帶有小數點的數字	0.0	4.01

預設值

變數必須具有預設值。當 Amazon 詐騙偵測器產生詐騙預測時，如果 Amazon 詐騙偵測器未收到變數的值，則會使用此預設值執行規則或模型。您提供的預設值必須與選取的資料類型相符。在 AWS 主控台中，Amazon 詐騙偵測器會`0`為整數、布林值、`false`浮點數和字串 (空白) 指派預設值。`0.0`您可以為任何這些資料類型設定自訂預設值。

變數類型

當您建立變數時，您可以選擇性地將變數指派給變數類型。變數類型代表用來訓練模型和產生詐騙預測的常見資料元素。只有具有關聯變數類型的變數才能用於模型訓練。做為模型訓練程序的一部分，Amazon 詐騙偵測器會使用與變數關聯的變數類型來執行變數擴充、功能工程和風險評分。

Amazon 詐騙偵測器已預先定義下列可用於指派給變數的變數類型。

類別	變數類型	描述	資料類型	範例	
Se (工作階段	IP_ADDRES S	活動期間收集的 IP 位址	字串	192.0.2.0 注意：Amazon 詐騙偵測器	

類別	變數類型	描述	資料類型	範例		
				會豐富這項資料。如需詳細資訊，請參閱地理位置豐富		

類別	變數類型	描述	資料類型	範例
	用戶代理	在事件期間收集的使用者代理程式	字串	Mozilla 5.0 (視窗新界 10.0, 64, RV: 68.0) 壁虎
	指紋	用於事件之裝置的唯一識別碼	字串	薩德福烏
	SESSION_ID	事件作用中工作階段的工作階段 ID	字串	sid123456789
	是有效的憑證	指出用於事件登入的認證是否有效	Bool	True
使用者	電子郵件地址	活動期間收集的電子郵件地址	字串	abc@domain.com

類別	變數類型	描述	資料類型	範例
	PHONE_NUMBER	活動期間收集的電話號碼	字串	+1555-0100 注意：Amazon 詐騙偵測器會豐富這項資料。如需詳細資訊，請參閱電話號碼

類別	變數類型	描述	資料類型	範例		
				豐富		
帳單	帳單名稱	與帳單地址相關聯的名稱	字串	约翰·杜		

類別	變數類型	描述	資料類型	範例
	帳單電話	與帳單地址相關聯的電話號碼	字串	+1 555-0100 注意：Amazon 詐騙偵測器會豐富這項資料。如需詳細資訊，請參閱電話號碼

類別	變數類型	描述	資料類型	範例
				豐富
	帳單地址	帳單地址的第一行	字串	任何街道
	帳單地址	帳單地址的第二行	字串	任何單位 123
	帳單城市	帳單地址中的城市	字串	任何城市
	帳單狀態	帳單地址中的州或省	字串	任何州或省

類別	變數類型	描述	資料類型	範例		
	帳單國家	帳單地址中的國家/地區	字串	任何國家 注意：Amazon 詐騙偵測器會豐富這項資料。如需詳細資訊，請參閱地理位置		

類別	變數類型	描述	資料類型	範例		
				豐富		

類別	變數類型	描述	資料類型	範例
	帳單拉鍊	帳單地址中的郵遞區號	字串	01234 注意：Amazon 詐騙偵測器會豐富這項資料。如需詳細資訊，請參閱地理位置豐富

類別	變數類型	描述	資料類型	範例		
運費	出貨名稱	與運送地址相關聯的名稱	字串	约翰·杜		

類別	變數類型	描述	資料類型	範例
	運送電話	與運送地址相關聯的電話號碼	字串	+1 555-0100 注意：Amazon 詐騙偵測器會豐富這項資料。如需詳細資訊，請參閱電話號碼

類別	變數類型	描述	資料類型	範例
				豐富
	運送地址_L1	送貨地址的第一行	字串	任何街道
	運送地址_L2	送貨地址的第二行	字串	第 123 單元
	運送城市	運送地址中的城市	字串	任何城市
	運送狀態	運送地址中的州或省	字串	任何州

類別	變數類型	描述	資料類型	範例
	運送國家	運送地址中的國家/地區	字串	任何國家 注意：Amazon 詐騙偵測器會豐富這項資料。如需詳細資訊，請參閱地理位置

類別	變數類型	描述	資料類型	範例		
				豐富		

類別	變數類型	描述	資料類型	範例
	出貨_拉鍊	運送地址中的郵遞區號	字串	01234 注意：Amazon 詐騙偵測器會豐富這項資料。如需詳細資訊，請參閱地理位置豐富

類別	變數類型	描述	資料類型	範例
付款	訂單識別碼	交易的唯一識別碼	字串	LUX60
	價格	總訂單價格	字串	560.00
	貨幣代碼	新加坡貨幣代碼	字串	USD
	付款類型	活動期間用於付款的付款方式	字串	信用卡
	驗證碼	信用卡發卡機構或發卡銀行所傳送的英文字母代碼	字串	0000
	AVS	記憶卡處理器的位址驗證系統 (AVS) 回應碼	字串	Y
產品	產品類別	訂單項目的產品類別	字串	廚房
自訂	NUMERIC	任何可以表示為實數的變數	Floa	1.224
	CATEGORICAL	描述類別、區段或群組的任何變數	字串	大型

類別	變數類型	描述	資料類型	範例
	自由格式文字	作為活動一部分擷取的任何自由格式文字 (例如，客戶評論或留言)	字串	自由格式文本輸入的示例

將變量分配給變量類型

如果您打算使用變數來訓練模型，請務必選擇正確的變數類型來指派給變數。不正確的變數類型指派可能會對模型效能產生負面影響。對於稍後更改分配也會變得非常困難，特別是如果多個模型和事件使用了該變量。

您可以為變數指派任何一種預先定義的變數類型或其中一個自訂變數類型 — FREE_FORM_TEXT CATEGORICAL、或NUMERIC。

將變數指派給正確變數類型的重要注意事項

1. 如果變數與其中一個預先定義的變數類型相符，請使用它。請確定變數類型對應於變數。例如，如果您將 ip_address 變數指派給EMAIL_ADDRESS變數類型，則 ip_address 變數將不會充實豐富，例如 ASN、ISP、地理位置和風險評分。如需詳細資訊，請參閱變數豐富。
2. 如果變數與任何預先定義的變數類型不相符，請遵循下列建議指派其中一個自訂變數類型。
3. 將CATEGORICAL變數類型指派給通常沒有自然順序且可以放入類別、區段或群組的變數。您用來訓練模型的資料集可能具有 ID 變數，例如，商業識別碼、活動識別碼或政策識別碼。這些變數代表群組 (例如，具有相同政策_id 的所有客戶代表一個群組)。具有以下數據的變量必須分配分類變量類型-
   - 包含客戶識別碼、區段 ID、顏色 ID 、部門代碼或產品 ID 等資料的變數。

- 包含具有真、假或空值之布林值資料的變數。
- 可以放入群組或類別的變數，例如公司名稱、產品類別、卡片類型或推薦媒介。

> **Note**
>
> ENTITY_ID是亞馬遜欺詐檢測器用於分配給 ENTITY_ID 變量的保留變量類型。ENTITY_ID 變數是啟動您要評估之動作的實體識別碼。如果您要建立交易詐騙洞察 (TFI) 模型類型，則必須提供 ENTITY_ID 變數。您將需要決定數據中的哪個變量唯一標識起始操作的實體，並將其作為 ENTITY_ID 變量傳遞。如果資料集中的所有其他 ID 存在，以及您是否使用它們進行模型訓練，請將 CATEGORICAL 變數類型指派給資料集中的所有其他 ID。其他不是資料集中實體的 ID 範例可以是商業 ID、政策識別碼和促銷活動 ID 。

4. 將FREE_FORM_TEXT變數類型指派給包含文字區塊的變數。FREE_FORM_TEXT 變數類型的範例包括 — 使用者評論、註解、日期和推薦代碼。FREE_FORM_TEXT 資料包含多個以分隔符號分隔的記號。分隔符可以是字母數字和下劃線符號以外的任何字符。例如，用戶評論和評論可以用「空格」分隔符分隔，日期和推薦代碼可以使用連字符作為分隔符來分隔出前綴，後綴和中間部分。亞馬遜詐騙偵測器使用分隔符號從 FREE_FORM_TEXT 變數擷取資料。
5. 將 NUMERIC 變數類型指派給實數且具有固有排序的變數。NUMERIC 變數的範例包括週的日期、事件嚴重性、客戶評級。雖然您可以將 CATEGORIAL 變數類型指派給這些變數，但我們強烈建議您將所有具有固有順序的實數變數指派給 NUMERIC 變數類型。

變數豐富

Amazon 詐騙偵測器可豐富您提供的某些原始資料元素，例如 IP 位址、銀行識別號碼 (BIN) 和電話號碼，以建立額外的輸入並提升使用這些資料元素的模型效能。強化功能有助於識別潛在的可疑情況，並幫助模型捕獲更多欺詐行為。

電話號碼豐富

Amazon 詐騙偵測器會使用與地理位置、原始電信業者和電話號碼有效性相關的其他資訊來豐富電話號碼資料。所有在 2021 年 12 月 13 日或之後接受訓練且電話號碼包含國家/地區代碼 (+xxx) 的型號，都會自動啟用電話號碼強化功能。如果您已在模型中包含電話號碼變數，並且在 2021 年 12 月 13 日之前對其進行了訓練，請重新訓練模型，以便它可以利用此擴充功能。

我們強烈建議您對電話號碼變數使用以下格式，以確保資料能夠成功豐富。

變數	格式	描述
PHONE_NUMBER	國際標準	確保在電話號碼中包含國家/地區代碼（+xxx）。
電話和運費_電話	國際標準	確保在電話號碼中包含國家/地區代碼（+xxx）。

地理位置豐富

從 2022 年 2 月 8 日開始，亞馬遜欺詐偵測器會計算您為事件提供的 IP_ADDRESS、BILLING_ZIP 和運送 _ZIP 值之間的實際距離。計算出的距離會用作詐騙偵測模型的輸入。

若要啟用地理位置擴充功能，您的事件資料必須至少包含下列三個變數中的兩個：IP_ADDRESS、BILLING_ZIP 或出貨。此外，每個郵遞區號和運送郵遞區號必須分別具有有效的帳單國家代碼和運送國家代碼。如果您擁有在 2022 年 2 月 8 日之前進行訓練的模型，且其中包含這些變數，則必須重新訓練模型以啟用地理位置擴充。

如果由於資料無效，亞馬遜詐騙偵測器無法判斷事件的 IP_ADDRESS、BILLING_ZIP 或出貨值相關聯的位置，則會改用特殊的預留位置值。例如，假設事件具有有效的 IP_ADDRESS 和比林格 ZIP 值，但出貨 _ ZIP 值無效。在此情況下，僅針對 IP 位址 —> 帳單 ZIP 進行豐富。IP 位址 —> 郵遞區號和帳單郵遞區號-> 出貨 _ 郵遞不會完成豐富作業。取而代之的是，佔位符值用於它們的位置。無論您的模型是否啟用了地理位置擴充功能，模型的效能都不會改變。

您可以通過將您的 BILLING_ZIP 和運輸變量映射到自定義分類變量類型來選擇退出地理位置擴充。變更變數類型不會影響模型的效能。

地理位置變量格式

我們強烈建議您對地理位置變數使用以下格式，以確保您的位置資料能夠成功充實。

變數	格式	描述
IP_ADDRESS	IPv4 位址	舉個例子-1.1.1.1

變數	格式	描述
拉鍊和郵編付運輸	指定國家/地區的 ISO 3166-1 字母 2 字母郵遞區號	如需詳細資訊，請參閱本主題中的國家和地區代碼一節。
帳單國家及運送國家	兩個字母的標準國家代碼	如需詳細資訊，請參閱本主題中的國家和地區代碼一節。Amazon 詐騙偵測器會嘗試將國家/地區名稱的所有常見變體與 ISO 3166-1 兩個字母的標準國家/地區代碼相符。但是，我們不能保證它們會被正確匹配。

國家和地區代碼

下表提供 Amazon 詐騙偵測器支援用於擴充地理位置的國家和地區的完整清單。每個國家和地區都有一個指定的國家/地區代碼（特別是 ISO 3166-1 字母 2 字母的兩個字母的國家/地區代碼）和一個郵政編碼。

郵遞區號格式

- 9-號碼
- 一個-字母
- [X]-X 是可選的。例如，格爾斯尼「GY9 [9] 9aa」意味著「GY9 9 AA」和「GY99 9aa」都是有效的。使用一種格式。
- [X/XX]-可以使用 X 或 XX。例如，百慕達「aa [aa/99]」意味著「AA AA」和「AA 99」均為有效。請使用下列其中一種格式，但不要同時使用兩種格式。
- 某些國家/地區有固定的前綴 例如，安道爾的郵遞區號為 AD999。這意味著國家/地區代碼必須以 AD 字母開頭，後跟三個數字。

Code	名稱	郵政編碼
廣告	安道爾	AD999
AR	荷屬安地列斯	9999
AT	奧地利	9999
AU	澳洲	9999
AZ	亞塞拜然	AZ
BD	孟加拉	9999
是	比利時	9999
BG	保加利亞	9999
BM	百慕達	AA [aa/99]
BY	白俄羅斯	999999
CA	加拿大	a9a
CH	瑞士	9999
CL	智利	9999999
CO	哥倫比亞	999999
CR	哥斯大黎加	99999
CY	賽普勒斯	9999
鋯石	捷克	999 99
DE	德國	99999
DK	丹麥	9999
DO	多明尼加共和國	99999

Code	名稱	郵政編碼
DZ	阿爾及利亞	99999
EE	愛沙尼亞	99999
ES	西班牙	99999
FI	芬蘭	99999
FM	密克罗尼西亚联邦	99999
FO	法羅群島	999
法國	法國	99999
GB	英國	一個 [一] 9 [A/9] 9aa
GG	根西島	GY9 [9] 9 節
GL	格陵蘭	9999
GP	瓜地洛普	99999
GT	瓜地馬拉	99999
顧	關島	99999
小時	克羅埃西亞	99999
胡	匈牙利	9999
IE	愛爾蘭	一九九 [A/9] [A/9] [a/9] [a/9]
我	曼島	IM9 [9] 9AA
IN	印度	999999
IS	冰島	999
它	義大利	99999

Code	名稱	郵政編碼
流行性	澤西島	JE9 [9] 9
JP	日本	999-9999
KR	大韓民國	99999
李	列支敦斯登	9999
LK	斯里蘭卡	99999
LT	立陶宛	99999
呂	盧森堡	L-9999
LV	拉脫維亞	LV-9999
MC	摩納哥	99999
MD	摩尔多瓦共和国	9999
MH	馬紹爾群島	99999
MK	北馬其頓	9999
MP	北马里亚纳群岛	99999
MQ	馬提尼克	99999
山	馬爾他	AAA 9999
MX	墨西哥	99999
我的	馬來西亞	99999
NL	荷蘭	九九九
NO	挪威	9999
NZ	紐西蘭	9999

Code	名稱	郵政編碼
酸鹼度	菲律賓	9999
PK	巴基斯坦	99999
PL	波蘭	99-999
PR	波多黎各	99999
PT	葡萄牙	9999-999
PW	帛琉	99999
回覆	團圓	99999
RO	羅馬尼亞	999999
茹	俄罗斯联邦	999999
SE	瑞典	999 99
SG	新加坡	999999
SI	斯洛維尼亞	9999
SK	斯洛伐克	999 99
SM	聖馬利諾	99999
日	泰國	99999
TR	土耳其	99999
UA	烏克蘭	99999
美國	美國	99999
UY	烏拉圭	99999
六	美屬維京群島	99999

Code	名稱	郵政編碼
WF	瓦利斯和富圖納群島	99999
YT	馬約特島	99999
ZA	南非	9999

使用者代理程式豐富

如果您建立帳戶接管見解 (ATI) 模型，則必須在資料集中提供useragent變數類型的變數。此變數包含登入事件的瀏覽器、裝置和作業系統資料。Amazon 詐騙偵測器透過其他資訊 (例如user_agent_familyOS_family、和) 來豐富使用者代理程式資料。device_family

創建一個變量

您可以使用建立變數命令，在 Amazon 詐騙偵測器主控台中建立變數，使用，或使CreateVariable用 AWS SDK for Python (Boto3)

使用 Amazon 詐騙偵測器主控台建立變數

此範例會建立兩個變數，email_address和ip_address，並將它們指派給對應的變數類型 (EMAIL_ADDRESS和IP_ADDRESS)。這些變數可作為範例使用。如果您要建立用於模型訓練的變數，請使用資料集中適合您使用案例的變數。確保在創建變量變數豐富之前閱讀有關以變數類型及更多內容。

若要建立變數，

1. 開啟AWS管理主控台並登入您的帳戶。
2. 導覽至 Amazon 詐騙偵測器，在左側導覽中選擇「變數」，然後選擇「建立」。
3. 在 [新變數] 頁面中email_address，輸入變數名稱。選擇性地輸入變數的說明。
4. 在變數類型中，選擇 [電子郵件地址]。
5. Amazon 詐騙偵測器會自動選取此變數類型的資料類型，因為此變數類型已預先定義。如果您的變數未自動指派變數類型，請從清單中選取變數類型。如需詳細資訊，請參閱變數類型。
6. 如果您要為變數提供預設值，請選取「定義自訂預設值」，然後輸入變數的預設值。如果您正在遵循此範例，請略過此步驟。
7. 選擇 建立 。

8. 在 email_address 概述頁面中，確認您剛剛創建的變量的詳細信息。

   如果您需要更新，請選擇 [編輯] 並提供更新。選擇 Save changes (儲存變更)。

9. 重複此程序以建立另一個變數，ip_address並為變數類型選擇 IP 位址。

10. 「變數」頁面會顯示新建立的變數。

> **Important**
>
> 我們建議您從資料集建立任意數量的變數。您可以稍後在建立事件類型時決定要包含哪些變數，以訓練模型以偵測詐騙並產生詐騙偵測。

使用建立變數 AWS SDK for Python (Boto3)

下列範例顯示 CreateVariableAPI 的要求。此範例會建立兩個變數，email_address和ip_address，並將它們指派給對應的變數類型(EMAIL_ADDRESS和IP_ADDRESS)。

這些變數可作為範例使用。如果您要建立用於模型訓練的變數，請使用資料集中適合您使用案例的變數。確保在創建變量變數豐富之前閱讀有關以變數類型及更多內容。

請務必指定變數來源。它有助於識別變量值的派生位置。如果變數來源為 EVENT，則會將變數值做為GetEventPrediction要求的一部分傳送。如果變數值為MODEL_SCORE，則會由 Amazon 詐騙偵測器填入。如果EXTERNAL_MODEL_SCORE，則會由匯入的SageMaker模型填入變數值。

```
import boto3
fraudDetector = boto3.client('frauddetector')

 #Create variable email_address
   fraudDetector.create_variable(
     name = 'email_address',
     variableType = 'EMAIL_ADDRESS',
     dataSource = 'EVENT',
     dataType = 'STRING',
     defaultValue = '<unknown>'
     )

#Create variable ip_address
   fraudDetector.create_variable(
     name = 'ip_address',
```

```
    variableType = 'IP_ADDRESS',
    dataSource = 'EVENT',
    dataType = 'STRING',
    defaultValue = '<unknown>'
    )
```

刪除變數

刪除變數時，Amazon 詐騙偵測器會永久刪除該變數，且資料不會再儲存在 Amazon 詐騙偵測器中。

您無法刪除 Amazon 詐騙偵測器中包含在事件類型中的變數。您必須先刪除與變數相關聯的事件類型，然後再刪除變數。

您無法手動刪除 Amazon 詐騙偵測器模型輸出變數和SageMaker模型輸出變數。刪除模型時，Amazon 詐騙偵測器會自動刪除模型輸出變數。

您可以在 Amazon 詐騙偵測器主控台中刪除變數、使用刪除變數 CLI 命令、使用 DeleteVariableAPI 或使用 AWS SDK for Python (Boto3)

使用控制台刪除變量

若要刪除變數，

1. 登入AWS Management Console並開啟亞馬遜詐騙偵測器主控台，網址為 https://console.aws.amazon.com/frauddetector。
2. 在 Amazon 詐騙偵測器主控台的左側導覽窗格中，選擇「資源」，然後選擇「變數」。
3. 選擇您要刪除的變數。
4. 選擇 動作，然後選擇 刪除。
5. 輸入變數名稱，然後選擇 [刪除變數]。

使用刪除變數 AWS SDK for Python (Boto3)

下列程式碼範例會使用 API 刪除變數的DeleteVariable顧客名稱。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.delete_variable (
```

```
name = 'customer_name'

)
```

標籤

標籤會將事件分類為詐騙或合法。標籤與事件類型相關聯，且用來在 Amazon Fraud Detector 中培訓機器學習模型。如果您打算訓練「線上詐騙洞察」(OFI) 或「交易詐騙洞察」(TFI) 模型，則訓練資料集中至少有 400 個事件必須歸類為框架或合法事件。您可以使用任何標籤 (例如欺詐、合法、1 或 0) 來分類訓練資料集中的事件。訓練完成後，訓練過的模型會評估事件是否存在詐騙，並使用這些值將事件分類為詐騙或合法事件。

您必須先使用訓練資料集中使用的值建立標籤，然後將標籤與用於建立和訓練詐騙偵測模型的事件類型產生關聯。

建立標籤

您可以在 Amazon Fraud Detector 主控台中建立標籤、使用 put-label 命令、使用 PutLabelAPI 或使用 AWS SDK for Python (Boto3).

使用 Amazon Fraud Detector 主控台建立標籤

若要建立標示，

1. 開啟AWS管理主控台並登入您的帳戶。
2. 導覽至 Amazon Fraud Detector，在左側導覽中選擇「標籤」，然後選擇「建立」。
3. 在「建立標籤」頁面中，輸入詐騙事件的標籤名稱作為標籤名稱。標籤名稱必須與代表訓練資料集中欺詐活動的標籤相對應。選擇性輸入標籤的描述。
4. 選擇「建立標籤」。
5. 建立第二個標籤，並輸入合法事件的標籤名稱。請確定標籤名稱對應於您訓練資料集中代表合法活動的值。

使用建立標籤AWS SDK for Python (Boto3)

以下示AWS SDK for Python (Boto3)例代碼使用 PutLabelAPI 創建兩個標籤（欺詐，合法）。建立標籤之後，您可以將標籤新增至事件類型，以對特定事件進行分類。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_label(
name = 'fraud',
description = 'label for fraud events'
)

fraudDetector.put_label(
name = 'legit',
description = 'label for legitimate events'
)
```

更新標籤

如果您的事件資料集與 Amazon Fraud Detector 一起儲存，您可能需要新增或更新已儲存事件的標籤，例如當您針對事件執行離線詐騙調查，並想要關閉機器學習反饋迴圈時。

您可以使用命update-event-label令、使用 UpdateEventLabelAPI 或使用AWS SDK for Python (Boto3)

下列AWS SDK for Python (Boto3)範例程式碼會新增與使用`UpdateEventLabel` API 的事件類型註冊相關聯的標籤詐騙。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.update_event_label(
            eventId        = '802454d3-f7d8-482d-97e8-c4b6db9a0428',
            eventTypeName  = 'registration',
            assignedLabel  = 'fraud',
            labelTimestamp = '2020-07-13T23:18:21Z'
)
```

更新 Amazon Fraud Detector 中儲存的事件資料中的事件標籤

您可能需要針對已儲存在 Amazon Fraud Detector 中的事件新增或更新詐騙標籤，例如當您針對事件執行離線詐騙調查，並想要關閉機器學習回饋迴圈時。若要更新已儲存在 Amazon Fraud Detector 中

的事件標籤，請使用UpdateEventLabel API 操作。關於 UpdateEventLabel API 調用的範例如下所示。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.update_event_label(
            eventId        = '802454d3-f7d8-482d-97e8-c4b6db9a0428',
            eventTypeName  = 'sample_registration',
            assignedLabel  = 'fraud',
            labelTimestamp = '2020-07-13T23:18:21Z'
)
```

刪除標籤

刪除標籤時，Amazon Fraud Detector 會永久刪除該標籤，而資料將不再儲存在 Amazon Fraud Detector 中。

無法刪除 Amazon Fraud Detector 中包含在事件類型中的標籤。且無法刪除指派給事件 ID 的標籤。必須先刪除相關的事件 ID。

您可以在 Amazon Fraud Detector 主控台中刪除標籤、使用刪除標籤命令、使用 DeleteLabelAPI 或使用AWS SDK for Python (Boto3)

使用主控台刪除標籤

刪除標籤

1. 登入，開啟位於 https://console.aws.amazon.com/frauddetector 的 Amazon Fraud Detector 主控台。AWS Management Console
2. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇「資源」，然後選擇「標籤」。
3. 選擇想要刪除的標籤。
4. 選擇 動作，然後選擇 刪除。
5. 輸入標籤名稱，然後選擇 [刪除標籤]。

使用刪除標籤AWS SDK for Python (Boto3)

下列AWS SDK for Python (Boto3)範例程式碼會刪除使用 DeleteLabelAPI 合法的標籤。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.delete_event_label (
    name = 'legit'
)
```

規則

規則是告知 Amazon 詐騙偵測器如何在詐騙預測期間解譯變數值的條件。規則是檢測器邏輯的一部分，它由以下元素組成：

- 變數或清單 — 變數代表您要在詐騙預測中使用的事件資料集中的資料元素。清單是事件資料集中變數的一組輸入資料元素。規則中使用的變數必須在評估的事件類型中預先定義，且規則中使用的清單必須與變數類型相關聯。如需詳細資訊，請參閱 Variables 及 清單。
- 運算式 — 規則中的運算式會擷取您的商務邏輯。如果您在規則中使用變數，則會使用變數、比較運算子 (例如 >、<、<=、>=. ==) 和值來建構簡單的規則運算式。如果您使用清單，則規則運算式會建構為清單項目和清單名稱。in如需詳細資訊，請參閱規則語言參考。您可以使用and和將多個運算式組合在一起or。所有運算式都必須評估為布林值 (真或假)，且長度小於 4,000 個字元。不支援如果其他類型條件。
- 結果 — 結果是 Amazon 詐騙偵測器在符合規則時傳回的回應。結果表明欺詐預測的結果。您可以為每個可能的詐騙預測建立結果，並將其新增至規則。如需詳細資訊，請參閱成果。

偵測器必須至少有一個關聯的規則。一個規則最多可以有 3 個清單，一個偵測器最多可以有 30 個清單。您可以將規則建立為偵測器建立程序的一部分。您也可以建立新規則，並將其與現有偵測器建立關聯。

規則語言參考

下一節概述 Amazon 詐騙偵測器中的運算式 (亦即規則寫入) 功能。

使用變數

您可以使用已評估事件類型中定義的任何變數做為運算式的一部分。使用美元符號來表示一個變量：

```
$example_variable < 100
```

使用清單

您可以使用與變數類型相關聯且已填入項目做為規則運算式一部分的任何清單。使用美元符號來指示清單項目值：

```
$example_list_variable in @list_name
```

比較，成員資格和身份運營商

Amazon 詐騙偵測器包括下列比較運算子：>、>=、<、<=、！=，==，在中，不在

範例如下：

範例：

```
$variable < 100
```

範例：在中，不在

```
$variable in [5, 10, 25, 100]
```

例如：！ =

```
$variable != "US"
```

範例：

```
$variable == 1000
```

運算子表

運算子	亞馬遜欺詐檢測器操
等於	==
不等於	!=
大於	>

運算子	亞馬遜欺詐檢測器操
小於	<
大於或等於	>=
小於或等於	<=
In (入)	in
及	以及
或	或
Not	!

基本數學

您可以在運算式中使用基本數學運算子 (例如，+、-、*、/)。典型的使用案例是當您需要在評估期間合併變數時。

在下面的規則中，我們$variable_1使用添加變量$variable_2，並檢查總數是否小於 10。

```
$variable_1 + $variable_2 < 10
```

基本數學表資料

運算子	亞馬遜欺詐檢測器操
加	+
減去	-
Multiply	*
Divide	/
模	%

正則表達式

您可以使用正則表達式來搜索特定的模式作為表達式的一部分。如果您希望為其中一個變量匹配特定的字符串或數值，這將特別有用。Amazon 詐騙偵測器僅在使用規則運算式時支援比對 (例如，它會根據提供的字串是否與規則運算式相符，傳回 True/False)。亞馬遜欺詐檢測器的正則表達式支持基於 Java 中的 .match（）（使用 RE2J 正則表達式庫）。互聯網上有幾個有用的網站可用於測試不同的正則表達式模式。

在下面的第一個例子中，我們首先將變量轉換email為小寫。然後，我們檢查模式@gmail.com是否在email變量中。請注意，第二個週期被轉義，以便我們可以明確地檢查字符串.com。

```
regex_match(".*@gmail\.com", lowercase($email))
```

在第二個範例中，我們檢查變數是否phone_number包含國家/地區代碼，+1以判斷電話號碼是否來自美國。加號被轉義，以便我們可以明確地檢查字符串+1。

```
regex_match(".*\+1", $phone_number)
```

正則表達式

運算子	亞馬遜欺詐檢測器示
匹配任何以開頭的字符串	正則表達式匹配（「^ 我的字符串」，$ 變量）
完全匹配整個字符串	正則表達式匹配（「我的字符串」，$ 變量）
匹配除新行以外的任何字符	正則表達式匹配（」。「，$ 變量）
匹配任意數量的字符，除了「我的字符串」之前的新行	正則表達式匹配 (」. * 我的字符串」，$ 變量）
跳脫特殊字元	\

檢查缺少值

有時，檢查該值是否丟失是有益的。在亞馬遜欺詐檢測器，這是由 null 表示。您可以使用以下語法來執行此操作：

```
$variable != null
```

同樣，如果您想檢查一個值是否不存在，則可以執行以下操作：

```
$variable == null
```

多重條件

您可以使用and和將多個運算式組合在一起or。找到單個真值時，Amazon 詐騙偵測器會在OR運算式中停止，並在找到單個 false 值AND時停止。

在下面的例子中，我們正在檢查使用條件兩個條and件。在第一條語句中，我們正在檢查變量 1 是否小於 100。在第二，我們檢查變量 2 是否不是美國。

由於規則使用and，兩者都必須為 TRUE，整個條件才能評估為 TRUE。

```
$variable_1 < 100 and $variable_2 != "US"
```

您可以使用括號來分組布林運算，如下所示：

```
$variable_1 < 100 and $variable_2 != "US" or ($variable_1 * 100.0 > $variable_3)
```

其他運算式類型

DateTime函數

函數	描述	範例
獲取當前日期時間（）	以 ISO8601 UTC 格式提供規則執行的目前時間。您可以使用極限毫秒（獲取目前日期時間（））來執行其他操作	獲取當前日期時間（）=「2023 年 3 月 28 日」
伊斯之前 (DateTime1, DateTime 2)	返回一個布爾值（真/假），如果調用者 DateTime 1 是 2 之前 DateTime	之前（獲取當前日期時間（），「2019 年 11 月 30 日 01:01 Z」）==「假」 是之前（獲取當前日期時間（），「2050-11-30 噸 01:05 Z」）==「真」

函數	描述	範例
伊斯福DateTime特 (1, DateTime 2)	返回一個布爾值（真/假），如果調用者 DateTime 1 是 2 之後 DateTime	之後（獲取當前日期時間（），「2019 年 11 月 30 日 01 日 Z」）==「真」 之後（獲取當前日期時間（），「2050-11-30 嘛 01:05 Z」）==「假」
平均毫秒 () DateTime	需要 a DateTime 並返回以DateTime紀元毫秒為單位。對於在日期執行數學運算非常有用	毫秒（「2019 年 11 月 1 日 1 時 1 時」）== 1575032461

字串運算子

運算子	範例
將字符串轉換為大寫	大寫（$ 變量）
將字符串轉換為小寫	小寫（$ 變量）

其他

運算子	註解
添加評論	# 我的評論

建立 規則

您可以在 Amazon 詐騙偵測器主控台中建立規則、使用建立規則命令、使用 CreateRuleAPI 或使用. AWS SDK for Python (Boto3)

每個規則都必須包含可擷取您商務邏輯的單一運算式。所有運算式都必須評估為布林值 (真或假)，且長度小於 4,000 個字元。不支援如果其他類型條件。運算式中使用的所有變數都必須在評估的事件類型中預先定義。同樣地，運算式中使用的所有清單都必須預先定義，並與可變類型相關聯，並填入項目。

下列範例會high_risk為現有偵測器建立規則payments_detector。規則會將運算式和結果verify_customer與規則相關聯。

先決條件

若要遵循下列步驟，請確定您已完成下列步驟，然後再繼續建立規則：

- 建立偵測器
- 建立結果

如果您要為使用案例建立偵測器、規則和結果，請以與您的使用案例相關的名稱和運算式取代範例偵測器名稱、規則名稱、規則運算式和結果名稱。

在 Amazon 詐騙偵測器主控台中建立新規則

1. 開啟AWS管理主控台並登入您的帳戶。導航到亞馬遜欺詐檢測器。
2. 在左側導覽窗格中，選擇 [偵測器]，然後選取您為使用案例建立的偵測器，範例 pay ments_偵測器。
3. 在 payments_偵測器頁面中，選擇「關聯的規則」標籤，然後選擇「建立規則」。
4. 在 [新增規則] 頁面中，輸入下列內容：

    a. 在名稱中，輸入規則的名稱，範例 **high_risk**

    b. 在「描述-選擇性」中，選擇性地輸入規則說明，範例 **This rule captures events with a high ML model score**

    c. 在「表示式」中，使用「表示式」快速參考指南為您的使用案例輸入規則運算式。範例 `$sample_fraud_detection_model_insightscore >900`

    d. 在「成果」中，選擇您為使用案例建立的結果，例如 verify _customer。結果是欺詐預測的結果，如果規則在評估期間相符，則會傳回結果。
5. 選擇儲存規則

您已為偵測器建立新規則。這是 Amazon 詐騙偵測器會自動讓偵測器使其可供偵測器使用的規則第 1 版。

使用建立規則 AWS SDK for Python (Boto3)

下列範例程式碼使用 CreateRuleAPI 建立現有偵測器的規則high_riskpayments_detector。範例程式碼也會在規則中加入規則運算式和結果verify_customer。

先決條件

若要使用範例程式碼，請在繼續建立規則之前，先確定您已完成下列步驟：

- 建立偵測器
- 建立結果

如果您要為使用案例建立偵測器、規則和結果，請使用與您的使用案例相關的名稱和運算式來取代範例偵測器名稱、規則名稱、規則運算式和結果名稱。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_rule(
ruleId = 'high_risk',
detectorId = 'payments_detector',
expression = '$sample_fraud_detection_model_insightscore > 900',
language = 'DETECTORPL',
outcomes = ['verify_customer']
)
```

您已建立規則的第 1 版，Amazon 詐騙偵測器會自動提供該規則供偵測器使用。

更新規則

您可以隨時更新規則，方法是新增或更新規則說明、更新規則運算式，或新增或移除規則的結果。當您更新規則時，會建立新的規則版本。

您可以在 Amazon 詐騙偵測器主控台中使用update-rule-version命令、使用 UpdateRuleVersionAPI 或使用 AWS SDK 更新規則。

更新規則後，請務必更新偵測器版本以使用新的規則版本。

在 Amazon 詐騙偵測器主控台中更新規則

若要更新規則，

1. 開啟AWS管理主控台並登入您的帳戶。導航到亞馬遜欺詐檢測器。
2. 在左側導覽窗格中，選擇「偵測器」。
3. 在「偵測器」窗格中，選取與您要更新之規則相關聯的偵測器。

4. 在偵測器頁面中，選擇 [關聯規則] 索引標籤，然後選取您要更新的規則。
5. 在規則頁面中，選擇「動作」，然後選取「建立版本」。
6. 請注意，版本已變更。輸入更新的描述、表示式或結果。
7. 選擇「儲存新版本」

使用更新規則 AWS SDK for Python (Boto3)

下列範例程式碼會使用 UpdateRuleVersionAPI 將規則的臨界值`high_risk`從 900 更新為 950。此規則與偵測器相關聯`payments_detector`。

```
fraudDetector.update_rule_version(
rule = {
    'detectorId' : 'payments_detector',
    'ruleId' : 'high_risk',
    'ruleVersion' : '1'
},
expression = '$sample_fraud_detection_model_insightscore > 950',
language = 'DETECTORPL',
outcomes = ['verify_customer']
)
```

清單

清單是事件資料集中變數的一組輸入資料。您可以在與偵測器相關聯的規則中使用輸入資料。規則是指示 Amazon Fraud Detector 如何在 Fraud Detector 預測期間解譯輸入資料的條件。例如，您可以建立 IP 位址清單，然後建立規則，以便在清單中有特定 IP 位址時拒絕存取。使用清單的規則會以`@list_name`格`$ip_address_value`式表示。

使用 Amazon Fraud Detector，您可以透過新增或移除資料來管理清單，而無需更新關聯的規則。與清單相關聯的規則會自動合併新增或移除的資料。

清單最多可包含 100,000 個唯一項目，每個項目最多可包含 320 個字元。依預設，您在規則中使用的每個清單都與 Amazon 詐騙偵測器的變數類型 FREE_FORM_TEXT 相關聯。您可以隨時為清單指派變數類型。一個規則中最多可以使用 3 個清單。

您可以使用 API、或使用AWS SDK，在 Amazon Fraud Detector 主控台中建立清單、新增項目到清單、刪除清單中的一或多個項目，或在 Amazon 詐騙偵測器主控台中為清單指派變數類型。AWS CLI

建立清單

您可以建立包含事件資料集中變數輸入資料 (項目) 的清單，並在規則運算式中使用該清單。您可以動態管理清單中的項目，而無需更新使用清單的規則。

若要建立清單，您必須先指定名稱，然後選擇性地將清單與 Amazon Fraud Detector變數類型 支援的名稱建立關聯。根據預設，亞馬遜 Fraud Detector 會假設該清單為 FREE_FORM_TEXT 變數類型。

您可以使用 API，或使用AWS SDK，在 Amazon Fraud Detector 主控台中建立清單。AWS CLI

使用 Amazon Fraud Detector 主控台建立清單

建立清單

1. 開啟AWS管理主控台並登入您的帳戶。導覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇清單。
3. 在列表詳細信息
   a. 在清單名稱中，輸入清單名稱。
   b. 在描述中，選用地輸入描述。
   c. (選擇性) 在「變數」類型中，為清單選取變數類型。

> **Important**
> 如果您的清單包含 IP 位址，請務必選取 IP_ADDRESS 作為變數類型。如果您未選取變數類型，Amazon Fraud Detector 會假設該清單為 FREE_FORM_TEXT 變數類型。

4. 在「添加列表數據」中，添加列表條目，每行中有一個條目。您也可以從試算表複製和貼上項目。

> **Note**
> 請確定項目並未使用逗號分隔，且在清單中是唯一的。如果輸入兩個相同的項目，則只會新增一個項目。

5. 選擇 建立 。

使用建立清單AWS SDK for Python (Boto3)

您可以透過指定清單名稱來建立清單。建立清單時，您可以選擇性地提供說明、關聯變數類型，或將項目新增至清單。或者，您可以稍後透過新增項目或說明來更新清單。如果在創建列表時尚未分配變量類型，則可以稍後將變量類型分配給列表。列表的變量類型在分配後不能更改。

> **Important**
>
> 如果您的清單包含 IP 位址，請務必將 IP_ADDRESS 指派為變數類型。如果您未指派變數類型，Amazon Fraud Detector 會假設清單為 FREE_FORM_TEXT 變數類型。

下`allow_email_ids`列範例會使用 CreateListAPI 作業，藉由提供說明、變數類型，以及新增四個清單項目來建立清單。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_list (
     name = 'allow_email_ids',
     description = 'legitimate email_ids'
     variableType = 'EMAIL_ADDRESS',
     elements = ['emailId _1', 'emailId_2', 'emailId_3','emailId_4']
     )
```

在列表中添加條目

建立清單後，您可以隨時在清單中新增或附加項目。當您在清單中新增或附加項目時，您就不必更新清單中關聯的規則。規則會自動合併新增的項目。

您的清單最多可包含 100,000 個不重複項目，每個項目最多可包含 320 個字元。

您可以使用 API，或使用AWS SDK，在 Amazon Fraud Detector 主控台中新增項目。AWS CLI

使用 Amazon Fraud Detector 主控台在清單中新增項目

若要在清單中新增一或多個項目

1. 開啟AWS管理主控台並登入您的帳戶。導覽至 Amazon Fraud Detector。

2. 在左側導覽窗格中選擇清單。
3. 在「清單」頁面中，選取要新增項目的清單。
4. 在清單詳細資料頁面中，選取「清單資料」標籤，然後選擇「新增資料
5. 在「新增清單資料」方塊中，在每一行新增一個項目，或複製並貼上試算表中的項目。請確定不要使用逗號來分隔項目。
6. 選擇 Add (新增)。

使用新增清單中的項目AWS SDK for Python (Boto3)

下列範例會使用 UpdateListAPI 作業，在清單中新增兩個新項`allow_email_ids`目。請確定您要新增的項目在清單中是唯一的。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.update_list (
     name = 'allow_email_ids',
     updateMode = 'APPEND'
     elements = ['emailId_11','emailId_12']
```

將變量類型分配給列表

您在規則中使用的每個清單都必須與 Amazon 詐騙偵測器的變數類型變數類型相關聯。根據預設，亞馬遜 Fraud Detector 會假設該清單為 FREE_FORM_TEXT 變數類型。重要的是要注意，由 IP 地址組成的列表必須與 IP_ADDRESS 變量類型相關聯。

您可以在建立清單時或稍後隨時將清單與變數類型產生關聯。如果您已將清單與變數類型產生關聯，而且想要稍後變更它，則必須建立新清單。您無法更改清單的變數類型。

您可以使用 API，或使用AWS SDK，在 Amazon Fraud Detector 主控台中AWS CLI指派變數類型。

使用 Amazon Fraud Detector 主控台將變數類型指派給清單

若要將變數類型指派給清單

1. 開啟AWS管理主控台並登入您的帳戶。導覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇清單。

3. 在「清單」頁面中，選取您要指派變數類型的清單。
4. 在清單詳細資料頁面中，選擇「動作」並選取「編輯清單」。
5. 在 [編輯] 清單方塊中，選取清單的變數類型。
6. 選擇 儲存 。

使用指派變數類型給清單AWS SDK for Python (Boto3)

下列範例會使用 UpdateListAPI 作業，將變數類型指派給`allow_ip_address`清單。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.update_list (
     name = 'allow_ip_address',
     variableType = 'IP_ADDRESS'
)
```

刪除清單

您可以刪除未在任何規則中使用的清單。刪除清單時，Amazon Fraud Detector 會永久刪除該清單及清單中的所有項目。

您可以使用AWS CLI或AWS SDK，使用 API 在 Amazon Fraud Detector 主控台中刪除清單。

使用 Amazon Fraud Detector 主控台刪除清單

若要刪除清單

1. 開啟AWS管理主控台並登入您的帳戶。導覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇清單
3. 在清單頁面中選取您要刪除的清單。
4. 在清單詳細資料頁面中，選擇「動作」，然後選取「刪除清單
5. 選擇 [刪除清單]。

使用刪除清單AWS SDK for Python (Boto3)

下列範例會使用 DeleteListAPI 作業來刪除`allow_email_ids`。

```
import boto3
                        fraudDetector = boto3.client('frauddetector')
fraudDetector.delete_list(
   name = 'allow_email_ids'
)
```

從清單中刪除項目

您可以隨時從清單中刪除一或多個項目。刪除清單中的項目時，您不需要更新與清單相關聯的規則。規則會自動合併更新的清單。

您可以使用AWS CLI或AWS SDK，使用 API 從 Amazon Fraud Detector 主控台的清單中刪除項目。

使用 Amazon Fraud Detector 主控台刪除清單中的項目

若要從清單中刪除一或多個項目

1. 開啟AWS管理主控台並登入您的帳戶。導覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇清單
3. 在清單頁面中選取包含您要刪除之項目的清單。
4. 在清單詳細資料頁面中，選取 [列出資料] 索引標籤，然後選取您要刪除的項目。
5. 選擇「刪除」並再次選擇「刪除」以確認。

使用刪除清單中的項目AWS SDK for Python (Boto3)

在下列範例中，UpdateListAPI 作業會從`allow_email_ids`清單中刪除項目。

```
import boto3
                        fraudDetector = boto3.client('frauddetector')
fraudDetector.update_list(
   name = 'allow_email_ids',
   updateMode = 'REMOVE',
   elements = ['emailId_4', 'emailId_12']
)
```

刪除清單中的所有項目

如果該清單未在規則中使用，您可以刪除清單中的所有項目。您可以刪除清單中的所有項目，稍後在同一清單中新增項目。

您可以使用AWS CLI或AWS SDK，使用 API 從 Amazon Fraud Detector 主控台的清單中刪除項目。

使用 Amazon Fraud Detector 主控台刪除清單中的所有項目

從清單中刪除所有項目的步驟

1. 開啟AWS管理主控台並登入您的帳戶。導覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇清單
3. 在清單頁面中選取包含您要刪除之項目的清單。
4. 在清單詳細資料頁面中，選取「清單資料」標籤，然後選擇「全部刪除
5. 在 [全部刪除] 方塊中，輸`delete all`入確認，然後選擇 [刪除所有清單資料]。

使用刪除清單中的所有項目AWS SDK for Python (Boto3)

在下列範例中，UpdateListAPI 作業會刪除`allow_email_ids`清單中的所有項目。

```
import boto3
                        fraudDetector = boto3.client('frauddetector')
fraudDetector.update_list(
   name = 'allow_email_ids',
   updateMode = 'REPLACE',
   elements = []
)
```

成果

結果是欺詐預測的結果。您可以為每個可能的欺詐預測結果創建結果。例如，您可能希望結果代表風險等級（高風險，中等風險和低風險）或操作（批准，審查）。建立結果之後，您可以在規則新增一或多個結果。作為回GetEventPrediction應的一部分，Amazon Fraud Detector 會傳回任何符合規則的定義結果。

建立結果

您可以在 Amazon Fraud Detector 主控台、使用放置結果命令、使用 PutOutcomeAPI 或使用AWS SDK for Python (Boto3).

使用 Amazon Fraud Detector 主控台建立結果

若要建立一或多個結果，

1. 開啟AWS管理主控台並登入您的帳戶。導航到 Amazon Fraud Detector。
2. 在左側導覽窗格中選擇結果。
3. 在「成果」頁面中，選擇「建立」。
4. 在「新增結果」頁面中，輸入下列內容：
   a. 在「結果」名稱中，輸入結果的名稱。
   b. 在結果描述中，您可以在其中新增一個描述。
5. 選擇 [儲存結果]。
6. 重複步驟 2 至 5 以建立其他結果。

使用建立結果AWS SDK for Python (Boto3)

下列範例會使用PutOutcome API 建立三個結果。它們是verify_customerreview、和approve。建立結果後，您可以將它們指派給規則。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_outcome(
name = 'verify_customer',
description = 'this outcome initiates a verification workflow'
)

fraudDetector.put_outcome(
name = 'review',
description = 'this outcome sidelines event for review'
)

fraudDetector.put_outcome(
name = 'approve',
```

```
description = 'this outcome approves the event'
)
```

刪除結果

無法刪除規則版本中使用的結果。

刪除結果時，Amazon Fraud Detector 會永久刪除該結果，且資料不會再儲存在 Amazon Fraud Detector 中。

您可以在 Amazon Fraud Detector 主控台中刪除結果、使用刪除結果命令、使用 DeleteOutcomeAPI 或使用AWS SDK for Python (Boto3)

在 Amazon Fraud Detector 主控台中刪除結果

若要刪除結果

1. 登入，開啟位於 https://console.aws.amazon.com/frauddetector 的 Amazon Fraud Detector 主控台。AWS Management Console
2. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇 [資源]，然後選擇 [成果]。
3. 選擇想要刪除的結果。
4. 選擇 動作，然後選擇 刪除。
5. 輸入結果名稱，然後選擇 [刪除結果]。

使用刪除結果AWS SDK for Python (Boto3)

下列範例會使用 DeleteOutcomeAPI 刪除`verify_customer`結果。刪除結果後，您就無法再將其指定給規則。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.delete_outcome(
name = 'verify_customer'
)
```

實體

實體代表正在執行事件的人員或物件。實體類型會將實體分類。範例分類包括客戶、商家、使用者或帳戶。您提供實體類型 (ENTITY_TYPE) 和實體識別碼 (ENTITTY_ID) 做為事件資料集的一部分，以指示執行事件的特定實體。

Amazon Fraud Detector 會在產生事件的詐騙預測時使用實體類型，以指出執行事件的人員。您要在詐騙預測中使用的實體類型必須先在 Amazon Fraud Detector 中建立，然後在建立事件類型時新增至事件。

建立實體類型

您可以在 Amazon Fraud Detector 主控台中建立實體類型、使用put-entity-type命令、PutEntityTypeAPI 或使用AWS SDK for Python (Boto3). 下列範例使用`customer`了 SDK to Python (Boto3) 來建立實體類型。如果您要建立與事件類型相關聯的實體類型以訓練詐騙偵測模型，請使用事件資料集中適合您使用案例的實體類型。

使用 Amazon Fraud Detector 主控台建立實體類型

建立實體類型，

1. 開啟AWS管理主控台並登入您的帳戶。
2. 導覽至 Amazon Fraud Detector，在左側導覽中選擇「實體」，然後選擇「建立」。
3. 在 [建立實體] 頁面中，輸入 customer 做為實體類型名稱。選擇性輸入實體的描述。
4. 選擇 Create entity (建立實體)。

使用建立實體類型AWS SDK for Python (Boto3)

下列AWS SDK for Python (Boto3)程式碼範例會使用`PutEntityType` API 建立實體類型`customer`。如果您要建立與事件類型相關聯的實體類型以訓練詐騙偵測模型，請使用事件資料集中適合您使用案例的實體。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.put_entity_type(
name = 'customer',
description = 'customer'
```

```
)
```

刪除實體類型

在 Amazon Fraud Detector 中，無法刪除包含在事件類型中的實體類型。您必須先刪除與實體相關聯的事件類型，然後刪除實體類型。

刪除實體類型時，Amazon Fraud Detector 會永久刪除該實體類型，且資料不會再儲存在 Amazon Fraud Detector 中。

您可以在 Amazon Fraud Detector 主控台中刪除實體類型、使用delete-entity-type命令、DeleteEntityTypeAPI 或使用AWS SDK for Python (Boto3)

在 Amazon Fraud Detector 主控台中刪除實體類型

若要刪除實體類型，

1. 登入，開啟位於 https://console.aws.amazon.com/frauddetector 的 Amazon Fraud Detector 主控台。AWS Management Console
2. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇「資源」，然後選擇「實體」。
3. 選擇想要刪除的實體類型。
4. 選擇 動作，然後選擇 刪除。
5. 輸入實體類型名稱，然後選擇 [刪除實體類型]。

使用刪除實體類型AWS SDK for Python (Boto3)

下列AWS SDK for Python (Boto3)範例程式碼會刪除使用 DeleteEntityTypeAPI 的實體類型客戶。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.delete_entity_type (

name = 'customer'

)
```

使用管理 Amazon Fraud Detector 資源AWS CloudFormation

Amazon Fraud Detector 的模型並對這些資源進行設定。AWS CloudFormation您可以建立一個範本，描述所有您想要的 Amazon FraFraud Detector 的資源 (例如偵測器和標籤)，會為您AWS CloudFormation佈建和設定這些資源。 EntityType EventType您可以重複使用該範本，在多個 AWS 帳戶和區域內重複佈建和設定資源。

使用 AWS 無需額外收費 CloudFormation。

建立 Amazon FFraud Detector 範本

若要佈建和設定 Amazon FraFraud Detector 的資源，您必須了解AWS CloudFormation範本。範本是以 JSON 或 YAML 格式化的文本檔案。而您亦可以透過這些範本的說明，了解欲在 AWS CloudFormation 堆疊中佈建的資源。如果您不熟悉 JSON 或 YAML，您可以使用 AWS CloudFormation Designer 協助您開始使用 AWS CloudFormation 範本。如需詳細資訊，請參閱 AWS CloudFormation 使用者指南中的什麼是 AWS CloudFormation Designer？。

您也可以使用AWS CloudFormation範本建立、更新和刪除 Amazon FraFraud Detector。如需詳細資訊，包括資源的 JSON 和 YAML 範本範本範例，請參閱AWS CloudFormation使用者指南中的 Amazon Fraud Detector 資源類型參考。

如果您已在使用 CloudFormation，則無需管理其他 IAM 政策或 CloudTrail 記錄。

管理 Amazon Fraud Detector

您可以透過 CloudFormation 主控台或透過 AWS CLI 建立、更新和刪除 Amazon Fraud Detector 堆疊。

若要建立堆疊，您必須有一個範本說明 AWS CloudFormation 會在您堆疊中包含的資源。您也可以將已建立的 Amazon Fraud Detector 資源匯入到新的或現有的堆疊中，將已建立的 Amazon 詐騙偵測器資源匯入 CloudFormation 管理中。

如需管理堆疊的詳細說明，請參閱AWS CloudFormation使用者指南，瞭解如何建立、更新和刪除堆疊。

組織您的 Amazon Fraud Detector

組織AWS CloudFormation堆疊的方式完全由您決定。通常，最佳做法是按生命週期和所有權組織堆棧。這表示依資源變更頻率或負責更新資源的團隊來分組資源。

您可以選擇通過為每個檢測器及其檢測邏輯（例如規則，變量等）創建一個堆棧來組織堆棧。如果您正在使用其他服務，則應考慮是否要將 Amazon Fraud Detector 資源與其他服務的資源堆疊在一起。例如，您可以建立包含 Kinesis 資源的堆疊，以協助收集資料，以及處理資料的 Amazon Fraud Detector 資源。這可以是確保您所有欺詐團隊的產品一起工作的有效方法。

了解 Amazon Fraud Detec CloudFormation tor

除了所有 CloudFormation 範本中可用的標準參數之外，Amazon Fraud Detector 還引入了兩個額外參數，協助您管理部署行為。如果您不包括這些參數中的一個或兩個參數， CloudFormation 將使用如下所示的預設值。

參數	值	預設值
DetectorVersionStatus	活動：將新的/更新的檢測器版本設置為活動狀態 草稿：將新的/更新的檢測器版本設置為草稿狀態	草案
內嵌	TRUE： CloudFormation 允許在建立/更新/刪除資源。 FALSE： CloudFormation 允許驗證對象是否存在，但不對對對象進行任何更改。	TRUE

Amazon FraFraud Detector 的AWS CloudFormation範本

以下是用於管理偵測器和AWS CloudFormation相關聯的偵測器和相關聯的偵測器和相關聯的偵測器和

```
# Simple Detector resource containing inline Rule, EventType, Variable, EntityType and
 Label resource definitions
Resources:
  TestDetectorLogicalId:
    Type: AWS::FraudDetector::Detector
    Properties:
      DetectorId: "sample_cfn_created_detector"
      DetectorVersionStatus: "DRAFT"
      Description: "A detector defined and created in a CloudFormation stack!"

      Rules:
```

```
      - RuleId: "over_threshold_investigate"
        Description: "Automatically sends transactions of $10000 or more to an
investigation queue"
        DetectorId: "sample_cfn_created_detector"
        Expression: "$amount >= 10000"
        Language: "DETECTORPL"
        Outcomes:
          - Name: "investigate"
            Inline: true
      - RuleId: "under_threshold_approve"
        Description: "Automatically approves transactions of less than $10000"
        DetectorId: "sample_cfn_created_detector"
        Expression: "$amount <10000"
        Language: "DETECTORPL"
        Outcomes:
          - Name: "approve"
            Inline: true
    EventType:
      Inline: "true"
      Name: "online_transaction"
      EventVariables:
        - Name: "amount"
          DataSource: 'EVENT'
          DataType: 'FLOAT'
          DefaultValue: '0'
          VariableType: "PRICE"
          Inline: 'true'
      EntityTypes:
        - Name: "customer"
          Inline: 'true'
      Labels:
        - Name: "legitimate"
          Inline: 'true'
        - Name: "fraudulent"
          Inline: 'true'
```

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》https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html
- AWS CloudFormation API 參考
- 《AWS CloudFormation 命令列介面使用者指南》https://docs.aws.amazon.com/cloudformation-cli/latest/userguide/what-is-cloudformation-cli.html

詐騙預測

您可以使用 Amazon Fraud Detector 即時取得單一事件的詐騙預測，或離線取得一組事件的詐騙預測。若要針對單一事件或一組事件產生詐騙預測，您需要向 Amazon Fraud Detector 提供下列資訊：

- 詐騙預測邏輯
- 事件中繼資

詐騙偵測邏輯

詐騙預測邏輯會使用一或多個規則來評估與事件相關聯的資料，然後提供結果和詐騙預測分數。您可以使用下列元件建立詐騙預測邏輯：

- 事件類型-定義事件的結構
- 模型-定義預測欺詐的算法和數據要求
- 變量-表示與事件相關聯的數據元素
- 規則-指示 Amazon Fraud Detector 如何在詐騙預測期間解譯變數值
- 結果-詐騙預測產生的結果
- 偵測器版本-包含特定事件的詐騙預測邏輯

如需用於建立詐騙偵測邏輯之元件的詳細資訊，請參閱 Amazon Fraud Detector 概念。在開始生成欺詐預測之前，請確保您已創建並發布包含欺詐預測邏輯的檢測器版本。您可以使用 Fraud Detector 主控台或 API 建立和發佈偵測器版本。如需使用主控台的說明，請參閱「」。有關使用 API 的說明，請參閱創建檢測器版本。

事件元數據

事件元數據提供了正在評估的事件的詳細信息。您要評估的每個事件都必須包含與檢測器版本關聯的事件類型中的每個變量的值。此外，事件中繼資料必須包含下列各項：

- 事件識別碼 — 事件的識別元。例如，如果您的活動是線上交易，EVENT_ID 可能是提供給客戶的交易參考編號。

  關於事件 ID 的重要注意事項

  - 該事件必須是唯一的

- 應該代表對您的業務有意義的信息
- 必須滿足正則表達式模式：`^[0-9a-z_-]+$.`
- 必須保存。EVENT_ID 是事件的參考，用於對事件執行操作，例如刪除事件。
- 不建議將時間戳記附加到 EVENT_ID，因為這可能會導致以後您想要更新事件時發生問題，因為您需要提供完全相同的 EVENT_ID。

- ENTITY_TYPE — 執行事件的實體，例如商家或客戶。
- ENTITY_ID-執行事件之實體的識別碼。ENTITY_ID 必須滿足以下規則運算式模`^[0-9a-z_-]+$`式：如果 ENTITY_ID 在評估時不可用，請傳遞未知的字符串。
- 事件時間戳記-事件發生時的時間戳記。時間戳記必須是 ISO 8601 標準 (世界標準時間戳記)。

實時預測

您可以通過調用`GetEventPrediction` API 實時評估在線活動是否有欺詐。您可以在每個要求中提供有關單一事件的資訊，並根據與指定偵測器相關聯的詐騙預測邏輯同步接收模型分數和結果。

實時欺詐預測的工作原理

`GetEventPrediction`API 使用指定的偵測器版本來評估為事件提供的事件中繼資料。在評估期間，Amazon Fraud Detector 會先為新增至偵測器版本的模型產生模型分數，然後將結果傳遞至規則以進行評估。規則會依規則執行模式指定執行 (請參閱建立偵測器版本)。作為回應的一部分，Amazon Fraud Detector 提供模型分數以及與相符規則相關的任何結果。

獲取實時欺詐預測

要獲得實時欺詐預測，請確保您已創建並發布包含欺詐預測模型和規則的檢測器，或者只是一個規則集。

您可以使用AWS命令列界面 (AWSCLI) 或其中一個 Amazon Fraud Detector SDK 呼叫 GetEventPredictionAPI 作業，即時取得事件的詐騙預測。

若要使用 API，請在每個請求中提供單一事件的資訊。作為請求的一部分，您必須指`detectorId`定 Amazon Fraud Detector 將用於評估事件。您可以選擇指定「」`detectorVersionId`。如果`detectorVersionId`未指定，Amazon Fraud Detector 將使用偵測器的`ACTIVE` 版本。

您可以選擇性地傳送資料以呼叫 SageMaker 模型，方法是在欄位中傳遞資料`externalModelEndpointBlobs`。

使用以下方式取得詐騙預測AWS SDK for Python (Boto3)

若要產生詐騙預測，請呼叫GetEventPrediction API。以下範例假設您已完成B 部分：產生詐騙預測。作為回應的一部分，您將收到模型分數以及任何匹配的規則和相應的結果。您可以在aws-fraud-detector-samples GitHub 儲存庫中找到其他GetEventPrediction要求範例。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.get_event_prediction(
detectorId = 'sample_detector',
eventId = '802454d3-f7d8-482d-97e8-c4b6db9a0428',
eventTypeName = 'sample_registration',
eventTimestamp = '2020-07-13T23:18:21Z',
entities = [{'entityType':'sample_customer', 'entityId':'12345'}],
eventVariables = {
    'email_address' : 'johndoe@exampledomain.com',
    'ip_address' : '1.2.3.4'
}
)
```

批次預測

您可以在 Amazon Fraud Detector 中使用批次預測任務，取得一組不需要即時評分的事件預測。例如，您可以建立批次預測工作以離線執行proof-of-concept，或回溯評估每小時、每天或每週的事件風險。

您可以使用 Amazon Fraud Detector 主控台建立批次預測任務，或使用AWS命令列界面 (AWSCLI) 或其中一個 Amazon Fraud Detector 開發套件呼叫 CreateBatchPredictionJobAPI 操作。

主題

- 批次預測如何運作
- 輸入和輸出檔案
- 取得批次預測
- 有關角色的指南
- 取得批次詐騙預測 AWS SDK for Python (Boto3)

批次預測如何運作

CreateBatchPredictionJobAPI 操作使用指定的偵測器版本，根據 Amazon S3 儲存貯體中輸入 CSV 檔案中提供的資料進行預測。接著，API 接著會將產生的 CSV 檔案傳回 S3 儲存貯體。

Batch 預測工GetEventPrediction作會以與作業相同的方式計算模型評分和預測結果。與建立批次預測工作類似，您必須先建立事件類型，選擇性地訓練模型，然後建立用於評估批次工作中事件的偵測器版本。GetEventPrediction

批次預測工作評估的事件風險評分的定價與 GetEventPrediction API 建立分數的定價相同。如需詳細資訊，請參閱 Amazon Fraud Detector 定價。

您一次只能執行一個批次預測工作。

輸入和輸出檔案

輸入 CSV 檔案應包含與所選偵測器版本相關聯的事件類型相符的標頭。輸入資料檔案的大小上限為 1GB。活動數量將根據您的活動規模而有所不同。

Amazon Fraud Detector 會在與輸入檔案相同的儲存貯體中建立輸出檔案，除非您為輸出資料指定不同的位置。輸出檔案包含來自輸入檔案的原始資料和以下附加欄：

- MODEL_SCORES— 詳細說明與所選檢測器版本相關聯的每個模型中事件的模型分數。
- OUTCOMES— 詳細說明由所選檢測器版本及其規則評估的事件結果。
- STATUS— 指示是否已成功評估事件。如果未成功評估事件，此欄會顯示失敗的原因代碼。
- RULE_RESULTS— 以規則執行模式為基礎的所有符合規則的清單。

取得批次預測

下列步驟假設您已建立事件類型、使用該事件類型 (選用) 訓練模型，並為該事件類型建立偵測器版本。

取得批次預測

1. 登入，AWS Management Console並前往 https://console.aws.amazon.com/frauddetector 開啟 Amazon Fraud Detector 主控台。
2. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇「Batch 預測」，然後選擇「新增批次預測」。

3. 在 Job 名稱中，指定批次預測工作的名稱。如果您未指定名稱，Amazon Fraud Detector 會隨機產生任務名稱。
4. 在偵測器中，選擇此批次預測的偵測器。
5. 在偵測器版本中，選擇此批次預測的偵測器版本。您可以選擇任何狀態的檢測器版本。如果您的偵測器`Active`狀態為偵測器版本，則會自動選取該版本，但您也可以視需要變更此選項。
6. 在 IAM 角色中，選擇或建立對您的輸入和輸出 Amazon S3 儲存貯體具有讀寫存取權限的角色。如需詳細資訊，請參閱 有關角色的指南。

   若要取得批次預測，呼叫`CreateBatchPredictionJob`作業的 IAM 角色必須具有輸入 S3 儲存貯體的讀取權限，以及對輸出 S3 儲存貯體的寫入許可。如需儲存貯體許可的詳細資訊，請參閱 Amazon S3 使用者指南中的使用者政策範例。
7. 在輸入資料位置中，指定輸入資料的 Amazon S3 位置。如果您希望輸出檔案位於不同的 S3 儲存貯體，請選取單獨的輸出資料位置，並為輸出資料提供 Amazon S3 位置。
8. (選擇性) 建立批次預測工作的標籤。
9. 選擇 Start (啟動)。

   Amazon Fraud Detector 會建立批次預測任務，而任務的狀態為`In progress`。Batch 預測工作處理時間會因事件數量和偵測器版本配置而有所不同。

若要停止正在進行的批次預測工作，請移至批次預測工作詳細資訊頁面，選擇 [動作]，然後選擇 [停止批次預測]。如果停止批次預測工作，將不會收到該工作的任何結果。

批次預測任務的狀態變更為時`Complete`，您可以從指定的輸出 Amazon S3 儲存貯體擷取任務的輸出。輸出檔案的名稱格式為`batch prediction job name_file creation timestamp_output.csv`。例如，工作的輸出檔案`mybatchjob`為`mybatchjob_1611170650_output.csv`。

若要搜尋由批次預測任務評估的特定事件，請在 Amazon Fraud Detector 主控台的左側導覽窗格中選擇搜尋過去的預測。

若要刪除已完成的批次預測工作，請移至批次預測工作詳細資訊頁面，選擇 [動作]，然後選擇 [刪除批次預測]。

有關角色的指南

若要取得批次預測，呼叫`CreateBatchPredictionJob`作業的 IAM 角色必須具有輸入 S3 儲存貯體的讀取權限，以及對輸出 S3 儲存貯體的寫入許可。如需有關儲存貯體權限的詳細資訊，請參閱《Amazon S3

使用者指南》中的使用者政策範例 在 Amazon Fraud Detector 主控台上，您有三個選項可選擇 Batch 預測的 IAM 角色：

1. 在建立新的 Batch 預測工作時建立角色。
2. 選取您先前在 Amazon Fraud Detector 主控台建立的現有 IAM 角色。執行此步驟之前，請務必將`S3:PutObject`權限新增至角色。
3. 為先前建立的 IAM 角色輸入自訂 ARN。

如果您收到與 IAM 角色相關的錯誤，請驗證下列項目：

1. 您的 Amazon S3 儲存貯體與您的偵測器位於相同的區域。
2. 您使用的 IAM 角色具有輸入 S3 儲存貯體的`s3:GetObject`許`s3:PutObject`可，以及輸出 S3 儲存貯體的許可。
3. 您使用的 IAM 角色具有服務主體的信任政策`frauddetector.amazonaws.com`。

取得批次詐騙預測 AWS SDK for Python (Boto3)

以下範例會顯示 CreateBatchPredictionJobAPI 的範例請求。批次預測工作必須包含下列現有資源：偵測器、偵測器版本和事件類型名稱。下列範例假設您已建立事件類型`sample_registration``sample_detector`、偵測器和偵測器版本`1`。

```
import boto3
fraudDetector = boto3.client('frauddetector')

fraudDetector.create_batch_prediction_job (
   jobId = 'sample_batch',
   inputPath = 's3://bucket_name/input_file_name.csv',
   outputPath = 's3://bucket_name/',
   eventTypeName = 'sample_registration',
   detectorName = 'sample_detector',
   detectorVersion = '1',
   iamRoleArn = 'arn:aws:iam::**:role/service-role/AmazonFraudDetector-DataAccessRole-
**'
)
```

預測說明

預測說明可深入瞭解每個事件變數如何影響模型的詐騙預測分數，並自動產生作為詐騙預測的一部分。每個欺詐預測都具有 1 到 1000 之間的風險評分。預測說明提供每個事件變數對風險評分影響的詳細資訊，其中包括數量級別 (0-5，5 為最高) 和方向 (驅動器得分較高或更低)。您也可以針對下列工作使用預測說明：

- 當事件被標記為待審核時，識別手動反對期間的最高風險指標。
- 縮小導致誤判預測的根本原因（例如，合法事件的高風險評分）。
- 分析事件資料中的詐騙模式，並偵測資料集中的偏差 (如果有的話)。

> **Important**
>
> 預測說明會自動產生，且僅適用於 2021 年 6 月 30 日或之後訓練的模型。若要接收 2021 年 6 月 30 日之前訓練過的模型的預測說明，請重新訓練這些模型。

預測說明會針對用來訓練模型的每個事件變數提供下列一組值。

相對影響

提供變數對詐騙預測分數影響程度的視覺化參考。相對影響值包括星級評級（0-5，5 為最高）和欺詐風險的方向（增加/減少）影響。

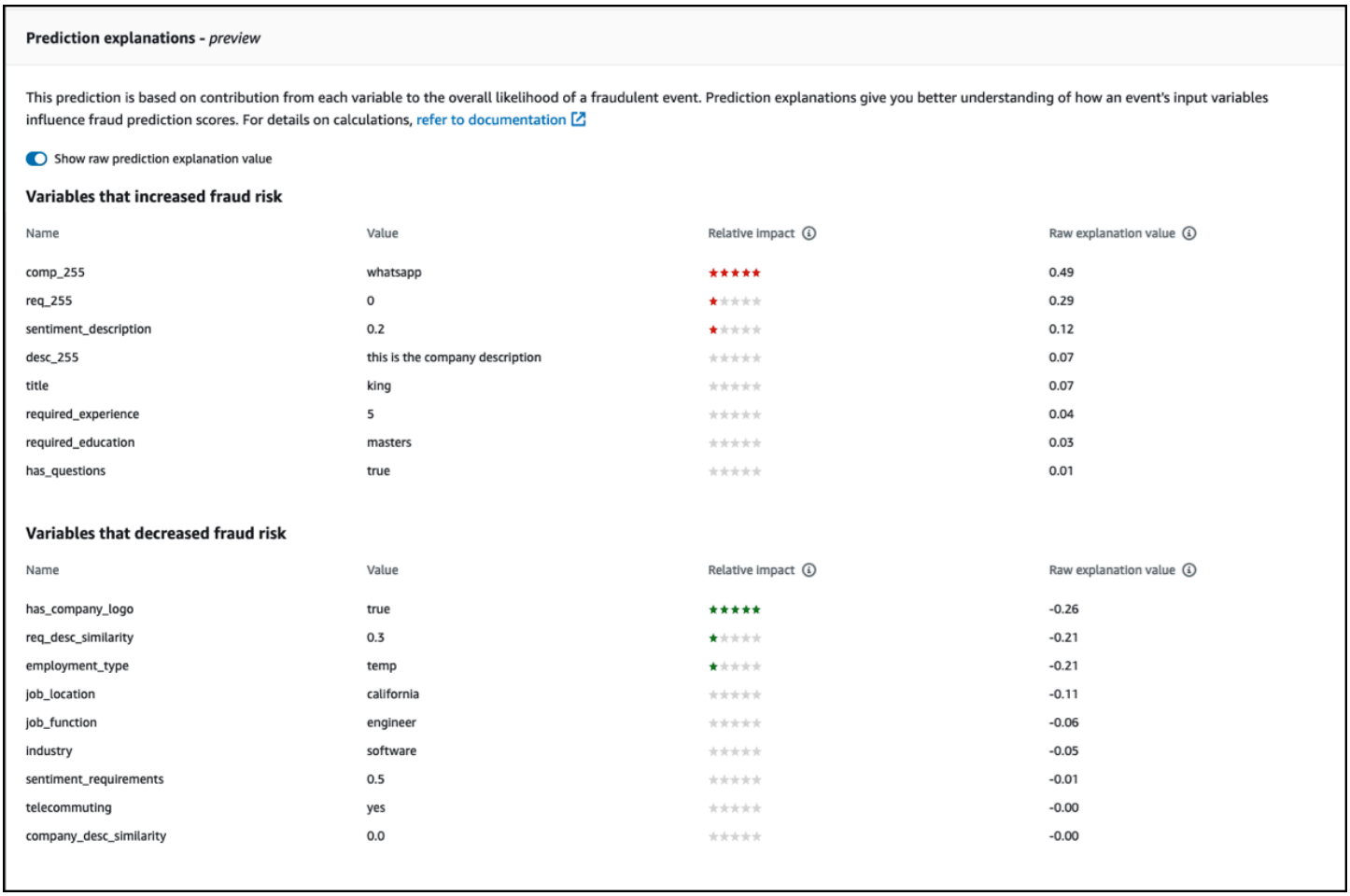
- 增加欺詐風險的變量由紅色星星表示。紅色星星的數量越高，變量越高，欺詐分數越高，欺詐的可能性就越高。
- 降低欺詐風險的變量由綠色星星表示。綠色起始次數越多，變量就越降低欺詐風險評分並降低欺詐的可能性。
- 所有變量的零星表明，沒有任何變量本身的變量顯著改變了欺詐風險。

原始說明值

提供表示為欺詐日誌賠率的原始、未解釋的價值。這些值通常介於 -10 到 +10 之間，但範圍從-無窮大到 + 無窮大。

- 正值表示變數會提高風險分數。
- 負值表示變數會降低風險評分。

在 Amazon Fraud Detector 主控台中，預測說明值顯示如下。彩色星級評等和對應的原始數值可讓您輕鬆查看變數之間的相對影響。



Prediction explanations - *preview*

This prediction is based on contribution from each variable to the overall likelihood of a fraudulent event. Prediction explanations give you better understanding of how an event's input variables influence fraud prediction scores. For details on calculations, refer to documentation

Show raw prediction explanation value

Variables that increased fraud risk

Name	Value	Relative impact	Raw explanation value
comp_255	whatsapp	★★★★★	0.49
req_255	0	★☆☆☆☆	0.29
sentiment_description	0.2	★☆☆☆☆	0.12
desc_255	this is the company description	☆☆☆☆☆	0.07
title	king	☆☆☆☆☆	0.07
required_experience	5	☆☆☆☆☆	0.04
required_education	masters	☆☆☆☆☆	0.03
has_questions	true	☆☆☆☆☆	0.01

Variables that decreased fraud risk

Name	Value	Relative impact	Raw explanation value
has_company_logo	true	★★★★★	-0.26
req_desc_similarity	0.3	★☆☆☆☆	-0.21
employment_type	temp	★☆☆☆☆	-0.21
job_location	california	☆☆☆☆☆	-0.11
job_function	engineer	☆☆☆☆☆	-0.06
industry	software	☆☆☆☆☆	-0.05
sentiment_requirements	0.5	☆☆☆☆☆	-0.01
telecommuting	yes	☆☆☆☆☆	-0.00
company_desc_similarity	0.0	☆☆☆☆☆	-0.00

檢視預測說明

產生詐騙預測後，您可以在 Amazon Fraud Detector 主控台中檢視預測說明。若要使用 AWS SDK 中的 API 檢視預測說明，您必須先呼叫 `ListEventPrediction` API 以取得事件的預測時間戳記，然後呼叫 `GetEventPredictionMetadata` API 以取得預測說明。

使用 Amazon Fraud Detector 主控台檢視預測說明

若要使用主控台檢視預測說明，

1. 開啟主AWS控台並登入您的帳戶。導航到 Amazon Fraud Detector。
2. 在左側導覽窗格中，選擇 [搜尋過去的預測]。
3. 使用「性質」、「運算子」和「值」篩選來選取您要檢閱的預測。
4. 在頂端篩選器窗格中，請務必選取產生您要檢閱之預測的時段。

5. 「結果」窗格會顯示在指定時段內產生的所有預測清單。按一下預測的事件 ID 以檢視預測說明。
6. 向下捲動至「預測說明」窗格。
7. 將 [顯示原始預測說明值] 按鈕設定為開啟，以檢視所有變數的原始預測說明值。

使用適用於 Python 的 AWS 開發套件 (Boto3) 檢視預測說明

下列範例顯示使用`ListEventPredictions`和 AWS SDK 中的 `GetEventPredictionMetadata` API 檢視預測說明的範例要求。

範例 1：使用 **`ListEventPredictions`** API 取得最近預測的清單

```
import boto3
fraudDetector = boto3.client('frauddetector')
fraudDetector.list_event_predictions(
  maxResults = 10,
  predictionTimeRange = {
     end_time: '2022-01-13T23:18:21Z',
     start_time: '2022-01-13T20:18:21Z'
    }
 )
```

範例 2；使用 **`ListEventPredictions`** API 取得事件類型「註冊」的過去預測清單

```
import boto3
fraudDetector = boto3.client('frauddetector')
fraudDetector.list_event_predictions(
   eventType = {
      value = 'registration'
    }
   maxResults = 70,
   nextToken = "10",
   predictionTimeRange = {
     end_time: '2021-07-13T23:18:21Z',
     start_time: '2021-07-13T20:18:21Z'
    }
 )
```

範例 3：取得在指定時段內使用 **`GetEventPredictionMetadata`** API 產生之指定事件 ID、事件類型、偵測器 ID 和偵測器版本 ID 的過去預測詳細資訊。

針對此要求的predictionTimestamp指定是透過先呼叫 ListEventPredictions API 來取得。

```
import boto3
fraudDetector = boto3.client('frauddetector')
fraudDetector.get_event_prediction_metadata (
   detectorId = 'sample_detector',
   detectorVersionId = '1',
   eventId = '802454d3-f7d8-482d-97e8-c4b6db9a0428',
   eventTypeName = 'sample_registration',
   predictionTimestamp = '2021-07-13T21:18:21Z'
 )
```

了解預測解釋的計算方式

Amazon Fraud Detector 使用 SHAP (ShapEley 加法解釋)，透過計算用於模型訓練之每個事件變數的原始說明值來說明個別事件預測。產生預測時，模型會計算原始說明值，做為分類演算法的一部分。這些原始說明值代表每個輸入對欺詐賠率對數的貢獻。使用映射將原始解釋值（從無窮大到 + 無窮大）轉換為相對衝擊值（-5 到 +5）。從原始解釋值得出的相對影響值代表欺詐（正）或合法（負面）的機率增加的次數，使得預測解釋更容易理解。

Amazon 欺 Fraud Detector 的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。若要了解適用於 Amazon Fraud Detector 的合規計劃，請參閱合規計劃 AWS 服務範。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用 Amazon Fraud Detector 時套用共同責任模型。下列主題說明如何設定 Amazon Fraud Detector，以符合安全和合規目標。您也會學到如何使用其他可協助您監控和保護 Amazon Fraud Detector 資源的 AWS 服務。

主題

Amazon Fraud Detector 中的資料保護

AWS 共同責任模型適用於 Amazon Fraud Detector 中的資料保護。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API 或 AWS 開發套件 AWS 服務 使用 Amazon Fraud Detector 或其他使用時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

加密靜態資料

Amazon Fraud Detector 會使用您選擇的加密金鑰來加密靜態資料。您可以選擇下列其中之一：

- AWS 擁有的 KMS 金鑰。如果您未指定加密金鑰，預設情況下，您的資料會使用此金鑰加密。
- 客戶管理的 KMS 金鑰。您可以使用金鑰原則來控制對客戶受管 KMS 金鑰的存取。如需建立和管理客戶受管 KMS 金鑰的相關資訊，請參閱金鑰管理。

加密傳輸中的資料

Amazon Fraud Detector 會將資料從您的帳戶複製出來，並在內部 AWS 系統中進行處理。根據預設，Amazon Fraud Detector 會使用 TLS 1.2 搭配 AWS 憑證來加密傳輸中的資料。

金鑰管理

Amazon Fraud Detector 會使用下列其中一種金鑰來加密您的資料：

- AWS 擁有的 KMS 金鑰。此為預設值。
- 客戶管理的 KMS 金鑰。

建立客戶受管 KMS 金鑰

您可以使用 KMS 主控台或 CreateKeyAPI 建立客戶受管 AWS KMS 金鑰。創建密鑰時，請確保您，

- 選取對稱加密客戶受管 KMS 金鑰，Amazon Fraud Detector 不支援非對稱 KMS 金鑰。如需詳細資訊，請參閱金鑰管理服務開發人員指南 AWS KMS中的非對稱金 AWS 鑰。
- 建立單一區域 KMS 金鑰。Amazon Fraud Detector 不支援多區域 KMS 金鑰。如需詳細資訊，請參閱金鑰管理服務開發人員指南 AWS KMS中的多區域金鑰。 AWS
- 提供下列金鑰政策，以授與 Amazon Fraud Detector 使用金鑰的許可。

```
        {
    "Effect": "Allow",
    "Principal": {
        "Service": "frauddetector.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
    ],
    "Resource": "*"
}
```

如需金鑰原則的相關資訊，請參閱金鑰管理服務開發人員指南中的使用 AWS KMS 中的金 AWS 鑰原則。

使用客戶代管的 KMS 金鑰加密資料

使用 Amazon Fraud Detector 的 PutKMS EncryptionKey API，使用客戶受管的 KMS 金鑰加密您的 Amazon 詐騙偵測器靜態資料。您可以隨時使用 `PutKMSEncryptionKey` API 變更加密設定。

關於加密資料的重要備註

- 設定客戶受管 KMS 金鑰後產生的資料會加密。在設定客戶受管 KMS 金鑰之前產生的資料將保持未加密狀態。

- 如果變更客戶管理的 KMS 金鑰，使用先前加密設定加密的資料將不會重新加密。

檢閱資料

當您使用客戶受管 KMS 金鑰加密 Amazon Fraud Detector 資料時，使用此方法加密的資料無法使用 Amazon Fraud Detector 主控台的搜尋過去預測區域中的篩選器進行搜尋。若要確保完整的搜尋結果，請使用下列一或多個屬性來篩選結果：

- 事件 ID
- 評估時間戳
- 偵測器狀態
- 偵測器版本
- 模型版本
- 模型類型
- 規則評估狀態
- 規則執行模式
- 規則符合狀態
- 規則版本
- 可變資料來源

如果客戶受管 KMS 金鑰遭到刪除或排程刪除，您的資料可能無法使用。如需詳細資訊，請參閱刪除 KMS 金鑰。

Amazon Fraud Detector 和 VPC 端點介面 ()AWS PrivateLink

您可以透過建立介面 VPC 端點，在 VPC 和 Amazon Fraud Detector 之間建立私有連線。界面端點採用這種技術 AWS PrivateLink，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線的情況下私有存取 Amazon Fraud Detector API。VPC 中的執行個體不需要公有 IP 地址即可與 Amazon Fraud Detector API 進行通訊。您的 VPC 和 Amazon Fraud Detector 之間的流量不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個彈性網路介面表示。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的介面虛擬私人雲端端點 (AWS PrivateLink)。

Amazon Fraud Detector VPC 端點的注意事項

在為 Amazon Fraud Detector 設定介面 VPC 端點之前，請務必先查看 Amazon VPC 使用者指南中的界面端點屬性和限制。

Amazon Fraud Detector 支援從您的 VPC 呼叫其所有 API 動作。

Amazon Fraud Detector 支援 VPC 端點政策。依預設，允許透過端點完整存取 Amazon Fraud Detector。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用 VPC 端點控制對服務的存取。

為 Amazon Fraud Detector 建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI) 為 Amazon Fraud Detector 服務建立 VPC 端點。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面端點。

使用下列服務名稱為 Amazon Fraud Detector 建立 VPC 端點：

- com.amazonaws.*region*.frauddetector

如果您為端點啟用私有 DNS，則可以使用該區域的預設 DNS 名稱向 Amazon Fraud Detector 發出 API 請求，例如，`frauddetector.us-east-1.amazonaws.com`。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的透過介面端點存取服務。

為 Amazon Fraud Detector 建立 VPC 端點政策

您可以為 Amazon Fraud Detector 的介面 VPC 端點建立政策，以指定下列項目：

- 可執行動作的委託人
- 可執行的動作
- 可在其中執行動作的資源

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 VPC 端點控制服務的存取。

下列範例 VPC 端點政策指定允許所有具有 VPC 介面端點存取權的使用者存取名為的 Amazon Fraud Detector 偵測器。`my_detector`

```
{
  "Statement": [
      {
          "Action": "frauddetector:*Detector",
          "Effect": "Allow",
          "Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/
my_detector",
          "Principal": "*"
      }
  ]
}
```

在這個範例中，拒絕以下各項：

- 其他 Amazon Fraud Detector API 動作
- 調用 Amazon Fraud Detector API `GetEventPrediction`

> **Note**
>
> 在此範例中，使用者仍然可以從 VPC 外部採取其他 Amazon Fraud Detector API 動作。如需有關如何僅限於從 VPC 內進行 API 呼叫的資訊，請參閱Amazon Fraud Detector 身分型政策。

選擇不使用您的資料以改善服務

您提供用於訓練模型和產生預測的歷史事件資料僅用於提供和維護您的服務。此資料也可能用於改善 Amazon Fraud Detector 的品質。您的信任、隱私和內容的安全性是我們的首要任務，並確保我們的使用符合我們對您的承諾。如需詳細資訊，請參閱資料隱私權

您可以透過造訪 AWS Organizations 使用者指南中的 AI 服務退出政策頁面，選擇不讓事件資料用於開發或改善 Amazon F raud Detector 的品質，並按照其中說明的程序進行操作。

> **Note**
>
> 您的 AWS 帳戶必須由 AWS Organizations 集中管理，您才能使用退出政策。如果您尚未為 AWS 帳戶建立組織，請瀏覽建立和管理組織頁面，並按照其中說明的程序進行操作。

Amazon Fraud Detector 的身分識別和存取管理

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。AWS 服務 IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有許可) 來使用 Amazon Fraud Detector 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在 Amazon Fraud Detector 中所做的工作。

服務使用者 — 如果您使用 Amazon Fraud Detector 服務執行工作，則管理員會為您提供所需的登入資料和許可。當您使用更多 Amazon Fraud Detector 功能來完成工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Amazon Fraud Detector 中的功能，請參閱疑難排解 Amazon Fraud Detector 身分和存取。

服務管理員 — 如果您負責公司的 Amazon Fraud Detector 資源，您可能擁有 Amazon Fraud Detector 的完整存取權。判斷服務使用者應存取哪些 Amazon Fraud Detector 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何將 IAM 與 Amazon Fraud Detector 搭配使用，請參閱Amazon Fraud Detector 如何與 IAM 配合使。

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 Amazon Fraud Detector 存取權的詳細資訊。若要檢視可在 IAM 中使用的 Amazon Fraud Detector 以身分識別為基礎的政策範例，請參閱。Amazon Fraud Detector 身分型政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS 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驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用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。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 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。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 ACL，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原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon Fraud Detector 如何與 IAM 配合使

在您使用 IAM 管理 Amazon Fraud Detector 的存取權限之前，您應該瞭解哪些 IAM 功能可與 Amazon Fraud Detector 搭配使用。若要深入瞭解 Amazon Fraud Detector 和其他 AWS 服務如何與 IAM 搭配使用，請參閱 IAM 使用者指南中的與 IAM 搭配使用的AWS 服務。

主題

- Amazon Fraud Detector 身分型政策
- Amazon Fraud Detector 資源型政策
- 基於 Amazon Fraud Detector 的授權 Tags
- Amazon Fraud Detector IAM 角色

Amazon Fraud Detector 身分型政策

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。Amazon Fraud Detector 支援特定動作、資源和條件金鑰。若要了解您在 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 JSON 政策元素參考。

若要開始使用 Amazon Fraud Detector，我們建議您建立一個使用者，其存取權限僅限於 Amazon Fraud Detector 操作和所需許可。您可以視需要新增其他許可。下列政策提供使用 Amazon Fraud Detector 所需的權限：`AmazonFraudDetectorFullAccessPolicy`和`AmazonS3FullAccess`。如需使用這些政策設定 Amazon Fraud Detector 的詳細資訊，請參閱設置 Amazon Fraud Detector。

動作

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

Amazon Fraud Detector 中的政策動作在動作前使用下列前置詞：`frauddetector:`例如，若要使用 Amazon Fraud Detector `CreateRule` API 作業建立規則，請在政策中包含該`frauddetector:CreateRule`動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Amazon Fraud Detector 會定義自己的一組動作，說明您可以使用此服務執行的任務。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

```
"Action": [
      "frauddetector:action1",
      "frauddetector:action2"
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 `Describe` 文字的所有動作，請包含以下動作：

```
"Action": "frauddetector:Describe*"
```

若要查看 Amazon Fraud Detector 動作清單，請參閱 IAM 使用者指南中的 Amazon Fraud Detector 定義的動作。

資源

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

Amazon Fraud Detector 定義的資源類型會列出所有 Amazon Fraud Detector 資源 ARN。

例如，若要在陳述式中指定`my_detector`偵測器，請使用下列 ARN：

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/my_detector"
```

如需 ARN 格式的詳細資訊，請參閱 Amazon 資源名稱 (ARN) 和 AWS 服務命名空間。

若要指定屬於特定帳戶的所有偵測器，請使用萬用字元 (*)：

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/*"
```

某些 Amazon Fraud Detector 動作 (例如用於建立資源的動作) 無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (*)。

```
"Resource": "*"
```

若要查看 Amazon Fraud Detector 資源類型及其 ARN 的清單，請參閱 IAM 使用者指南中的 Amazon Fraud Detector 定義的資源。若要了解哪些動作可以指定每個資源的 ARN，請參閱 Amazon Fraud Detector 定義的動作。

條件索引鍵

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

Amazon Fraud Detector 會定義自己的一組條件金鑰，並支援使用某些全域條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱 IAM 使用者指南中的AWS 全域條件內容金鑰。

若要查看 Amazon Fraud Detector 條件金鑰清單，請參閱 IAM 使用者指南中的 Amazon Fraud Detector 的條件金鑰。若要了解您可以使用條件金鑰的動作和資源，請參閱 Amazon Fraud Detector 定義的動作。

範例

若要檢視 Amazon Fraud Detector 身分型政策的範例，請參閱。Amazon Fraud Detector 身分型政策範例

Amazon Fraud Detector 資源型政策

Amazon Fraud Detector 不支援以資源為基礎的政策。

基於 Amazon Fraud Detector 的授權 Tags

您可以將標籤附加到 Amazon Fraud Detector 資源，或將請求中的標籤傳遞給 Amazon Fraud Detector。若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

Amazon Fraud Detector IAM 角色

IAM 角色是您 AWS 帳戶中具有特定許可的實體。

使用臨時登入資料搭配 Amazon Fraud Detector

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫AssumeRole或等 AWS STS API 作業來取得臨時安全登入資料GetFederationToken。

Amazon Fraud Detector 支援使用臨時登入資料。

服務連結角色

服務連結角色可讓 AWS 服務存取其他服務中的資源，以代表您完成動作。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

Amazon Fraud Detector 不支援服務連結角色。

服務角色

此功能可讓服務代表您擔任服務角色。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務角色會出現在您的 帳戶，且由該帳戶所擁有。這表示 管理員可以變更此角色的許可。不過，這樣可能會破壞此服務的功能。

Amazon Fraud Detector 支援服務角色。

Amazon Fraud Detector 身分型政策範例

依預設，使用者和 IAM 角色沒有建立或修改 Amazon Fraud Detector 資源的權限。他們也無法使用 AWS Management Console AWS CLI、或 AWS API 執行工作。管理員必須建立 IAM 政策，授與使用

者和角色在指定資源上執行特定 API 操作所需的許可。管理員接著必須將這些政策連接至需要這些許可的使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 IAM 使用者指南中的在 JSON 索引標籤上建立政策。

主題

政策最佳實務

以身分識別為基礎的政策決定某人是否可以在您的帳戶中建立、存取或刪除 Amazon Fraud Detector 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access

Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

適用於 Amazon Fraud Detector 的 AWS 管理 (預先定義) 政策

AWS 透過提供由建立和管理的獨立 IAM 政策來解決許多常見使用案例 AWS。這些 AWS 受管理的政策會為常見使用案例授與必要的權限，因此您可以避免調查需要哪些權限。如需詳細資訊，請參閱AWS Identity and Access Management 管理使用者指南中的 AWS 受管政策。

Amazon Fraud Detector 專用的下列 AWS 受管政策 (您可以附加至帳戶中的使用者)：

`AmazonFraudDetectorFullAccess`：授予對 Amazon Fraud Detector 資源、動作和支援操作的完整存取權，包括：

- 列出並描述 Amazon 中的所有模型端點 SageMaker
- 列出帳戶中的所有 IAM 角色
- 列出所有 Amazon S3 存儲桶
- 允許 IAM 通過角色將角色傳遞給 Amazon Fraud Detector

此政策不提供不受限制的 S3 存取。如果您需要將模型訓練資料集上傳到 S3，也需要`AmazonS3FullAccess`受管政策 (或縮小範圍的自訂 Amazon S3 存取政策)。

您可以登入 IAM 主控台並依政策名稱進行搜尋，以檢閱政策的許可。您也可以建立自己的自訂 IAM 政策，以根據需要允許 Amazon Fraud Detector 動作和資源的許可。您可以將這些自訂政策連接至需要這些政策的 使用者或群組。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

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

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

允許完整存取 Amazon Fraud Detector 資源

下列範例可讓使用者 AWS 帳戶 完整存取所有 Amazon Fraud Detector 資源和動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "frauddetector:*"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

允許 Amazon Fraud Detector 資源的唯讀存取

在此範例中，您授與使用者對 Amazon Fraud Detector 資源的 AWS 帳戶 唯讀存取權。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "frauddetector:GetEventTypes",
                "frauddetector:BatchGetVariable",
                "frauddetector:DescribeDetector",
                "frauddetector:GetModelVersion",
                "frauddetector:GetEventPrediction",
                "frauddetector:GetExternalModels",
                "frauddetector:GetLabels",
                "frauddetector:GetVariables",
                "frauddetector:GetDetectors",
                "frauddetector:GetRules",
                "frauddetector:ListTagsForResource",
                "frauddetector:GetKMSEncryptionKey",
                "frauddetector:DescribeModelVersions",
                "frauddetector:GetDetectorVersion",
                "frauddetector:GetPrediction",
                "frauddetector:GetOutcomes",
                "frauddetector:GetEntityTypes",
                "frauddetector:GetModels"
            ],
            "Resource": "*"
        }
    ]
}
```

允許存取特定資源

在此資源層級政策範例中，您將 AWS 帳戶 存取所有動作和資源的權限授與使用者，但一個特定偵測器資源除外。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "frauddetector:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "frauddetector:*Detector"
            ],
            "Resource": "arn:${Partition}:frauddetector:${Region}:${Account}:detector/
${detector-name}"
        }
    ]
}
```

使用雙模式 API 時允許存取特定資源

Amazon Fraud Detector 提供雙重模式 get API，可同時作為「清單」和「描述」操作使用。如果沒有任何參數調用雙模式 API，則返回與您關聯的指定資源的列表 AWS 帳戶。使用參數調用時，雙模式 API 返回指定資源的詳細信息。資源可以是模型、變數、事件類型或實體類型。

雙模式 API 支援 IAM 政策中的資源層級許可。不過，只有在要求中提供一或多個參數時，才會套用資源層級權限。例如，如果使用者呼叫 GetVariablesAPI 並提供變數名稱，而且如果變數資源或變數名稱附加了 IAM 拒絕政策，則使用者將會收到`AccessDeniedException`錯誤訊息。如果使用者呼叫 `GetVariables` API 且未指定變數名稱，則會傳回所有變數，這可能會造成資訊洩漏。

若要允許使用者僅檢視特定資源的詳細資料，請在 IAM 拒絕`NotResource`政策中使用 IAM 政策元素。將此政策元素新增至 IAM Deny 政策後，使用者只能檢視`NotResource`區塊中指定之資源的詳細資料。如需詳細資訊，請參閱 IAM JSON 政策元素： NotResource在 IAM 使用者指南中。

下列範例政策可讓使用者存取 Amazon 詐騙偵測器的所有資源。不過，`NotResource`政策元素是用來將 GetVariablesAPI 呼叫限制為只有前置詞`user*`、`job_*`、和`var*`的變數名稱。

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

```
 "Statement": [
  {
    "Effect": "Allow",
    "Action": "frauddetector:*",
    "Resource": "*"
  },
 {
    "Effect": "Deny",
    "Action": "frauddetector:GetVariables",
    "NotResource": [
       "arn:aws:frauddetector:*:*:variable/user*",
       "arn:aws:frauddetector:*:*:variable/job_*",
       "arn:aws:frauddetector:*:*:variable/var*"
    ]
  }
 ]
}
```

回應

針對此範例原則，回應會出現下列行為：

- 不包含變數名稱的 GetVariables 呼叫會導致`AccessDeniedException`錯誤，因為要求會對應至 Deny 陳述式。
- 包含不允許的變數名稱的 GetVariables 呼叫會導致`AccessDeniedException`錯誤，因為變數名稱未對應至`NotResource`區塊中的變數名稱。例如，具有變數名稱的 GetVariables 呼叫會`email_address`導致錯`AccessDeniedException`誤。
- 如預期般傳回包含與`NotResource`區塊中變數名稱相符的變數名稱的 GetVariables 呼叫。例如，包含變數名稱的 GetVariables 呼叫會`job_cpa`傳回變`job_cpa`數的詳細資訊。

根據標籤限制存取

此範例政策示範如何根據資源標籤限制對 Amazon Fraud Detector 的存取。此範例假設：

- 在 AWS 帳戶 你的你已經定義了兩個不同的組，名為 Team1 和 Team2
- 您已建立四個偵測器
- 您想要允許 Team1 的成員在 2 個偵測器上進行 API 呼叫
- 您想要允許 Team2 的成員對其他 2 個偵測器進行 API 呼叫

控制對 API 呼叫的存取權 (範例)

1. 將包含金鑰Project和值的標籤新增A至 Team1 使用的偵測器。
2. 在 Team2 使用的偵測器中新增包含金鑰Project和值B的標籤。
3. 建立具有拒絕存取具有金鑰Project和值標籤的偵測器的ResourceTag條件的 IAM 政策B，並將該政策附加到 Team1。
4. 建立具有拒絕存取具有金鑰Project和值標籤的偵測器的ResourceTag條件的 IAM 政策A，並將該政策附加到 Team2。

以下是一個政策範例，該政策會拒絕任何 Amazon Fraud Detector 資源的特定動作，該資源的標籤含有鍵值Project且值為：B

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "frauddetector:*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",

      "Action": [

        "frauddetector:CreateModel",
        "frauddetector:CancelBatchPredictionJob",
        "frauddetector:CreateBatchPredictionJob",
        "frauddetector:DeleteBatchPredictionJob",
        "frauddetector:DeleteDetector"
      ],

      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "B"
        }
      }
    }
  ]
}
```

預防混淆代理人

當沒有執行動作權限的實體可能會強制更具權限的實體執行動作時，就會發生混淆的副問題。 AWS 如果您提供第三方（稱為跨帳戶）或其他 AWS 服務（稱為跨服務）訪問帳戶中的資源，則提供了可幫助您保護帳戶的工具。

當一個服務（呼叫服務）調用另一個服務（被調用的服務）時，可能會發生跨服務混淆的副問題。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了防止這種情況發生，您可以建立政策，以協助您使用已授予服務資源存取權的服務主體來保護所有服務的資料。

Amazon Fraud Detector 支援在您的許可政策中使用服務角色，以允許服務代表您存取其他服務的資源。角色需要兩個政策：指定允許承擔角色的主體的角色信任政策；以及指定角色可執行動作的許可政策。當服務代表您擔任角色時，必須允許服務主體執行角色信任政策中的 `sts:AssumeRole` 動作。當服務呼叫時`sts:AssumeRole`，會 AWS STS 傳回服務主體用來存取角色權限原則所允許之資源的一組暫時安全性登入資料。

為了避免跨服務混淆的副問題，Amazon Fraud Detector 建議在角色信任政策中使用`aws:SourceArn`和`aws:SourceAccount`全域條件上下文金鑰，將角色的存取限制為只有預期資源產生的請求。

會`aws:SourceAccount`指定帳號 ID，並`aws:SourceArn`指定與跨服務存取關聯之資源的 ARN。`aws:SourceArn`必須使用 ARN 格式來指定。在同一份保單聲明中使用時，請確保`aws:SourceAccount`和`aws:SourceArn`使用相同的帳戶 ID。

防範混淆代理人問題的最有效方法是使用 `aws:SourceArn` 全域條件內容索引鍵，以及資源的完整 ARN。如果您不知道資源的完整 ARN，或者您要指定多個資源，請針對 ARN 的未知部分使用萬用字元 (*) 的`aws:SourceArn`全域內容條件索引鍵。例如 `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`。如需可在許可政策中使用的 Amazon Fraud Detector 資源和動作的相關資訊，請參閱 Amazon Fraud Detector 的動作、資源和條件金鑰。

下列角色信任政策範例在`aws:SourceArn`條件金鑰中使用萬用字元 (*)，允許 Amazon Fraud Detector 存取與帳戶 ID 關聯的多個資源。

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

```
                "Principal": {
                "Service": [
                    "frauddetector.amazonaws.com"
                    ]
                },
                "Action": "sts:AssumeRole",
                "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                  "StringLike": {
                     "aws:SourceArn": "arn:aws:frauddetector:us-west-2:123456789012:*"
        }
      }
    }
  ]
}
```

下列角色信任政策允許 Amazon Fraud Detector 僅存取external-model資源。請注意「條件」區塊中的aws:SourceArn參數。資源限定詞是使用提供用於進行 PutExternalModel API 調用的模型端點構建的。

```
    {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "frauddetector.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:frauddetector:us-west-2:123456789012:external-
model/MyExternalModeldoNotDelete-ReadOnly"
        }
      }
```

```
    }
  ]
}
```

疑難排解 Amazon Fraud Detector 身分和存取

使用下列資訊協助您診斷和修正使用 Amazon Fraud Detector 和 IAM 時可能會遇到的常見問題。

主題

- 我無權在 Amazon Fraud Detector 中執行動作
- 我沒有授權執行 iam：PassRole
- 我想允許 AWS 帳戶以外的人員存取我的 Amazon Fraud Detector 資源
- Amazon Fraud Detector 無法承擔給定的角色

我無權在 Amazon Fraud Detector 中執行動作

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡管理員以尋求協助。您的管理員是為您提供簽署憑證的人員。

當使用mateojackson者嘗試使用主控台來檢視有關###的詳細資料，但沒有frauddetector:*GetDetectors*權限時，就會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 frauddetector:GetDetectors on resource: my-example-detector
```

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-detector* 動作存取 frauddetector:*GetDetectors* 資源。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的政策以允許您將角色傳遞給 Amazon Fraud Detector。

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。

當名為的 IAM 使用者marymajor嘗試使用主控台在 Amazon Fraud Detector 中執行動作時，會發生下列範例錯誤。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 系統管理員。您的管理員提供您的簽署憑證。

我想允許 AWS 帳戶以外的人員存取我的 Amazon Fraud Detector 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。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon Fraud Detector 是否支援這些功能，請參閱Amazon Fraud Detector 如何與 IAM 配合使。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策的差異。

Amazon Fraud Detector 無法承擔給定的角色

如果您收到 Amazon Fraud Detector 無法擔任指定角色的錯誤訊息，則必須更新指定角色的信任關係。透過將 Amazon Fraud Detector 指定為受信任的實體，服務可以擔任該角色。當您使用 Amazon Fraud Detector 建立角色時，會自動設定此信任關係。您只需要為非 Amazon Fraud Detector 建立的 IAM 角色建立此信任關係。

為 Amazon Fraud Detector 的現有角色建立信任關係

1. 開啟身分與存取權管理主控台 https://console.aws.amazon.com/iam/
2. 在導覽窗格中選擇 [角色]。
3. 選擇您要修改的角色名稱，然後選擇「信任關係」標籤。

4. 選擇編輯信任關係。
5. 在 Policy Document (政策文件) 下，貼上下列內容，然後選擇 Update Trust Policy (更新信任政策)。

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

Amazon Fraud Detector 中的記錄和監控

AWS 提供下列監控工具來觀看 Amazon Fraud Detector、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。如需有關的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南。
- AWS CloudTrail擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。若要取得更多資訊 CloudTrail，請參閱《AWS CloudTrail 使用指南》。

如需監控 Amazon Fraud Detector 的詳細資訊，請參閱監控 Amazon Fraud Detector。

Amazon Fraud Detector 的合規驗證

協力廠商稽核人員會評估 AWS 服務的安全性與合規性，作為多重 AWS 合規計畫的一部分，例如 SOC、PCI、FedRAMP 和 HIPAA。

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳做法。
- 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，例如 PCI DSS，滿足特定合規性架構所規定的入侵偵測需求。
- 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。

Amazon 欺 Fraud Detector 的彈性

AWS 全球基礎設施以 AWS 區域與可用區域為中心建置。AWS 區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援聯網相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴充能力，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 全球基礎設施。

Amazon Fraud Detector 的基礎設施安全

作為受管服務，Amazon Fraud Detector 受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取 Amazon Fraud Detector。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

監控 Amazon Fraud Detector

監控是維護 Amazon Fraud Detector 和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。AWS 提供下列監控工具來觀看 Amazon Fraud Detector、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- AWS CloudTrail擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

主題

用 Amazon 監控 Amazon Fraud Detector CloudWatch

您可以使用監控 Amazon Fraud Detector CloudWatch，該偵測器會收集原始資料並將其處理為可讀且近乎即時的指標。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

主題

使用 CloudWatch Amazon Fraud Detector 的指標。

要使用指標，您必須指定下列資訊：

- 測量結果命名空間。命名空間是 Amazon Fraud Detector 用來將其指標發佈到的 CloudWatch 容器。如果您使用 CloudWatch ListMetricsAPI 或列表指標命令來檢視 Amazon Fraud Detector 的指標，請`AWS/FraudDetector`為命名空間指定。

- 指標維度。維度是名稱-值配對，可協助您唯一識別量度，例如，DetectorId可以是維度名稱。指定量度維度是選擇性的。
- 指標名稱，例如 GetEventPrediction。

您可以使用 AWS Management Console、或 CloudWatch API 取得 Amazon Fraud Detector 的 AWS CLI監控資料。您也可以透過其中 CloudWatch 一個 Amazon AWS 軟體開發套件 (開發套件) 或 CloudWatch API 工具使用 API。控制台根據來自 CloudWatch API 的原始數據顯示一系列圖形。根據需求，您可能偏好使用顯示於主控台中的圖形或自 API 擷取的圖形。

下列清單顯示一些常見的指標用途。這些是協助您開始的建議，而不是完整清單。

我要如何？	相關指標
如何追蹤已執行的預測數量？	監控 GetEventPrediction 指標。
如何監控GetEventPrediction 錯誤？	使用GetEventPrediction5xxError 和指GetEventPrediction4xxError 標。
如何監控 GetEventPrediction 呼叫延遲？	使用 GetEventPredictionLatency 指標。

您必須擁有適當的 CloudWatch 許可，才能使用監控 Amazon Fraud Detector CloudWatch。如需詳細資訊，請參閱 Amazon 的身分驗證和存取控制 CloudWatch。

存取 Amazon Fraud Detector 指標

以下步驟說明如何使用 CloudWatch 主控台存取 Amazon Fraud Detector 指標。

檢視指標 (主控台)

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 選擇「指標」，選擇「所有指標」標籤，然後選擇「Fra ud Detector」。
3. 選擇指標維度。
4. 從清單中選擇所需指標，然後選擇圖形的期間。

建立警示

您可以建立 CloudWatch 警示，在警示狀態變更時傳送 Amazon 簡單通知服務 (Amazon SNS) 訊息。警示會在您指定的期間監看單一指標。警示會根據在數個期間與指定閾值相關的指標值，來執行一個或多個動作。此動作是傳送到 Amazon SNS 主題或 Auto Scaling 政策的通知。

警示只會呼叫持續狀態變更的動作。 CloudWatch 警報不會僅僅因為它們處於特定狀態而調用操作。狀態必須發生變更並維持一段指定的時間。

若要設定警示 (主控台)

1. 請登入 AWS Management Console 並開啟 CloudWatch 主控台，網址為 https://console.aws.amazon.com/cloudwatch/。
2. 在功能窗格中，選擇 [鬧鐘]，然後選擇 [建立鬧鐘]。這會開啟 [建立警示精靈]。
3. 選擇選取指標。
4. 在「所有指標」標籤中，選擇「Fra ud Detector」。
5. 選擇 [依偵測器 ID]，然後選擇GetEventPrediction量度。
6. 選擇 Graphed metrics (圖表化指標) 標籤。
7. 在 Statistic (統計資料) 中選擇 Sum (總和)。
8. 選擇選取指標。
9. 在「條件」中，選擇「靜態」做為「臨界值」類型，在「每當...」中選擇「更大」，然後輸入您選擇的最大值。選擇下一步。
10. 若要傳送警示到現有的 Amazon SNS 主題，請在傳送通知至：選項中選擇現有的 SNS 主題。若要設定新電子郵件訂閱清單的名稱和電子郵件地址，請選擇 [新增清單]。 CloudWatch 保存列表並將其顯示在字段中，以便您可以使用它來設置將 future 的警報。

   > **Note**
   >
   > 如果您使用新清單建立新的 Amazon SNS 主題，則必須先驗證電子郵件地址，才能收到預定的收件者收到通知。Amazon SNS 只會在警示進入警示狀態時才會傳送電子郵件。如果在驗證電子郵件地址之前發生此警示狀態變更，預定收件者將不會收到通知。

11. 選擇下一步。為鬧鐘新增名稱和可選描述。選擇下一步。
12. 選擇建立警示 。

Amazon Fraud Detector 指

Amazon Fraud Detector 會將下列指標傳送至 CloudWatch。所有測量結果都支援以下統計資料：AverageMinimum、Maximum、、Sum。

指標	描述
GetEventPrediction	GetEventPrediction API 要求的數目。 有效維度：DetectorID
GetEventPredictionLatency	從要求回應用戶端要求所花費的時間間隔。GetEventPrediction 有效維度：DetectorID 單位：毫秒
GetEventPrediction4XXError	Amazon Fraud Detector 傳回 4xx HTTP 回應碼的 GetEventPrediction 請求數目。對於每個 4xx 響應，將發送 1 個。 有效維度：DetectorID
GetEventPrediction5XXError	Amazon Fraud Detector 傳回 5xx HTTP 回應碼的 GetEventPrediction 請求數目。針對每個 5xx 回應，就會傳送 1 個。 有效維度：DetectorID
Prediction	預測的數量。如果成功，則傳送 1。 有效尺寸:DetectorID ，DetectorVersionID
PredictionLatency	預測作業所使用的時間間隔。 有效尺寸:DetectorID ，DetectorVersionID 單位：毫秒

指標	描述
PredictionError	Amazon Fraud Detector 遇到錯誤的預測次數。遇到錯誤時會傳送 1。 有效尺寸:DetectorID ，DetectorVersionID
VariableUsed	使用變數作為評估一部分的 GetEventPrediction 要求數目。 有效尺寸:DetectorID ,DetectorVersionID ，VariableName
VariableDefaultReturned	在事件屬性中不存在變數的 GetEventPrediction 要求數目，因此在評估期間會使用變數的預設值。 有效尺寸:DetectorID ,DetectorVersionID ，VariableName
RuleNotEvaluated	因為先前的規則相符而未評估規則的 GetEventPrediction 要求數目。 有效尺寸:DetectorID ,DetectorVersionID ，RuleID
RuleEvaluateTrue	規則觸發為 True 且傳回規則結果的 GetEventPrediction 要求數目。 有效尺寸:DetectorID ,DetectorVersionID ，RuleID
RuleEvaluateFalse	規則評估為 False 的 GetEventPrediction 要求數目。 有效尺寸:DetectorID ,DetectorVersionID ，RuleID
RuleEvaluateError	規則評估錯誤的 GetEventPrediction 要求數目 有效尺寸:DetectorID ,DetectorVersionID ，RuleID

指標	描述
OutcomeReturned	傳回指定結果的 GetEventPrediction 呼叫次數。 有效尺寸:DetectorID ,DetectorVersionID , OutcomeName
ModelInvocation (Amazon SageMaker model endpoint)	在評估過 GetEventPrediction 程中呼叫 SageMaker 模型端點的要求數目。 有效尺寸:DetectorID ,DetectorVersionID , ModelEndpoint
ModelInvocationError (Amazon SageMaker model endpoint)	呼叫的 SageMaker 模型端點在評估期間傳回錯誤的 GetEventPrediction 要求數目。 有效尺寸:DetectorID ,DetectorVersionID , ModelEndpoint
ModelInvocationLatency (Amazon SageMaker model endpoint)	從 Amazon Fraud Detector 檢視的匯入模型回應所花費的時間間隔。此間隔僅包含模型呼叫。 有效尺寸:DetectorID ,DetectorVersionID , ModelEndpoint 單位：毫秒
ModelInvocation	作為評估一部分叫用模型的 GetEventPrediction 要求數目。 有效尺寸:DetectorID ,DetectorVersionID ,ModelType , ModelID
ModelInvocationError	Amazon Fraud Detector 模型在評估期間傳回錯誤的 GetEventPrediction 請求數。 有效尺寸:DetectorID ,DetectorVersionID ,ModelType , ModelID

指標	描述
ModelInvocationLatency	從 Amazon Fraud Detector 檢視的 Amazon Fraud Detector 模型回應所花費的時間間隔。此間隔僅包含模型呼叫。 有效尺寸:DetectorID ,DetectorVersionID ,ModelType , ModelID 單位：毫秒

使用記錄 Amazon Fraud Detector API 呼叫 AWS CloudTrail

Amazon Fraud Detector 與服務整合在一起 AWS CloudTrail，可提供 Amazon Fraud Detector 中使用者、角色或 AWS 服務所採取的動作記錄的服務。 CloudTrail 將 Amazon Fraud Detector 的所有 API 呼叫擷取為事件，包括來自 Amazon Fraud Detector 主控台的呼叫，以及從程式碼到 Amazon Fraud Detector API 的呼叫。

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 Amazon Fraud Detector 的事件。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，您可以判斷向 Amazon Fraud Detector 提出的請求、提出請求的來源 IP 位址、提出請求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

Amazon Fraud Detector 信息 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。當 Amazon Fraud Detector 中發生活動時，該活動會與 CloudTrail 事件歷史記錄中的其他 AWS 服務事件一起記錄在事件中。您可以在帳戶中查看，搜索和下載最近的事 AWS 件。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

如需 AWS 帳戶中持續記錄事件 (包括 Amazon Fraud Detector 的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有 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，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄檔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 記錄檔並從多個帳戶接收 CloudTrail記錄檔

Amazon Fraud Detector 支援將每個動作 (API 操作) 記錄為 CloudTrail 日誌檔中的事件。如需詳細資訊，請參閱動作。

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：

- 該請求是否使用根或使用者憑證提出。
- 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。

了解 Amazon Fraud Detector 日誌檔項目

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，操作的日期和時間，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。

下列範例顯示示範`GetDetectors`作業的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "principal-id",
        "arn": "arn:aws:iam::user-arn",
        "accountId": "account-id",
        "accessKeyId": "access-key",
        "userName": "user-name"
    },
    "eventTime": "2019-11-22T02:18:03Z",
    "eventSource": "frauddetector.amazonaws.com",
    "eventName": "GetDetectors",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "source-ip-address",
```

```
    "userAgent": "aws-cli/1.11.16 Python/2.7.11 Darwin/15.6.0 botocore/1.4.73",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "request-id",
    "eventID": "event-id",
    "eventType": "AwsApiCall",
    "recipientAccountId": "recipient-account-id"
}
```

疑難排解

以下各節可協助您疑難排解使用 Amazon Fraud Detector 時可能遇到的問題

排解訓練資料問題

使用本節中的資訊，協助診斷和解決您在訓練模型時，Amazon Fraud Detector 主控台的模型訓練診斷窗格中可能會看到的問題。

模型訓練診斷窗格中顯示的問題分類如下。解決此問題的要求取決於問題的類別。

-  錯誤-導致模型訓練失敗。必須解決這些問題，模型才能成功訓練。
-  警告-使模型訓練繼續進行，但是某些變數可能會在訓練過程中排除。請查看本節中的相關指引，以改善資料集的品質。
-  資訊 (資訊)-對模型訓練沒有影響，且所有變數都用於訓練。我們建議您查看本節中的相關指南，以進一步改善資料集的品質和模型效能。

主題

- 在給定的數據集不穩定的欺詐率
- 資料不足
- 缺少或不同的事件標籤值
- 缺少或不正確的事件時間戳記值
- 未擷取資料
- 變數不足
- 缺少或不正確的變數類型
- 缺少變數值
- 唯一變數值不足
- 變數運算式不正
- 唯一實體不足

在給定的數據集不穩定的欺詐率

問題類型：錯誤

Description

給定數據中的欺詐率隨著時間的推移過於不穩定。請確保您的欺詐和合法事件隨著時間的推移均勻採樣。

原因

如果資料集中的詐騙和合法事件分佈不均，而且是從不同的時段擷取，就會發生這個錯誤。Amazon Fraud Detector 模型訓練程序會根據 EVENT_TIMESTAMP 對您的資料集進行範例和分區 例如，如果您的資料集包含從過去 6 個月擷取的詐騙事件，但只包含最後一個月的合法事件，則該資料集會被視為不穩定。不穩定的資料集可能會導致模型效能評估出現偏差。

解決方案

確保從同一時間段提供欺詐和合法事件數據，並且欺詐率不會隨著時間的推移而發生巨大變化。

資料不足

1. 問題類型：錯誤

   Description

   少於 50 列會被標記為詐騙事件。確保詐騙和合法事件都超過 50 次的最低數量，然後重新訓練模型。

   原因

   如果您的資料集標記為詐騙事件的事件少於模型訓練所需的事件，就會發生此錯誤。Amazon Fraud Detector 至少需要 50 個詐騙事件來訓練您的模型。

   解決方案

   請確定您的資料集包含至少 50 個詐騙事件。如果需要，您可以通過覆蓋更長的時間來確保這一點。

2. 問題類型：錯誤

   Description

少於 50 個資料列會標示為合法事件。確保欺詐和合法事件都超過 $ 閾值的最低計數，並重新訓練模型。

原因

如果您的資料集具有標記為合法的事件少於模型訓練所需的事件，就會發生此錯誤。Amazon Fraud Detector 至少需要 50 個合法事件來訓練您的模型。

解決方案

請確定您的資料集包含至少 50 個合法事件。如果需要，您可以通過覆蓋更長的時間來確保這一點。

3. 問題類型：錯誤

   Description

   與欺詐相關的唯一實體數量少於 100。考慮包括更多欺詐實體的例子，以提高績效。

   原因

   如果您的資料集具有詐騙事件的實體少於模型訓練所需的實體，就會發生此錯誤。交易欺詐見解（TFI）模型要求至少 100 個發生欺詐事件的實體，以確保欺詐空間的最大覆蓋範圍。如果所有欺詐事件都是由一小群實體執行，則該模型可能無法很好地概括起來。

   解決方案

   請確定您的資料集包含至少 100 個發生詐騙事件的實體。如果需要，您可以確保這覆蓋更長的時間段。

4. 問題類型：錯誤

   Description

   與合法關聯的唯一實體數量少於 100。請考慮加入更多合法實體的範例，以提升效能。

   原因

   如果您的資料集具有合法事件的實體少於模型訓練所需的實體，就會發生此錯誤。交易欺詐見解（TFI）模型要求至少 100 個具有合法事件的實體，以確保欺詐空間的最大覆蓋範圍。如果所有合法事件都是由一小群實體執行，則該模型可能無法很好地推廣。

   解決方案

請確定您的資料集包含至少 100 個具有合法事件的實體。如果需要，您可以確保這覆蓋更長的時間段。

5. 問題類型：錯誤

   Description

   資料集中的資料列少於 100 個。請確定總資料集中有 100 個以上的資料列，而且至少 50 列被標記為詐騙資料列。

   原因

   如果您的資料集包含少於 100 筆記錄，就會發生這個錯誤。Amazon Fraud Detector 需要資料集中至少 100 個事件 (記錄) 中的資料，以進行模型訓練。

   解決方案

   請確定您的資料集中有來自 100 個以上事件的資料。

缺少或不同的事件標籤值

1. 問題類型：錯誤

   Description

   大於 1% 的 EVENT_LABEL 資料欄為空值，或是模型組態中定義的值以外的值。**$label_values**請確保 EVENT_LABEL 欄中缺少於 1% 的值，而且這些值是在模型組態中定義的值。**$label_values**

   原因

   發生這個錯誤是因為下列其中一個原因：

   - 包含訓練資料的 CSV 檔案中，超過 1% 的記錄在「EVENT_LABEL」欄中缺少值。
   - 包含訓練資料的 CSV 檔案中，超過 1% 的記錄在 EVENT_LABEL 欄中的值與與您的事件類型相關聯的記錄不同。

   線上詐騙洞察 (OFI) 模型要求每筆記錄中的 EVENT_LABEL 資料欄填入其中一個與您的事件類型相關聯的標籤 (或對應)。`CreateModelVersion`

   解決方案

如果此錯誤是由於缺少 EVENT_LABEL 值，請考慮為這些記錄指派適當的標籤，或從資料集中刪除這些記錄。如果此錯誤是因為某些記錄的標籤不在其中**label_values**，請確定將 EVENT_LABEL 欄中的所有值新增至事件類型的標籤，並在建立模型時對應至詐騙或合法 (詐騙、合法)。

2. 問題類型：資訊

   Description

   您的 EVENT_LABEL 資料欄包含非模型組態中定義的空值或標籤值。**$label_values**這些不一致的值在培訓之前被轉換為「不欺詐」。

   原因

   您會因為下列其中一個原因而取得此資訊：

   - CSV 檔案中包含訓練資料的記錄中，少於 1% 的「EVENT_LABEL」欄中缺少值
   - 包含訓練資料的 CSV 檔案中，少於 1% 的記錄在 EVENT_LABEL 欄中的值與與事件類型相關聯的值不同。

   在這兩種情況下的模型培訓將成功。但是，那些缺少或未映射標籤值的事件的標籤值會轉換為合法的。如果您認為這是一個問題，請按照下面提供的解決方案進行操作。

   解決方案

   如果資料集中缺少 EVENT_LABEL 值，請考慮從資料集中刪除這些記錄。如果為這些 EVENT_LABELS 提供的值未對應，請確定所有這些值都對應至每個事件的詐騙或合法 (詐騙、合法)。

缺少或不正確的事件時間戳記值

1. 問題類型：錯誤

   Description

   您的訓練資料集包含含有不符合接受格式的時間戳記的 EVENT_TIMESTAMP。確保格式是接受的日期/時間戳記格式之一。

   原因

   如果 EVENT_TIMESTAMP 資料行包含的值不符合 Amazon Fraud Detector 支援的時間戳記格式，就會發生此錯誤。

解決方案

請確定為 EVENT_TIMESTAMP 資料行提供的值符合支援的時間戳記格式。如果 EVENT_TIMESTAMP 欄中缺少值，您可以使用支援的時間戳記格式回填具有值的值，或考慮完全刪除事件，而不必輸入字串，例如none、或。null missing

2. 問題類型：錯誤

   您的訓練資料集包含具有缺少值的事件 _ 時間戳記。請確定您沒有遺漏值。

   原因

   如果資料集中的 EVENT_TIMESTAMP 資料行缺少值，就會發生這個錯誤。Amazon Fraud Detector 要求資料集中的 EVENT_TIMESTAMP 資料行具有值。

   解決方案

   請確定資料集中的 EVENT_TIMESTAMP 資料行具有值，且這些值符合支援的時間戳記格式。如果 EVENT_TIMESTAMP 欄中缺少值，您可以使用支援的時間戳記格式回填具有值的值，或考慮完全刪除事件，而不必輸入字串，例如none、或。null missing

未擷取資料

問題類型：錯誤

Description

找不到用於訓練的攝入事件，請檢查您的訓練配置。

原因

如果您建立的模型包含使用 Amazon Fraud Detector 儲存的事件資料，但在開始訓練模型之前並未將資料集匯入 Amazon Fraud Detector，就會發生此錯誤。

解決方案

使用 SendEvent Amazon Fraud Detector 主控台中的 CreateBatchImportJob API 操作、API 操作或批次匯入功能，先匯入事件資料，然後訓練模型。如需詳細資訊，請參閱儲存的事件資料

> **Note**
>
> 我們建議您在資料匯入完成後等待 10 分鐘，然後再使用資料訓練模型。

您可以使用 Amazon Fraud Detector 主控台來檢查每個事件類型已存放的事件數量。如需詳細資訊，請參閱檢視已儲存事件的指標。

變數不足

問題類型：錯誤

Description

資料集必須包含至少 2 個適合訓練的變數。

原因

如果您的資料集包含少於 2 個適用於模型訓練的變數，就會發生這個錯誤。Amazon Fraud Detector 只會在通過所有驗證的情況下，才會考慮適合模型訓練的變數。如果變數驗證失敗，則會在模型訓練中排除該變數，而且您會在模型訓練診斷中看到訊息。

解決方案

請確定您的資料集至少有兩個填入值的變數，並通過所有資料驗證。請注意，您提供資料欄標題 (EVENT_TIMT_ID、ENTTY_ID、EVENT_LABEL 等) 的事件中繼資料列不會被視為變數。

缺少或不正確的變數類型

問題類型：警告

Description

的預期資料類型**$variable_name**為「數字」。在資料集**$variable_name**中檢閱和更新，然後重新訓練模型。

原因

如果變數定義為 NUMERIC 變數，但在資料集中，它的值無法轉換為 NUMERIC，就會收到此警告。因此，模型訓練中會排除該變數。

解決方案

如果要將其保留為 NUMERIC 變量，請確保您提供的值可以轉換為浮點數。請注意，如果變數包含缺少的值，請勿使用nonene、null或之類的字串填入它們missing。如果變數確實包含非數值，請將其重新建立為分類或 FREE_FORM_TEXT 變數類型。

缺少變數值

問題類型：警告

Description

訓練資料集中**$variable_name**缺少的大於的**$threshold**值。請考慮**$variable_name**在資料集中修改並重新訓練以改善效能。

原因

如果由於缺少值過多而丟棄指定的變量，則會收到此警告。Amazon Fraud Detector 允許缺少變數的值。但是，如果一個變數有太多的缺失值，它不會對模型有太多貢獻，而且該變數會在模型訓練中捨棄。

解決方案

首先，請確認那些缺失的值不是由於資料收集和準備中的錯誤所致。如果它們是錯誤的，那麼您可以考慮將它們從模型訓練中刪除。但是，如果您確實認為那些缺失的值很有價值，並且仍想要保留該變數，則可以在模型訓練和即時推論中使用常數來手動填入缺失值。

唯一變數值不足

問題類型：警告

Description

的唯一值的計**$variable_name**數低於 100。在資料集**$variable_name**中檢閱和更新，然後重新訓練模型。

原因

如果指定變數的唯一值數目小於 100，則會收到此警告。臨界值會根據變數類型而有所不同。具有極少數唯一值的情況下，存在資料集的一般性不足以涵蓋該變數的功能空間的風險。因此，該模型可能無法在實時預測中很好地概括起來。

解決方案

首先，確保變量分佈是代表真正的業務流量。然後，您可以採用具有較高基數的更精細訓練的變量，例如使用full_customer_name而不是first_name和last_name單獨使用，或者將變量類型更改為CAREGARICAL，這樣可以使基數較低。

變數運算式不正

1. 問題類型：資訊

   Description

   大於 50% 的**$email_variable_name**值不符合預期的規則運算式 http://emailregex.com。請考慮**$email_variable_name**在資料集中修改並重新訓練以改善效能。

   原因

   如果資料集中超過 50% 的記錄具有不符合規則電子郵件運算式的電子郵件值，因此驗證失敗，就會顯示此資訊。

   解決方案

   格式化電子郵件變數值以符合規則運算式。如果缺少電子郵件值，我們建議將其保留空白，而不要用字串 (例如nonenull、或) 填入missing。
2. 問題類型：資訊

   Description

   大於 50% 的**$IP_variable_name**值與 IPv4 或 IPv6 位址的規則運算式不符。commonly-used-regex https://digitalfortress.tech/tricks/top-15 請考慮**$IP_variable_name**在資料集中修改並重新訓練以改善效能。

   原因

   如果資料集中 50% 以上的記錄具有不符合規則 IP 運算式的 IP 值，因此驗證失敗，就會顯示此資訊。

   解決方案

   格式化 IP 值以符合規則運算式。如果缺少 IP 值，我們建議將它們保留空白，而不要用字串 (例如nonenull、或) 填入missing。

3. 問題類型：資訊

   Description

   大於 50% 的**$phone_variable_name**值與基本電話正則表達式 /$ 模式/不匹配。請考慮**$phone_variable_name**在資料集中修改並重新訓練以改善效能。

   原因

   如果資料集中超過 50% 的記錄包含不符合一般電話號碼運算式的電話號碼，因此驗證失敗，就會顯示此資訊。

   解決方案

   格式化電話號碼以符合規則運算式。如果缺少電話號碼，我們建議將它們留空，而不要用字符串填充none，例如null，或missing。

唯一實體不足

問題類型：資訊

Description

唯一實體的數目小於 1500。請考慮加入更多資料以改善效能。

原因

如果資料集的唯一實體數目少於建議數目，就會顯示此資訊。交易詐騙洞察 (TFI) 模型同時使用時間序列彙總和一般交易功能來提供最佳效能。如果您的資料集具有太少的唯一實體，則大部分的一般資料 (例如 IP_ADDRESS、EMAIL_ADDRESS) 可能沒有唯一的值。然後，還有一個風險，即此數據集不足以涵蓋該變量的功能空間。因此，該模型可能無法很好地概括來自新實體的交易。

解決方案

包括更多實體。視需要延長訓練資料的時間範圍。

配額

對於每項 Amazon 網路服務，您的AWS 帳戶有預設配額，先前稱為限制。除非另有說明，否則每個配額都是區域特定規定。對於下表中提到的所有可調整配額，您可請求提高配額。如需詳細資訊，請參閱請求提高配額

下表概述了各元件的 Amazon Fraud Detector 配額。

Amazon Fraud Detector

配額名稱	預設配額	可調整
訓練資料大小	5 GB	否
每個帳戶的模型數	50	否
每個機型的版本	200	否
每個帳戶部署的模型版本	5	否
每個帳戶的同時訓練工作	3	否
每個模型的同時訓練工作	1	否

Amazon Fraud Detector 偵測器/變數/結果/規則

配額名稱	預設配額	可調整
每個帳戶的變數	5000	否
每個 帳戶的規則數	5000	否
每個規則的清單	3	否
每個帳戶的結果	5000	否
每個帳戶的偵測器	100	否

配額名稱	預設配額	可調整
每個偵測器清單	30	否
每個偵測器草案版本	100	否
各偵測器版本的型號	10	否
每個帳戶的標籤	100	否
每個帳戶的事件	100	否
每個帳戶的實體	100	否

Amazon Fraud Detector

配額名稱	預設配額	可調整
GetEventPrediction 每秒 API 呼叫次數	200 TPS	是
每個 GetEventPrediction API 呼叫的承載大小	256 KB	否
每個 GetEventPrediction API 呼叫的輸入數	5000	否

文件歷史紀錄

下表說明 Amazon 詐騙偵測器使用者指南中的重要變更。我們也會經常更新 Amazon 詐騙偵測器使用者指南，以解決您傳送給我們的意見反應。

變更	描述	日期
新的變量和數據類型	Amazon 詐騙偵測器引入了新的變數類型以及可用來擷取有用資訊的資料類型。	2023年6月5 日
活動編排	事件編排可讓您使用 Amazon EventBridge 輕鬆將事件傳送到 AWS 服務下游處理。	2023 年 5 月 30 日
列表	L ist 資源可讓您參考一組值，例如 IP 位址或電子郵件地址，做為規則的一部分。使用規則中的清單來允許或拒絕存取或交易。	2023 年 2 月 14 日
資料模型總管	資料模型總管針對 Amazon 詐騙偵測器建立詐騙偵測模型所需的資料元素提供深入解析。在準備事件資料集之前，請先使用資料模型總管。	2022 年 12 月 15 日
帳戶接管洞察模型	使用帳戶接管見解 (ATI) 模型，偵測惡意接管、網路釣魚或憑證遭竊而遭到入侵的帳戶。	2022 年 7 月 21 日
章節更新	更新了介紹章節有關亞馬遜欺詐檢測器的其他信息	2022年4月11日
變數豐富	啟用您提供的某些原始資料，以提升使用這些資料元素且在	2022 年 2 月 8 日

	2022 年 2 月 8 日之前訓練過的模型的效能。	
退出政策	使用退出政策選擇退出您的事件資料用於開發或改善 Amazon 詐騙偵測器的品質。	2022 年 1 月 6 日
混淆副預防	建立原則以防止第三方或跨服務實體操控具有權限的實體，以代表其採取行動，以取得您帳戶中資源的存取權。	2021 年 12 月 6 日
建立事件資料集	使用建立事件資料集中提供的指導來準備和收集用於訓練模型的資料。	2021 年 11 月 22 日
預測說明	使用「預測」說明深入瞭解每個事件變數如何影響模型的詐騙預測分數。	2021 年 11 月 10 日
疑難排	使用訓練資料問題疑難排解中的資訊，協助診斷和解決訓練模型時可能在 Amazon 詐騙偵測器主控台中看到的問題。	2021 年 10 月 11 日
交易詐騙洞察模型	使用交易欺詐洞察（TFI）模型來檢測在線或card-not-present交易欺詐。	2021 年 10 月 11 日
存儲的事件	將您的事件資料存放在 Amazon 詐騙偵測器中，然後使用儲存的資料來訓練您的模型。透過將事件資料存放在 Amazon 詐騙偵測器中，您可以訓練使用自動計算變數的模型來提升效能、簡化模型再訓練，以及更新詐騙標籤以關閉機器學習回饋迴圈。	2021 年 10 月 11 日

模型變數重要性	使用模型變數重要性，深入瞭解模型上下推動效能的原因，以及哪些模型變數的貢獻最大。然後調整您的模型以提高整體性能。	2021 年 7 月 9 日
與 AWS CloudFormation 整合	用AWS CloudFormation於管理您的 Amazon 詐騙偵測器資源。	2021 年 5 月 10 日
批次預測	使用批次預測來取得一組不需要即時評分的事件的預測。	2021 年 3 月 31 日
章節返工	開始使用和其他部分的返工	2020 年 7 月 17 日
初始版本	初始版本	2019 年 12 月 2 日

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。