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 是一項全受管的詐騙偵測服務，可自動偵測潛在的線上詐騙活動。這些活動包括未經授權的交易和建立仿造帳戶。Amazon Fraud Detector 的運作方式是使用機器學習來分析您的資料。其做法是以 Amazon 超過 20 年詐騙偵測的豐富專業知識為基礎。

您可以使用 Amazon Fraud Detector 來建置自訂的詐騙偵測模型、新增決策邏輯來解譯模型的詐騙評估，以及為每個可能的詐騙評估指派結果，例如通過或傳送以供檢閱。使用 Amazon Fraud Detector，您不需要機器學習專業知識來偵測詐騙活動。

若要開始使用，請收集並準備您在組織中收集的詐騙資料。然後，Amazon Fraud Detector 會使用這些資料來代表您訓練、測試和部署自訂詐騙偵測模型。在此程序中，Amazon Fraud Detector 會使用機器學習模型，這些模型已從 AWS 和 Amazon 自己的詐騙專業知識中學習詐騙模式，以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 提供下列優點。這些好處可讓您快速偵測詐騙，而不需要投入傳統上建置和維護詐騙管理系統所需的時間和資源。

自動化詐騙模型建立

Amazon Fraud Detector 的詐騙偵測模型是全自動化的機器學習模型，專為滿足您的特定業務需求而自訂。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，例如新帳戶建立、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，因此您可以放棄與建立和訓練模型相關聯的許多步驟。這些步驟包括資料驗證和擴充、特徵工程、演算法選擇、超參數調校和模型部署。

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。您不需要知道編碼或具備機器學習專業知識，即可建立詐騙偵測模型。

發展和學習的詐騙模型

詐騙偵測模型必須不斷發展，才能跟上不斷變化的詐騙態勢。Amazon Fraud Detector 會透過計算帳戶存留期、自上次活動以來的時間和活動計數等資訊，自動執行此操作。結果是您的模型會了解經常進行

交易的信任客戶與詐騙者持續嘗試之間的差異。這有助於在重新訓練工作階段之間維持模型的效能更長。

詐騙模型效能視覺化

使用您提供的資料訓練模型後，Amazon Fraud Detector 會驗證模型效能。它還提供視覺化工具，供您評估效能。對於您訓練的每個模型，您可以看到模型效能分數、分數分佈圖、混淆矩陣、閾值表，以及您提供的所有輸入，根據其對模型效能的影響進行排名。使用這些效能工具，您可以了解模型的效能，以及驅動模型效能的輸入。如有需要，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。詐騙預測是對詐騙風險的業務活動進行評估。Amazon Fraud Detector 會使用預測邏輯與與活動相關聯的資料產生預測。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。

詐騙預測說明視覺化

Amazon Fraud Detector 會在詐騙預測程序中產生預測說明。預測說明可讓您深入了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。預測說明是使用視覺化工具提供，例如資料表和圖形。您可以使用這些工具，以視覺化方式識別每個資料元素對預測分數的影響程度。然後，您可以使用此資訊來分析整個資料集的詐騙模式，並偵測是否有任何偏差。最後，您也可以使用預測說明來識別手動詐騙調查程序期間的首要風險指標。這可協助您縮小導致誤報的根本原因。

規則型動作

訓練您的詐騙偵測模型之後，您可以新增規則，對評估的資料採取動作，例如接受資料、傳送資料以供檢閱或收集更多資料。規則是告訴 Amazon Fraud Detector 如何在詐騙預測期間解譯資料的條件。例如，您可以建立規則，標記要檢閱的可疑客戶帳戶。如果偵測到的模型分數都大於您的預定閾值，而且帳戶付款的授權碼 (AUTH_CODE) 無效，您可以設定此規則以啟動。

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

事件是您組織的商業活動，會評估詐騙風險。Amazon Fraud Detector 會產生事件的詐騙預測。

標籤

標籤會將單一事件分類為詐騙或合法。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 做為公司詐騙資料的一部分，以指出執行事件的特定實體。

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），以及分類事件的標籤。範例事件類型包括線上付款交易、帳戶註冊和身分驗證。

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針對特定商業活動或事件的歷史資料。例如，您公司的事件可能是線上帳戶註冊。來自單一事件（註冊）的資料可能包括相關聯的 IP 地址、電子郵件地址、帳單地址和事件時間戳記。您會提供事件資料集給 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

模型類型定義了模型訓練期間使用的演算法、擴充功能和特徵轉換。它也定義了訓練模型的資料需求。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 會評估資料集是否有詐騙活動，並產生介於 0 到 1000 之間的分數。對於此分數，0 代表低詐騙風險，而 1000 代表最高的詐騙風險。分數本身與誤報率 (FPR) 直接相關。

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 AI 模型端點

除了使用 Amazon Fraud Detector 建置模型之外，您還可以選擇在 Amazon Fraud Detector 評估中使用 SageMaker AI 託管模型端點。

如需在 SageMaker AI 中建置模型的詳細資訊，請參閱使用 訓練模型 Amazon SageMaker AI。

偵測器

偵測器包含偵測邏輯，例如您想要評估詐騙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 `Draft`、 `Active`或 `Inactive`。一次只能有一個偵測器版本處於 `Active` 狀態。

變數

變數代表與您想要在詐騙預測中使用的事件相關聯的資料元素。變數可以與事件一起傳送，做為詐騙預測的一部分或衍生，例如 Amazon Fraud Detector 模型的輸出或 Amazon SageMaker AI。

規則

規則是告訴 Amazon Fraud Detector 如何在詐騙預測期間解譯變數值的條件。規則包含一或多個變數、邏輯表達式和一或多個結果。規則中使用的變數必須是偵測器評估的事件資料集的一部分。此外，每個偵測器必須至少有一個與其相關聯的規則。

Outcome

這是詐騙預測的結果或輸出。用於詐騙預測的每個規則都必須指定一或多個結果。

詐騙預測

詐騙預測是評估單一事件或一組事件的詐騙。Amazon Fraud Detector 會根據規則同步提供模型分數和結果，即時產生單一線上事件的詐騙預測。Amazon Fraud Detector 會離線產生一組事件的詐騙預測。您可以使用預測來執行離線proof-of-concept，或每小時、每日或每週回溯性評估詐騙風險。

詐騙預測說明

詐騙預測說明可讓您深入了解每個變數如何影響模型的詐騙預測分數。它提供有關每個變數如何影響規模 （從 0 到 5，5 為最高） 和方向 （推高或降低分數） 的風險分數的資訊。

Amazon Fraud Detector 的運作方式

Amazon Fraud Detector 會建置機器學習模型，此模型是為偵測您企業中潛在的詐騙線上活動而自訂。若要開始使用，請提供您的業務使用案例。視您的業務使用案例而定，Amazon Fraud Detector 建議用來為您建立詐騙偵測模型的模型類型。此外，它還提供了您在業務歷史資料中需要提供的資料元素的洞見。Amazon Fraud Detector 使用歷史資料集自動為您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，以偵測特定業務使用案例的詐騙、驗證您提供的資料，以及執行資料操作來改善模型效能。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。如有需要，您可以從您提供用於訓練的資料集中新增或移除資料元素，並重新訓練模型以改善模型分數。

建立、訓練和啟用模型後，您需要設定決策邏輯，也稱為規則，告知模型如何解譯業務產生的資料，並指派如何處理每個活動的解譯結果。結果可以代表動作，例如核准或檢閱活動，也可以代表活動的風險層級，例如高風險、中等風險和低風險。

偵測器是存放模型和相關規則的容器。您需要建立、測試偵測器，並將偵測器部署到您的生產環境。

安裝在生產環境中的偵測器為您的業務應用程式提供詐騙偵測功能。為了執行詐騙評估，模型會比較所有來自業務活動的傳入資料與業務的歷史資料，並使用其複雜的機器學習演算法與您建立的規則，以分析結果並指派結果。使用 Amazon Fraud Detector，您可以即時評估來自單一業務活動的資料，或離線評估來自多個業務活動的資料。

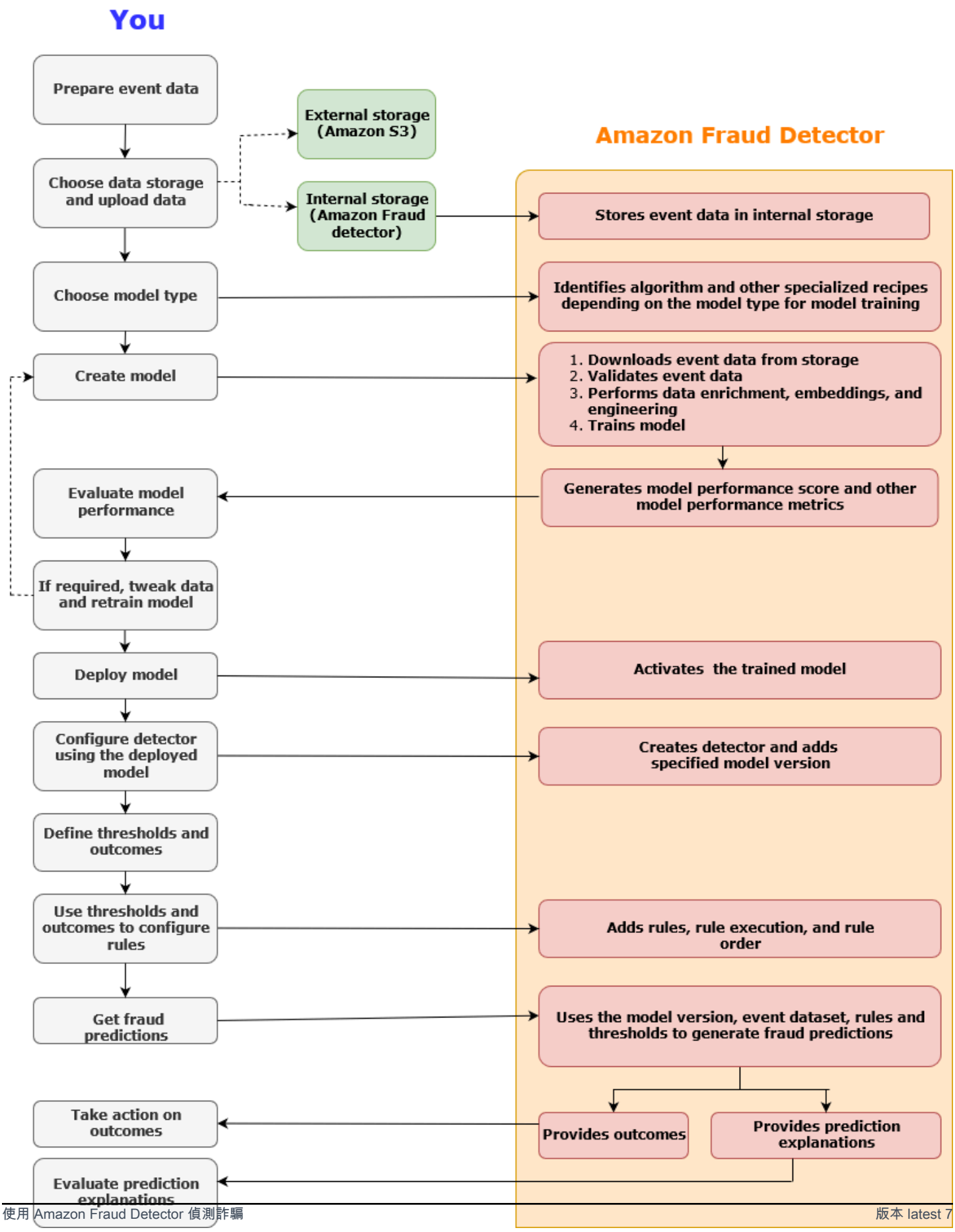
假設您有一個企業將線上資金轉移作為其活動之一。您想要使用 Amazon Fraud Detector 即時偵測資金轉移的詐騙請求。若要開始使用，您必須先向 Amazon Fraud Detector 提供過去資金轉移請求的資料。Amazon Fraud Detector 使用此資料來建立和訓練自訂的模型，以偵測資金轉移的詐騙請求。然後，您可以透過新增模型和設定模型的規則來解譯資料，來建立偵測器。線上資金轉移活動的規則範例是，如果資金轉移請求來自 xyz@example.com 電子郵件地址，請傳送請求以供審核。在您企業的生產環境中，當資金轉移請求進入時，模型會分析請求隨附的資料，並使用 規則來指派結果。然後，您可以根據指派的結果對請求採取動作。

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 偵測詐騙之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 偵測詐騙之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

詐騙偵測是一個持續的過程。部署模型之後，請務必根據預測說明來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，並偵測是否有任何偏差。若要提高預測的準確性，您可以調整資料集以包含新的或修訂的資料。然後，您可以使用更新的資料集重新訓練模型。隨著更多資料可供使用，您可以繼續重新訓練模型以提高準確性。

存取 Amazon Fraud Detector

Amazon Fraud Detector 提供多個 ， AWS 區域 並且可以使用 AWS 介面存取。

可用性

Amazon Fraud Detector 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）提供 AWS 區域。

介面

您可以使用下列任一界面來建立、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 提供以 Web 為基礎的使用者介面：Amazon Fraud Detector 主控台。如果您註冊 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 shell 中的命令與廣泛的 互動， AWS 服務包括 Amazon Fraud Detector。Amazon Fraud Detector 的 AWS CLI 命令實作與 Amazon Fraud Detector 主控台提供的功能相當的功能。

AWS SDK - 提供語言特定的 APIs 和管理許多連線詳細資訊，例如簽章計算、請求重試處理和錯誤處理。如需詳細資訊，請前往工具以建置 AWS頁面、向下捲動至 SDK 區段，然後選擇加號 (+) 以展開區段。

AWS CloudFormation - 提供可用來定義 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 時，您只需支付使用量的費用。沒有最低費用或者預付款項。系統會根據用於訓練和託管模型的運算時數、您使用的儲存量，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。

設定 Amazon Fraud Detector

若要使用 Amazon Fraud Detector，您首先需要 Amazon Web Services (AWS) 帳戶，然後必須設定授予所有介面 AWS 帳戶 存取權的許可。稍後當您開始建立 Amazon Fraud Detector 資源時，您需要授予許可，允許 Amazon Fraud Detector 存取您的帳戶以代表您執行任務，以及存取您擁有的資源。

完成本節中的下列任務，以設定使用 Amazon Fraud Detector：

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

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

註冊 AWS

當您註冊 Amazon Web Services (AWS) 時，您的 AWS 帳戶 會自動註冊所有 服務 AWS，包括 Amazon Fraud Detector。您只需針對所使用的服務付費。如果您已有 AWS 帳戶，請跳到下一個任務。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

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

   註冊程序的一部分包括接聽電話或文字訊息，並在電話鍵盤上輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 會在註冊程序完成後傳送確認電子郵件給您。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。

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立 管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS Management Console身分登入 。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)。

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （主控台） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

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 Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center《 使用者指南》中的使用預設值設定使用者存取 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 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 Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》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 Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

設定存取 Amazon Fraud Detector 介面的許可

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 AWS Identity and Access Management (IAM) 使用者，其存取權僅限於 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 所需的許可：

- `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 SageMaker AI 中的所有模型端點
  - 列出帳戶中的所有 IAM 角色
  - 列出所有 Amazon S3 儲存貯體
  - 允許 IAM Pass 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，這是必要的。

以下說明如何建立 IAM 使用者並指派所需的許可。

建立使用者並指派必要的許可

1. 登入 AWS Management Console 並開啟位於 https：//https://console.aws.amazon.com/iam/ 的 IAM 主控台。
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. （選用）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. 選擇建立群組。
8. 針對群組名稱輸入 **AmazonFraudDetectorGroup**。
9. 在政策清單中，選取 AmazonFraudDetectorFullAccessPolicy 和 AmazonS3FullAccess 的核取方塊。選擇建立群組。
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 中使用標籤的說明，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訊和許可摘要。當您準備好繼續時，請選擇建立使用者。

設定界面以使用 存取 Amazon Fraud Detector

您可以使用 Amazon Fraud Detector 主控台 AWS CLI或 AWS SDK 存取 Amazon Fraud Detector。您必須先設定 AWS CLI 和 AWS SDK，才能使用它們。

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 帳戶會授予您 的存取權 AWS Management Console。

若要存取 Amazon Fraud Detector 主控台，

1. 前往 https://console.aws.amazon.com/ 並登入您的 AWS 帳戶。
2. 導覽至 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 Shell 中執行命令，以使用 AWS Command Line Interface (AWS CLI) 與 Amazon Fraud Detector 互動。透過最少的組態，您可以使用 AWS CLI ，從終端機中的命令提示字元，針對與 Amazon Fraud Detector 主控台提供的類似功能執行命令。

設定 AWS CLI

下載和設定 AWS CLI。如需說明，請參閱 AWS Command Line Interface 《 使用者指南》中的下列主題：

- 使用 AWS 命令列界面進行設定
- 設定 AWS 命令列界面

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

設定 AWS SDK

您可以使用 AWS SDKs撰寫程式碼來建立和管理詐騙偵測資源，以及取得詐騙預測。 AWS SDKs 支援 JavaScript 和 Python (Boto3) 中的 Amazon Fraud Detector。

設定 適用於 Python (Boto3) 的 AWS SDK

您可以使用 適用於 Python (Boto3) 的 AWS SDK 來建立、設定和管理 AWS 服務。如需如何安裝 Boto 的說明，請參閱AWS 適用於 Python 的 SDK (Boto3)。請確定您使用的是 Boto3 SDK 1.14.29 版或更新版本。

安裝之後 適用於 Python (Boto3) 的 AWS SDK，請執行下列 Python 範例，確認您的環境已正確設定。如果設定正確，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)
```

設定 Java 的 AWS SDKs

如需如何安裝和載入 的指示 適用於 JavaScript 的 AWS SDK，請參閱設定適用於 JavaScript 的 SDK。

Amazon Fraud Detector 入門

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

使用本節中的實作教學，了解如何使用 Amazon Fraud Detector 來建置、訓練和部署詐騙偵測模型。在本教學課程中，您會使用機器學習模型擔任詐騙分析師的角色，以預測新帳戶註冊是否詐騙。模型必須使用來自帳戶註冊的資料進行訓練。Amazon Fraud Detector 提供本教學課程的範例帳戶註冊資料集。必須先上傳範例資料集，才能開始使用教學課程。

您可以使用下列其中一個界面來開始使用 Amazon Fraud Detector。開始使用教學課程之前，請務必遵循 的指示 取得和上傳範例資料集

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

取得和上傳範例資料集

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。資料集位於文字檔案中，使用 UTF-8 格式的逗號分隔值 (CSV)。CSV 資料集檔案的第一列包含 標頭。標頭列後面接著多個資料列。這些資料列都包含來自單一帳戶註冊的資料元素。為了您的方便，資料會加上標籤。資料集中的資料欄可識別帳戶註冊是否詐騙。

取得和上傳範例資料集

1. 前往範例。

   有兩個資料檔案具有線上帳戶註冊資料 - registration_data_20K_minimum.csv 和 registration_data_20K_full.csv。檔案僅`registration_data_20K_minimum`包含兩個變數：ip_address 和 email_address。檔案`registration_data_20K_full`包含其他變數。這些變數適用於每個事件，且包含 billing_address、phone_number 和 user_agent。這兩個資料檔案也包含兩個必要欄位：

   - EVENT_TIMESTAMP – 定義事件發生的時間
   - EVENT_LABEL – 將事件分類為詐騙或合法

   您可以在本教學課程中使用兩個檔案之一。下載您要使用的資料檔案。

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

   在此步驟中，您會建立外部儲存來存放資料集。此外部儲存體是 Amazon S3 儲存貯體。如需 Amazon S3 的詳細資訊，請參閱什麼是 Amazon S3？

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

   b. 在儲存貯體中，選擇建立儲存貯體。

   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儲存貯體命名規則，並提供全域唯一名稱。我們建議您使用描述儲存貯體用途的名稱。

   d. 針對 AWS 區域，選擇您要建立儲存貯 AWS 區域 體的 。您選擇的區域必須支援 Amazon Fraud Detector。若要減少延遲，請選擇最接近您地理位置 AWS 區域 的 。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、儲存貯體版本控制和標籤的預設設定。

   f. 針對預設加密，選擇停用此教學課程。

   g. 檢閱您的儲存貯體組態，然後選擇建立儲存貯體。

3. 將範例資料檔案上傳至 Amazon S3 儲存貯體。

   現在您已擁有儲存貯體，請將您先前下載的其中一個範例檔案上傳至您剛建立的 Amazon S3 儲存貯體。

   a. 在儲存貯體中，會列出您的儲存貯體名稱。選擇您的儲存貯體。

   b. 選擇上傳。

   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、許可和屬性的預設設定。

   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。記下儲存貯體位置。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。您稍後使用它。您可以另外複製 S3 儲存貯體的 Amazon Resource Name (ARN)，並加以儲存。

教學課程：開始使用 Amazon Fraud Detector 主控台

本教學課程包含兩個部分。第一部分說明如何建置、訓練和部署詐騙偵測模型。第二部分介紹如何使用模型即時產生詐騙預測。模型使用您上傳至 S3 儲存貯體的範例資料檔案進行訓練。在本教學課程結束時，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**
>
> 在繼續之前，請確定您已遵循 的指示 取得和上傳範例資料集

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

在 A 部分中，您會定義業務使用案例、定義事件、建置模型、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，您會使用資料模型總管，將業務使用案例與 Amazon Fraud Detector 支援的詐騙偵測模型類型進行比對。Data Model Explorer 是與 Amazon Fraud Detector 主控台整合的工具，建議使用模型類型來建立和訓練業務使用案例的詐騙偵測模型。資料模型探索器也提供洞見，了解您在資料集中需要包含的必要、建議和選用資料元素。資料集將用於建立和訓練您的詐騙偵測模型。

  在本教學課程中，您的商業使用案例是新帳戶註冊。指定業務使用案例後，資料模型總管會建議建立詐騙偵測模型的模型類型，也會提供您建立資料集所需的資料元素清單。由於您已上傳包含新帳戶註冊資料的範例資料集，因此您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。導覽至 Amazon Fraud Detector。
  b. 在左側導覽窗格中，選擇資料模型瀏覽器。
  c. 在資料模型瀏覽器頁面的業務使用案例下，選取新帳戶詐騙。
  d. Amazon Fraud Detector 會顯示建議的模型類型，用於為選取的業務使用案例建立詐騙偵測模型。模型類型定義 Amazon Fraud Detector 用來訓練詐騙偵測模型的演算法、擴充功能和轉換。

     記下建議的模型類型。稍後建立模型時，您將需要此項目。

e. 資料模型洞見窗格可讓您深入了解建立和訓練詐騙偵測模型所需的必要和建議資料元素。

請查看您下載的範例資料集，並確認其具有資料表中列出的所有強制性和一些建議的資料元素。

稍後當您為特定業務使用案例建立模型時，您將使用提供的洞見來建立資料集。

步驟 2：建立事件類型

- 在此步驟中，您會定義要評估詐騙的業務活動（事件）。定義事件涉及設定資料集中的變數、啟動事件的實體，以及分類事件的標籤。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。導覽至 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，輸入 `sample_registration`做為事件類型名稱，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，輸入 `sample_customer`做為實體類型名稱。或者，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，針對選擇如何定義此事件的變數，選擇從訓練資料集中選取變數。

i. 針對 IAM 角色，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。這是您在上傳範例資料之後儲存的S3 URI路徑。路徑類似：`S3://your-bucket-name/example dataset filename.csv`。

l. 選擇上傳。

Amazon Fraud Detector 會從範例資料檔案中擷取標頭，並使用變數類型映射它們。映射會顯示在 主控台中。

m. 在標籤 - 選用的標籤下，選擇建立新標籤。

n. 在建立標籤頁面中，輸入 `fraud`做為名稱。此標籤對應於代表範例資料集中詐騙帳戶註冊的值。

o. 選擇建立標籤。

p. 建立第二個標籤，然後輸入 `legit`做為名稱。此標籤對應於代表範例資料集中合法帳戶註冊的值。

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. 針對步驟 1 – 定義模型詳細資訊，輸入 `sample_fraud_detection_model`做為模型名稱。或者，新增模型的描述。
3. 針對模型類型，選擇線上詐騙洞見模型。
4. 針對事件類型，選擇 sample_registration。這是您在步驟 1 中建立的事件類型。
5. 在歷史事件資料中，

   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 Next (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，因為此標籤對應到代表範例資料集中詐騙事件的值。對於合法標籤，請選擇合法，因為此標籤對應至代表範例資料集中合法事件的值。
3. 對於未標記事件處理，請保留此範例資料集的預設選取項目忽略未標記的事件。
4. 選擇 Next (下一步)。
5. 檢閱後，選擇建立和訓練模型。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，狀態欄指出模型訓練的狀態。使用範例資料集的模型訓練大約需要 45 分鐘才能完成。狀態會在模型訓練完成後變更為準備部署。

步驟 5：檢閱模型效能

使用 Amazon Fraud Detector 的一個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，而這些資料並非用來訓練模型，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 (sample_fraud_detection_model)，然後選擇 1.0。這是 Amazon Fraud Detector 為模型建立的版本。

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。

   若要進一步了解此頁面上的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過的 Amazon Fraud Detector 模型都具有與本教學課程中看到的模型效能指標類似的實際詐騙偵測效能指標。

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後，即可產生詐騙預測，進而部署模型。

1. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇模型。
2. 在模型頁面中，選擇 sample_fraud_detection_model，然後選擇您要部署的特定模型版本。針對本教學課程，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。在部署完成後，狀態會變更為作用中。這表示模型版本已啟用，可用於產生詐騙預測。繼續B 部分：產生詐騙預測完成產生詐騙預測的步驟。

B 部分：產生詐騙預測

詐騙預測是對業務活動（事件）詐騙的評估。Amazon Fraud Detector 使用偵測器來產生詐騙預測。偵測器包含您想要評估詐騙的特定事件的偵測邏輯，例如模型和規則。偵測邏輯使用規則來告知 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 A 部分中，您建立、訓練和部署模型。在 B 部分中，您會為sample_registration事件類型建置偵測器、新增部署的模型、建立規則和規則執行順序，然後建立並啟用您用來產生詐騙預測的偵測器版本。

步驟 1：建置偵測器

建立偵測器

1. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇 Detectors。
2. 選擇建立偵測器。
3. 在定義偵測器詳細資訊頁面中，輸入sample_detector偵測器名稱。或者，輸入偵測器的描述，例如 my sample fraud detector。
4. 針對事件類型，選取 sample_registration。這是您在本教學課程 A 部分中建立的事件。
5. 選擇 Next (下一步)。

步驟 2：新增模型

如果您已完成本教學課程的 A 部分，則可能已有 Amazon Fraud Detector 模型可供新增至偵測器。如果您尚未建立模型，請前往 A 部分，完成建立、訓練和部署模型的步驟，然後繼續 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 模型名稱。針對選取版本，選擇已部署模型的模型版本。
3. 選擇 Add model (新增模型)。
4. 選擇 Next (下一步)。

步驟 3：新增規則

規則是告訴 Amazon Fraud Detector 在評估詐騙預測時如何解譯模型效能分數的條件。在本教學課程中，您會建立三個規則：high_fraud_risk、 medium_fraud_risk和 low_fraud_risk。

1. 在新增規則頁面中，定義規則下，輸入 high_fraud_risk 表示規則名稱，在描述 - 選擇性下，輸入 **This rule captures events with a high ML model score**表示規則的描述。
2. 在表達式中，使用 Amazon Fraud Detector 簡化規則表達式語言輸入下列規則表達式：

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```
3. 在結果中，選擇建立新結果。結果是詐騙預測的結果，如果規則在評估期間相符，則會傳回結果。

4. 在建立新的結果中，輸入 verify_customer做為結果名稱。或者，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。建立之後，Amazon Fraud Detector 會將規則用於偵測器。
7. 選擇新增另一個規則，然後選擇建立規則索引標籤。
8. 使用下列low_fraud_risk規則詳細資訊，再重複此程序兩次以建立您的 medium_fraud_risk和 規則：

   - medium_fraud_risk

     規則名稱： medium_fraud_risk

     結果： review

     表達式：

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

     ```
     $sample_fraud_detection_model_insightscore > 700
     ```

   - low_fraud_risk

     規則名稱： low_fraud_risk

     結果： approve

     表達式：

     ```
     $sample_fraud_detection_model_insightscore <= 700
     ```

   這些值是本教學課程使用的範例。當您為自己的偵測器建立規則時，請使用適合您模型和使用案例的值，
9. 建立全部三個規則後，請選擇下一步。

   如需建立和撰寫規則的詳細資訊，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判斷是否評估您定義的所有規則，或規則評估是否停止在第一個相符規則。而規則順序會決定您希望規則在其中執行的順序。

預設規則執行模式為 FIRST_MATCHED。

第一個相符項目

第一個相符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。

您在 中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。這會high_fraud_risk移至第一個位置。

重複此程序，讓您的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。

所有相符項目

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

針對此教學課程選取 FIRST_MATCHED ，然後選擇下一步。

步驟 5：檢閱並建立偵測器版本

偵測器版本定義用於產生詐騙預測的特定模型和規則。

1. 在檢閱和建立頁面中，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，請選擇對應區段旁的編輯。
2. 選擇建立偵測器。建立後，偵測器的第一個版本會出現在偵測器版本資料表中，其中包含Draft狀態。

   您可以使用草稿版本來測試偵測器。

步驟 6：測試和啟用偵測器版本

在 Amazon Fraud Detector 主控台中，您可以使用模擬資料搭配執行測試功能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. 針對事件中繼資料，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符。在本教學課程中，從時間戳記的日期選擇器中選取日期，然後輸入實體 ID 的「1234」。
3. 針對事件變數，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。這是因為它們是用來訓練 Amazon Fraud Detector 模型的輸入。您可以使用下列範例值。這假設您使用建議的變數名稱：

   - ip_address： `205.251.233.178`
   - email_address： `johndoe@exampledomain.com`
4. 選擇執行測試。
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。如果評估為 true，則會比對。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。這表示它們都被評估為 true。Amazon Fraud Detector 也會傳回新增至偵測器之任何模型的模型分數。

   您可以變更輸入並執行幾個測試，以查看不同的結果。您可以使用範例資料集的 ip_address 和 email_address 值進行測試，並檢查結果是否如預期。
6. 當您對偵測器的運作方式感到滿意時，請將偵測器從 提升`Draft`為 `Active`。這樣做可讓偵測器用於即時詐騙偵測。

   在偵測器版本詳細資訊頁面上，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，您的模型和相關聯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 來評估離線事件。如需詐騙預測的詳細資訊，請參閱 [詐騙預測]

完成本教學課程後，您便完成了以下操作：

- 已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。
- 部署詐騙偵測模型。
- 建立偵測器並新增部署的模型。
- 新增規則、規則執行順序和偵測器的結果。

- 提供不同的輸入並檢查規則和規則執行順序是否如預期般運作，以測試偵測器。
- 透過發佈偵測器來啟用偵測器。

教學課程：開始使用 適用於 Python (Boto3) 的 AWS SDK

本教學說明如何建置和訓練 Amazon Fraud Detector 模型，然後使用此模型來產生使用 的即時詐騙預測 適用於 Python (Boto3) 的 AWS SDK。模型使用您上傳至 Amazon S3 儲存貯體的帳戶註冊範例資料檔案進行訓練。

在本教學課程結束時，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

先決條件

以下是本教學課程的先決條件步驟。

- 已完成 設定 Amazon Fraud Detector。

  如果您已有 設定 AWS SDK，請確定您使用的是 Boto3 SDK 1.14.29 版或更新版本。
- 遵循本教學課程所需取得和上傳範例資料集檔案的說明。

開始使用

步驟 1：設定並驗證您的 Python 環境

Boto 是適用於 Python 的 Amazon Web Services (AWS) SDK。您可以使用它來建立、設定和管理 AWS 服務。如需如何安裝 Boto3 的說明，請參閱適用於 Python 的 AWS 開發套件 (Boto3)。

安裝之後 適用於 Python (Boto3) 的 AWS SDK，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，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)
```

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

變數是資料集中的資料元素，您想要用來建立事件類型、模型和規則。

在下列範例中，CreateVariable API 用於建立兩個變數。變數為 email_address和 ip_address。將它們指派給對應的變數類型： EMAIL_ADDRESS和 IP_ADDRESS。這些變數是您上傳的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。只有具有相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

實體代表執行事件的人員，而實體類型會分類實體。範例分類包括客戶、商家或帳戶。

在下列範例中，PutEntityType API 用於建立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，並用來訓練詐騙偵測模型。此模型會學習使用這些標籤值來分類事件。

在下列範例中，PutLabel API 用於建立兩個標籤 `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，您可以建置模型來評估風險和產生個別事件的詐騙預測。事件類型會定義個別事件的結構。

在下列範例中，PutEventType API 用於建立事件類型 `sample_registration`。您可以透過指定您在上一個步驟中建立的變數 (`email_address`、`ip_address`)、實體類型 (`sample_customer`) 和標籤 (`fraud`、`legit`) 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。在上一個步驟中，您建立了事件類型。在此步驟中，您可以建立和訓練事件類型的模型。此模型可做為模型版本的容器。每次訓練模型時，都會建立新的版本。

使用下列範例程式碼來建立和訓練線上詐騙洞見模型。此模型稱為 `sample_fraud_detection_model`。這是`sample_registration`針對使用您上傳到 Amazon S3 的帳戶註冊範例資料集的事件類型。

如需 Amazon Fraud Detector 支援的不同模型類型的詳細資訊，請參閱 選擇模型類型。

建立模型

在下列範例中，CreateModel API 用於建立模型。

```
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，CreateModelVersion API 用於訓練模型。`'EXTERNAL_EVENTS'` 指定您存放範例資料集的 `trainingDataSource`和 Amazon S3 位置，以及 Amazon S3 儲存貯體的 RoleArn`externalEventsDetail`。針對 `trainingDataSchema` 參數，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://amzn-s3-demo-bucket/your-example-data-
filename.csv',
              'dataAccessRoleArn' : 'role_arn'
}
)
```

您可以多次訓練模型。每次您訓練模型時，都會建立新的版本。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指標。

檢閱模型效能

使用 Amazon Fraud Detector 的一個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，而這些資料並非用來訓練模型。它會產生模型效能分數和其他效能指標。

使用 DescribeModelVersions API 來檢閱模型效能。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。

若要進一步了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過的 Amazon Fraud Detector 模型都具有真實世界的詐騙偵測效能指標，這與本教學課程中的指標類似。

部署模型

檢閱訓練模型的效能指標後，請部署模型，並讓 Amazon Fraud Detector 產生詐騙預測。若要部署訓練模型，請使用 UpdateModelVersionStatus API。在下列範例中，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

偵測器包含偵測邏輯，例如模型和規則。此邏輯適用於您想要評估詐騙的特定事件。規則是您指定告訴 Amazon Fraud Detector 如何在預測期間解譯變數值的條件。結果是詐騙預測的結果。偵測器可以具有多個版本，每個版本的狀態為 DRAFT、ACTIVE 或 INACTIVE。偵測器版本必須至少有一個與其相關聯的規則。

使用下列範例程式碼來建立偵測器、規則、結果，以及發佈偵測器。

建立偵測器

在下列範例中，PutDetector API 用於建立`sample_registration`事件類型的`sample_detector`偵測器。

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

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

建立結果

系統會為每個可能的詐騙預測結果建立結果。在下列範例中，PutOutcome API 用於建立三個結果：`verify_customer`、 `review`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

規則包含來自資料集的一或多個變數、邏輯表達式，以及一或多個結果。

在下列範例中，CreateRule API 用於建立三種不同的規則：high_risk、 medium_risk和 low_risk。建立規則表達式，將模型效能分數sample_fraud_detection_model_insightscore值與各種閾值進行比較。這是為了判斷事件的風險層級，並指派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

偵測器版本定義用於取得詐騙預測的模型和規則。

在下列範例中，CreateDetectorVersion API 用於建立偵測器版本。它透過提供模型版本詳細資訊、規則和規則執行模式 FIRST_MATCHED 來執行此操作。規則執行模式會指定評估規則的序列。規則執行模式 FIRST_MATCHED 指定規則會先循序地評估，再持續評估，在第一次符合的規則時停止。

```
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：產生詐騙預測

本教學課程的最後一個步驟使用上一個步驟中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。回應包括模型效能分數，以及與相符規則相關聯的任何結果。

在下列範例中，GetEventPrediction API 用於提供每個請求來自單一帳戶註冊的資料。在此教學課程中，請從帳戶註冊範例資料檔案取得資料 (email_address 和 ip_address)。頂端標頭行後面的每一行（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'
}
)
```

完成本教學課程後，您執行下列動作：

- 已將範例事件資料集上傳至 Amazon S3。
- 建立變數、實體和標籤，用於建立和訓練模型。
- 使用範例資料集建立和訓練模型。

- 檢視 Amazon Fraud Detector 產生的模型效能分數和其他效能指標。
- 部署詐騙偵測模型。
- 建立偵測器並新增部署的模型。
- 已將規則、規則執行順序和結果新增至偵測器。
- 已建立偵測器版本。
- 提供不同的輸入並檢查規則和規則執行順序是否如預期般運作，以測試偵測器。

（選用）使用 Jupyter (iPython) 筆記本探索 Amazon Fraud Detector APIs

如需如何使用 Amazon Fraud Detector APIs的更多範例，請參閱 aws-fraud-detector-samples GitHub 儲存庫。筆記本涵蓋的主題包括使用 Amazon Fraud Detector APIs 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

現在您已建立模型和偵測器，您可以更深入地探索並開始建立模型和偵測器，並產生詐騙預測。

Amazon Fraud Detector 使用者指南中的下列各節說明您的企業或組織如何使用 Amazon Fraud Detector 來偵測詐騙。

- 準備並建立您的事件資料集，以訓練您的模型。
- 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 以符合您的安全和合規目標
- 監控 Amazon Fraud Detector 並記錄 Amazon Fraud Detector API 呼叫
- 對 Amazon Fraud Detector 的問題進行故障診斷

事件資料集

事件資料集是貴公司的歷史詐騙資料。您可以將此資料提供給 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 Fraud Detector 的運作方式

用於建立詐騙偵測模型的資料集提供事件的詳細資訊。事件是評估詐騙風險的商業活動。例如，帳戶註冊可以是事件。與帳戶註冊事件相關聯的資料可以是事件資料集。Amazon Fraud Detector 使用此資料集來評估帳戶註冊詐騙。

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。您也需要決定如何使用模型，並定義指標，以評估模型是否根據您的特定需求執行。

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。
- 擷取詐騙註冊以供日後調查。

在您確定目標之後，下一步是決定您想要如何使用模型。使用詐騙偵測模型來評估註冊詐騙的一些範例如下：

- 用於每個帳戶註冊的即時詐騙偵測。
- 用於每小時所有帳戶註冊的離線評估。

可用於測量模型效能的指標範例包括：

- 執行一致優於生產中的目前基準。
- 使用 Y% 誤報率擷取 X% 詐騙註冊。
- 接受最多 5% 的詐騙自動核准註冊。

事件資料集結構

Amazon Fraud Detector 要求您以 UTF-8 格式使用逗號分隔值 (CSV) 在文字檔案中提供事件資料集。CSV 資料集檔案的第一行必須包含檔案標頭。檔案標頭包含事件中繼資料和事件變數，可描述與事件相關聯的每個資料元素。標頭後面接著事件資料。每一行都包含來自單一事件的資料元素。

- 事件中繼資料 - 提供事件的相關資訊。例如，EVENT_TIMESTAMP 是指定事件發生時間的事件中繼資料。視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而定，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，請使用與 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 - 代表您想要用來建立和訓練詐騙偵測模型之事件特有的資料元素。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 可能會要求或建議您提供特定事件變數。您也可以選擇性地提供其他事件變數，讓您想要在訓練模型時包含這些變數。線上註冊事件的事件變數範例可以是電子郵件地址、IP 地址和電話號碼。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。
- 事件資料 - 代表從實際事件收集的資料。在您的 CSV 檔案中，檔案標頭後面的每一列都包含來自單一事件的資料元素。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。資料列中的每個資料元素都必須與對應的事件中繼資料或事件變數相符。

以下是 CSV 檔案的範例，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和小寫的事件變數，後面接著事件資料。資料集中的每個資料列都包含與單一帳戶註冊相關聯的資料元素，每個資料元素都與 標頭對應。

使用 Data Model Explorer 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您的詐騙偵測模型。在 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。如果資料集不符合要求，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用於業務使用案例的模型類型，並深入了解已識別模型類型的資料集需求。

資料模型瀏覽器

資料模型總管是 Amazon Fraud Detector 主控台中的工具，可讓業務使用案例與 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的資料元素洞見。開始準備事件資料集之前，請使用資料模型總管來找出 Amazon Fraud Detector 建議用於業務的模型類型，以及查看建立資料集所需的必要、建議和選用資料元素清單。

若要使用資料模型瀏覽器，

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，選擇資料模型瀏覽器。
3. 在資料模型瀏覽器頁面的業務使用案例下，選取您要評估詐騙風險的業務使用案例。
4. Amazon Fraud Detector 會顯示符合您業務使用案例的建議模型類型。模型類型定義 Amazon Fraud Detector 用來訓練詐騙偵測模型的演算法、擴充功能和轉換。

   記下建議的模型類型。稍後建立模型時，您將需要此項目。

   > **Note**
   >
   > 如果您找不到您的商業使用案例，請使用描述中的聯絡我們連結來提供商業使用案例的詳細資訊。我們建議您使用 模型類型，為您的業務使用案例建立詐騙偵測模型。

5. 資料模型洞見窗格提供必要、建議和選用資料元素的洞見，以為您的業務使用案例建立和訓練詐騙偵測模型。使用洞見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。這是因為模型預測詐騙的效能取決於資料集的品質。當您開始收集您的事件資料時，請記住資料模型瀏覽器提供給您用來建立資料集的資料元素清單。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）。也請務必決定您要包含的每個事件變數的格式，以及資料集的總大小。

事件資料集品質

若要收集模型的高品質資料集，我們建議下列事項：

- 收集成熟的資料 - 使用最新的資料有助於識別最新的詐騙模式。不過，若要偵測詐騙使用案例，請允許資料成熟。到期期間取決於您的業務，可能需要兩週到三個月的時間。例如，如果您的事件包含信用卡交易，則資料的到期時間可能取決於信用卡的扣款期間或調查人員做出決定所花費的時間。

  確保用於訓練模型的資料集有足夠的時間根據您的業務成熟。
- 確保資料分佈不會大幅偏離 - Amazon Fraud Detector 模型訓練程序範例，並根據 EVENT_TIMESTAMP 分割資料集。例如，如果您的資料集包含從過去 6 個月提取的詐騙事件，但只包含最後一個月的合法事件，則資料分佈會被視為偏離和不穩定。不穩定的資料集可能會導致模型效能評估中的偏差。如果您發現資料分佈大幅偏離，請考慮透過收集類似目前資料分佈的資料來平衡資料集。
- 確保資料集代表實作/測試模型的使用案例 - 否則，估計效能可能會偏差。假設您使用模型自動拒絕所有室內申請人，但您的模型已使用具有先前核准的歷史資料/標籤的資料集進行訓練。然後，模型的評估可能不準確，因為評估是以沒有來自遭拒申請人的表示法的資料集為基礎。

事件資料格式

Amazon Fraud Detector 會在模型訓練過程中，將大部分的資料轉換為所需的格式。不過，您可以輕鬆使用一些標準格式來提供資料，有助於在 Amazon Fraud Detector 驗證資料集之後避免發生問題。下表提供提供建議事件中繼資料格式的指引。

> **Note**
>
> 當您建立 CSV 檔案時，請務必輸入事件中繼資料名稱，如下所示，以大寫字母表示。

中繼資料名稱	格式	必要
EVENT_ID	如果提供，則必須符合下列要求： • 該事件是唯一的。 • 它代表對您的業務有意義的資訊。 • 它遵循規則表達式模式（例如，`^[0-9a-z_-]+$`.） • 除了上述要求之外，建議您不要將時間戳記附加到	取決於模型類型

中繼資料名稱	格式	必要
	EVENT_ID。當您更新事件時，這樣做可能會導致問題。這是因為如果您這樣做，必須提供完全相同的 EVENT_ID。	

中繼資料名稱	格式	必要
EVENT_TIMESTAMP	• 必須以下列其中一種格式指定： • %yyyy-%mm-%ddT %hh：%mm：%ssZ (ISO 8601 標準，僅限 UTC，無毫秒) 範例：2019-11-30T13：01：01Z • %yyyy/%mm/%dd %hh：%mm：%ss (AM/PM) 範例：2019/11/30 下午 1：01：01 或 2019/11/30 下午 13：01：01 • %mm/%dd/%yyyy %hh：%mm：%ss 範例：11/30/2019 下午 1：01：01、11/30/2019 13：01：01 • %mm/%dd/%yy %hh：%mm：%ss 範例：11/30/19 下午 1：01：01、11/30/19 下午 13：01：01 • 剖析事件時間戳記的日期/時間戳記格式時，Amazon Fraud Detector 會做出下列假設： • 如果您使用的是 ISO 8601 標準，則必須完全符合上述規格	是

中繼資料名稱	格式	必要

	• 如果您使用的是其他格式之一，則有額外的彈性：
	  • 對於月和日，您可以提供單位數或雙位數。例如，1/12/2019 是有效的日期。
	  • 如果您沒有 hh：mm：ss （也就是說，您可以直接提供日期），則不需要包含 hh：mm：ss。您也可以提供僅小時和分鐘的子集 （例如，hh：mm)。不支援僅提供小時。也不支援毫秒。
	  • 如果您提供 AM/PM 標籤，則會假設 12 小時制。如果沒有 AM/PM 資訊，則會假設 24 小時制。
	  • 您可以使用 “/” 或 “-” 做為日期元素的分隔符號。時間戳記元素會採用 “ : ”。	

ENTITY_ID	• 它必須遵循規則表達式模式：`^[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。	取決於模型類型
ENTITY_TYPE	您可以使用任何字串	取決於模型類型

中繼資料名稱	格式	必要
EVENT_LABEL	您可以使用任何標籤，例如「詐騙」、「合法」、「1」或「0」。	如果包含 LABEL_TIMESTAMP，則為必要
LABEL_TIMESTAMP	它必須遵循時間戳記格式。	如果包含 EVENT_LABEL，則為必要

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洞見 (ATI) 模型，請參閱 以取得準備和選取資料準備資料的詳細資訊。

Null 或缺少值

EVENT_TIMESTAMP 和 EVENT_LABEL 變數不得包含任何 null 值或遺失值。您可以為其他變數設定 null 值或缺少值。不過，我們建議您只對這些變數使用少量 null。如果 Amazon Fraud Detector 判斷事件變數有太多 null 值或遺失值，則會自動從您的模型省略變數。

最小變數

建立模型時，除了所需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。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要求，才能成功訓練模型。

- 至少 100 個事件的資料。
- 資料集必須包含至少 50 個歸類為詐騙的事件 （ 資料列 ）。

建議

我們建議您的資料集包含下列項目，以成功訓練模型和提升模型效能。

- 包含至少三週的歷史資料，但最多六個月的資料。
- 包含至少 10K 個總事件資料。
- 包含至少 400 個分類為詐騙的事件 （ 列 ） 和 400 個分類為合法的事件 （ 列 ）。
- 如果您的模型類型需要 ENTITY_ID，請包含超過 100 個唯一的實體。

資料集驗證

在 Amazon Fraud Detector 開始建立模型之前，它會檢查資料集中包含的變數是否符合模型的大小、格式和其他需求。如果資料集未通過驗證，則不會建立模型。您必須先修正未通過驗證的變數，再建立模型。Amazon Fraud Detector 為您提供資料分析器，可在您開始訓練模型之前，用來協助您識別和修正資料集的問題

資料描述檔

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。此自動化資料描述檔可協助您避免常見的資料準備錯誤，並識別潛在的問題，例如映射錯誤變數類型，這些問題會對模型效能造成負面影響。分析器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。它提供變數類型的指導，以及將資料集轉換為 Amazon Fraud Detector 所需格式的選項。

使用資料描述檔

自動化資料分析器是使用 AWS CloudFormation 堆疊建置而成，只要按幾下滑鼠，就能輕鬆啟動。Github 上提供所有代碼。如需有關如何使用資料分析器的資訊，請使用適用於 Amazon Fraud Detector 的自動化資料分析器，更快速地遵循部落格 Train 模型中的指示

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。執行資料描述檔後，使用此清單在建立模型之前檢查資料集是否發生錯誤。

- CSV 檔案不是 UTF-8 格式。
- 資料集中的事件數小於 100。
- 識別為詐騙或合法的事件數量少於 50 個。
- 與詐騙事件相關聯的唯一實體數量少於 100。
- EVENT_TIMESTAMP 中超過 0.1% 的值包含 Null 或支援的日期/時間戳記格式以外的值。
- EVENT_LABEL 中超過 1% 的值包含 null 或值，而非事件類型中定義的值。

- 少於兩個變數可用於模型訓練。

資料集儲存

在您收集資料集之後，您可以使用 Amazon Fraud Detector 將資料集存放在內部，或使用 Amazon Simple Storage Service (Amazon S3) 儲存在外部。我們建議您根據用於產生詐騙預測的模型，選擇存放資料集的位置。如需模型類型的詳細資訊，請參閱選擇模型類型。如需存放資料集的詳細資訊，請參閱事件資料儲存。

事件類型

使用 Amazon Fraud Detector，您可以產生事件的詐騙預測。事件類型會定義傳送至 Amazon Fraud Detector 之個別事件的結構。定義之後，您可以建置模型和偵測器，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，指定實體類型和實體 ID 來定義事件執行者。
- 變數：定義哪些變數可以作為事件的一部分傳送。模型和規則會使用變數來評估詐騙風險。新增後，便無法從事件類型中移除變數。
- 標籤：將事件分類為詐騙或合法。在模型訓練期間使用。新增後，便無法從事件類型中移除標籤。

建立事件類型

建立詐騙偵測模型之前，您必須先建立事件類型。建立事件類型涉及定義您的業務活動（事件）來評估詐騙。定義事件涉及識別要包含在資料集中的事件變數以進行詐騙評估、指定啟動事件的實體，以及分類事件的標籤。

建立事件類型的先決條件

開始建立事件類型之前，請確定您已完成下列操作：

- 使用 資料模型瀏覽器工具深入了解 Amazon Fraud Detector 建立詐騙偵測模型所需的資料元素。
- 使用您從 Data Models Explorer 取得的洞見來建立事件資料集，並將資料集上傳到 Amazon S3 儲存貯體。
- 已建立 Variables、 實體和 標籤 ，您希望 Amazon Fraud Detector 用來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內。

您可以在 Amazon Fraud Detector 主控台、使用 API、使用 AWS CLI或使用 AWS SDK 建立事件類型。

在 Amazon Fraud Detector 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。導覽至 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，選擇建立。
4. 在事件類型詳細資訊下，
   a. 在名稱中，輸入事件的名稱。
   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. 在事件變數下，
   - 在選擇如何定義此事件的變數中，
     - 如果您已為此事件建立事件變數，請從變數清單中選取變數，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 Fraud Detector 用來存取包含資料集之 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。使用類似以下內容的S3 URI路徑：`S3://your-bucket-name/example dataset filename.csv`。
       - 選擇上傳。
       - 在變數下，會顯示 Amazon Fraud Detector 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來偵測詐騙，請在變數類型中選取變數類型。選擇移除，從包含的變數中移除以進行詐騙偵測。針對清單中的每個變數重複此步驟。
6. 在標籤（選用）下，在標籤中，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 EventBridge 的事件協調下 - 選用，開啟使用 Amazon EventBridge 啟用事件協調。如需事件協調的詳細資訊，請參閱 事件協調。

   > **Note**
   >
   > 您也可以在建立事件類型之後啟用事件協調。

8. 選擇建立事件類型。

使用 建立事件類型 適用於 Python (Boto3) 的 AWS SDK

下列範例顯示 PutEventType API 的範例請求。此範例假設您已建立變數 ip_address和 email_address、標籤 legit 和 fraud，以及實體類型 sample_customer。如需如何建立這些資源的資訊，請參閱資源。

> **Note**
>
> 您必須先建立變數、實體類型和標籤，再將它們新增至事件類型。

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

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

刪除事件或事件類型

當您刪除事件時，Amazon Fraud Detector 會永久刪除該事件，且與該事件相關聯的資料不會再存放在 Amazon Fraud Detector 中。

刪除 Amazon Fraud Detector 透過 **GetEventPrediction** API 評估的事件

1. 登入 AWS Management Console 並開啟 Amazon Fraud Detector 主控台，網址為 https：//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SendEvent操作的任何事件資料，以及透過GetEventPrediction操作產生的任何預測資料。

若要刪除存放在 Amazon Fraud Detector 中但尚未評估的事件（即透過 SendEvent操作存放的事件），您必須提出DeleteEvent請求並指定事件 ID 和事件類型 ID。如果您想要同時刪除事件和與該事件相關聯的任何預測歷史記錄，請將 deleteAuditHistory 參數的值設定為「true」。當deleteAuditHistory參數設為「true」時，事件資料可在刪除操作完成後，透過搜尋取得最多 30 秒。

刪除與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. 選擇您希望刪除所有事件的事件類型。
3. 導覽至儲存的事件索引標籤，然後選擇刪除儲存的事件

根據事件類型的預存事件數量，刪除所有預存事件可能需要一些時間。例如，1 GB 資料集（一般客戶大約需要 1 到 200 萬個事件）需要大約 2 小時才能刪除。在此期間，您傳送給此事件類型的 Amazon Fraud Detector 的新事件不會儲存，但您可以透過 GetEventPrediction操作繼續產生詐騙預測。

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，或具有關聯的預存事件。在刪除事件類型之前，您必須刪除與該事件類型相關聯的所有事件。

當您刪除事件類型時，Amazon Fraud Detector 會永久刪除該事件類型，且資料不會再存放在 Amazon Fraud Detector 中。

1. 在 Amazon Fraud Detector 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

收集資料集之後，您可以使用 Amazon Fraud Detector 在內部存放資料集，或使用 Amazon Simple Storage Service (Amazon S3) 在外部存放資料集。我們建議您根據用於產生詐騙預測的模型，選擇存放資料集的位置。以下是這兩個儲存選項的詳細明細。

- 內部儲存 - 您的資料集存放於 Amazon Fraud Detector。與事件相關聯的所有事件資料都會一起存放。您可以隨時上傳存放在 Amazon Fraud Detector 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)。當您使用與 Amazon Fraud Detector 一起存放的資料集來訓練模型時，您可以指定時間範圍來限制資料集的大小。
- 外部儲存 - 您的資料集存放在 Amazon Fraud Detector 以外的外部資料來源中。目前，Amazon Fraud Detector 支援為此目的使用 Amazon Simple Storage Service (Amazon S3)。如果您的模型位於上傳至 Amazon S3 的檔案上，則該檔案不能超過 5GB 的未壓縮資料。如果超過此值，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之資料來源的詳細資訊。

模型類型	相容的訓練資料來源
線上詐騙洞見	外部儲存、內部儲存
交易詐騙洞見	內部儲存
帳戶接管洞察	內部儲存

如需使用 Amazon Simple Storage Service 在外部存放資料集的資訊，請參閱 使用 Amazon S3 將事件資料存放在外部 。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 在內部存放事件資料。

使用 Amazon S3 將事件資料存放在外部

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

> **Note**
>
> 交易詐騙洞見和帳戶接管洞見模型類型不支援使用 Amazon S3 存放在外部的資料集

建立 CSV 檔案

Amazon Fraud Detector 要求您 CSV 檔案的第一列包含資料欄標頭。CSV 檔案中的資料欄標頭必須對應至事件類型中定義的變數。如需範例資料集，請參閱 取得和上傳範例資料集

Online Fraud Insights 模型需要的訓練資料集至少具有 2 個變數，最多 100 個變數。除了事件變數之外，訓練資料集必須包含下列標頭：

- EVENT_TIMESTAMP - 定義事件發生的時間
- EVENT_LABEL - 將事件分類為詐騙或合法。資料欄中的值必須對應至事件類型中定義的值。

以下範例 CSV 資料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 資料檔案可包含雙引號和逗號做為資料的一部分。

對應的事件類型的簡化版本如下所示。事件變數對應至 CSV 檔案中的標頭，而 中的值EVENT_LABEL對應至標籤清單中的值。

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

)

事件時間戳記格式

確保您的事件時間戳記為必要格式。作為模型建置程序的一部分，線上 Fraud Insights 模型類型會根據事件時間戳記來排序您的資料，並分割您的資料以供訓練和測試之用。為了獲得效能的公平預估，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`EVENT_TIMESTAMP`期間 中值的下列日期/時間戳記格式：

- %yyyy-%mm-%ddT%hh：%mm：%ssZ （僅限無毫秒的 UTC 中的 ISO 8601 標準）

  範例：2019-11-30T13：01：01Z
- %yyyy/%mm/%dd %hh：%mm：%ss (AM/PM)

  範例：2019/11/30 下午 1：01：01 或 2019/11/30 13：01：01
- %mm/%dd/%yyyy %hh：%mm：%ss

  範例：11/30/2019 下午 1：01：01、11/30/2019 13：01：01
- %mm/%dd/%yy %hh：%mm：%ss

  範例：11/30/19 下午 1：01：01、11/30/19 13：01：01

剖析事件時間戳記的日期/時間戳記格式時，Amazon Fraud Detector 會做出下列假設：

- 如果您使用的是 ISO 8601 標準，則必須完全符合上述規格
- 如果您使用其他其中一種格式，還有其他彈性：
  - 對於月和日，您可以提供單位數或雙位數。例如，1/12/2019 是有效的日期。
  - 如果您沒有 hh：mm：ss (taht 是您可以直接提供日期），則不需要包含 hh：mm：ss。您也可以提供僅小時和分鐘的子集（例如，hh：mm)。不支援僅提供小時。也不支援毫秒。
  - 如果您提供 AM/PM 標籤，則會假設 12 小時制。如果沒有 AM/PM 資訊，則會假設 24 小時制。
  - 您可以使用 "/" 或 "-" 做為日期元素的分隔符號。時間戳記元素會採用 "："。

跨時間取樣資料集

我們建議您提供相同時間範圍內的詐騙和合法範例。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

能會收到以下錯誤：「跨時間的詐騙分佈不可接受的波動。無法正確分割資料集。」 一般而言，此錯誤的最簡單修正方式是確保詐騙事件和合法事件在相同的時間範圍內進行平均抽樣。如果您在短時間內發生詐騙大幅遽增，您可能也需要移除資料。

如果您無法產生足夠的資料來建立平均分佈的資料集，其中一種方法是隨機化事件的 EVENT_TIMESTAMP，使其平均分佈。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。

Null 和遺失值

Amazon Fraud Detector 會處理 null 值和遺失值。不過，變數的 null 百分比應該受到限制。EVENT_TIMESTAMP 和 EVENT_LABEL 資料欄不應包含任何缺少的值。

檔案驗證

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

- 如果無法剖析 CSV
- 如果資料欄的資料類型不正確

將事件資料上傳至 Amazon S3 儲存貯體

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

上傳到 Amazon S3 儲存貯體

1. 登入 AWS Management Console 並開啟位於 https：//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資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的儲存貯體命名規則。

> **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. 在區域中，選擇您要儲存貯體所在的 AWS 區域。您必須選取使用 Amazon Fraud Detector 的相同區域，即美國東部（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）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狀態。如需封鎖公開存取的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的封鎖對 Amazon S3 儲存體的公開存取。
6. 選擇建立儲存貯體。
7. 將訓練資料檔案上傳至您的 Amazon S3 儲存貯體。請注意訓練檔案的 Amazon S3 位置路徑（例如 s3：//bucketname/object.csv)。

使用 Amazon Fraud Detector 在內部存放事件資料

您可以選擇將事件資料儲存在 Amazon Fraud Detector 中，並在稍後使用儲存的資料來訓練模型。透過將事件資料儲存在 Amazon Fraud Detector 中，您可以訓練使用自動計算變數來改善效能、簡化模型重新訓練，以及更新詐騙標籤以關閉機器學習回饋迴圈的模型。事件會存放在事件類型資源層級，因此相同事件類型的所有事件都會一起存放在單一事件類型資料集中。在定義事件類型時，您可以選擇在 Amazon Fraud Detector 主控台中切換事件擷取設定，以指定是否要存放該事件類型的事件。

您可以在 Amazon Fraud Detector 中存放單一事件或匯入大量事件資料集。您可以使用 GetEventPrediction API 或 SendEvent API 串流單一事件。使用 Amazon Fraud Detector 主控台中的批次匯入功能或使用 CreateBatchImportJob API，即可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 主控台來檢查已為每個事件類型存放的事件數量。

準備儲存的事件資料

Amazon Fraud Detector 內部存放的事件資料會存放在Event Type資源層級。因此，來自相同事件的所有事件資料都會存放在單一 中Event Type。儲存的事件稍後可用於訓練新模型或重新訓練現有模型。使用儲存的事件資料訓練模型時，您可以選擇指定事件的時間範圍，以限制訓練資料集的大小。

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

使用 Amazon Fraud Detector 在內部儲存資料的先決條件

- 為了確保您的事件資料通過驗證且資料集成功儲存，請確定您已使用 Data Model Explorer 提供的洞見來準備資料集。
- 為您要與 Amazon Fraud Detector 一起存放的事件資料建立事件類型。如果您還沒有，請遵循指示來建立事件類型。

智慧資料驗證

當您在 Amazon Fraud Detector 主控台中上傳資料集以進行批次匯入時，Amazon Fraud Detector 會使用智慧型資料驗證 (SDV) 在匯入資料之前驗證資料集。SDV 會掃描上傳的資料檔案，並識別遺失資料、格式不正確或資料類型等問題。除了驗證資料集之外，SDV 也提供驗證報告，列出已識別的所有問題，並建議採取動作來修正最具影響力的問題。SDV 識別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，請參閱智慧資料驗證報告。

SDV 會在檔案層級和資料（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問題，例如存取檔案的許可不足、檔案大小不正確、檔案格式和標頭（事件中繼資料和事件變數）。在資料層級，SDV 會掃描每個事件資料（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適用於 Amazon Fraud Detector 主控台，且預設會開啟驗證。如果您不希望 Amazon Fraud Detector 在匯入資料集之前使用智慧資料驗證，請在上傳資料集時關閉 Amazon Fraud Detector 主控台中的驗證。

使用 APIs或 AWS SDK 驗證儲存的資料

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

- 該事件類型的 EventIngestion 設定為 ENABLED。

- 無法更新事件時間戳記。具有重複事件 ID 和不同 EVENT_TIMESTAMP 的事件將被視為錯誤。
- 變數名稱和值符合其預期的格式。如需詳細資訊，請參閱建立變數
- 必要的變數會填入值。
- 所有事件時間戳記都不會超過 18 個月，也不會在未來。

使用批次匯入存放事件資料

使用批次匯入功能，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，請以 CSV 格式建立包含所有事件資料的輸入檔案，將 CSV 檔案上傳至 Amazon S3 儲存貯體，然後啟動匯入任務。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。匯入資料後，即可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 檔案必須包含符合相關聯事件類型中定義的變數加上四個必要變數的標頭。如需詳細資訊，請參閱準備儲存的事件資料。輸入資料檔案的大小上限為 20 GB (GB) 或約 5000 萬個事件。事件數量將根據您的事件大小而有所不同。如果匯入任務成功，則輸出檔案為空。如果匯入失敗，輸出檔案會包含錯誤日誌。

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聯事件類型中定義的變數完全相符的資料欄標頭，以及四個強制性變數：EVENT_ID、EVENT_TIMESTAMP、ENTITY_ID 和 ENTITY_TYPE。您也可以選擇性地包含 EVENT_LABEL 和 LABEL_TIMESTAMP（如果包含 EVENT_LABEL，則需要 LABEL_TIMESTAMP)。

定義強制性變數

強制性變數視為事件中繼資料，必須以大寫指定。事件中繼資料會自動包含在模型訓練中。下表列出強制變數、每個變數的描述，以及變數的必要格式。

名稱	描述	要求
EVENT_ID	事件的識別符。例如，如果您的事件是線上交易，EVENT	• 批次匯入任務需要 EVENT_ID。 • 該事件必須是唯一的。

名稱	描述	要求
	_ID 可能是提供給您客戶的交易參考號碼。	• 它應該代表對您的業務有意義的資訊。 • 它必須符合規則表達式模式（例如，`^[0-9a-z_-]+$`.） • 我們不建議您將時間戳記附加至 EVENT_ID。當您更新事件時，這樣做可能會導致問題。這是因為如果您這樣做，必須提供完全相同的 EVENT_ID。

名稱	描述	要求
EVENT_TIMESTAMP	事件發生時的時間戳記。時間戳記必須在 UTC 的 ISO 8601 標準中。	• 批次匯入任務需要 EVENT_TIMESTAMP。 • 必須以下列其中一種格式指定： • %yyyy-%mm-%ddT %hh：%mm：%ssZ（僅限無毫秒的 UTC 中的 ISO 8601 標準） 範例：2019-11-30T13：01：01Z • %yyyy/%mm/%dd %hh：%mm：%ss (AM/PM) 範例：2019/11/30 下午 1：01：01 或 2019/11/30 13：01：01 • %mm/%dd/%yyyy %hh：%mm：%ss 範例：11/30/2019 下午 1：01：01、11/30/2019 13：01：01 • %mm/%dd/%yy %hh：%mm：%ss 範例：11/30/19 下午 1：01：01、11/30/19 下午 13：01：01 • 剖析事件時間戳記的日期/時間戳記格式時，Amazon Fraud Detector 會做出下列假設：

名稱	描述	要求

		• 如果您使用的是 ISO 8601 標準，則必須完全符合上述規格
		• 如果您使用的是其他其中一種格式，還有其他彈性：
		  • 對於月和日，您可以提供單位數或雙位數。例如，1/12/2019 是有效的日期。
		  • 如果您沒有 hh：mm：ss（也就是說，您可以直接提供日期），則不需要包含 hh：mm：ss。您也可以提供僅小時和分鐘的子集（例如，hh：mm)。不支援僅提供小時。也不支援毫秒。
		  • 如果您提供 AM/PM 標籤，則會假設 12 小時制。如果沒有 AM/PM 資訊，則會假設 24 小時制。
		  • 您可以使用「/」或「-」做為日期元素的分隔符號。時間戳記元素會採用「：」。

名稱	描述	要求
ENTITY_ID	執行事件之實體的識別符。	• 批次匯入任務需要 ENTITY_ID • 它必須遵循規則表達式模式：`^[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。
ENTITY_TYPE	執行事件的實體，例如商家或客戶	批次匯入任務需要 ENTITY_TYPE
EVENT_LABEL	將事件分類為 `fraudulent` 或 `legitimate`	如果包含 LABEL_TIMESTAMP，則需要 EVENT_LABEL
LABEL_TIMESTAMP	事件標籤上次填入或更新的時間戳記	• 如果包含 EVENT_LABEL，則需要 LABEL_TIMESTAMP。 • 它必須遵循時間戳記格式。

將 CSV 檔案上傳至 Amazon S3 以進行批次匯入

使用資料建立 CSV 檔案後，請將檔案上傳至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。

將事件資料上傳至 Amazon S3 儲存貯體

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/s3/ 開啟 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資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的儲存貯體命名規則。

> **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. 在區域中，選擇您要儲存貯體所在的 AWS 區域。您必須選取您使用 Amazon Fraud Detector 的相同區域，即美國東部（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）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狀態。如需封鎖公開存取的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的封鎖對 Amazon S3 儲存體的公開存取。
6. 選擇建立儲存貯體。
7. 將訓練資料檔案上傳至您的 Amazon S3 儲存貯體。請注意訓練檔案的 Amazon S3 位置路徑（例如 s3：//bucketname/object.csv)。

Amazon Fraud Detector 主控台中的批次匯入事件資料

您可以使用 `CreateBatchImportJob` API 或使用 AWS 開發套件，在 Amazon Fraud Detector 主控台中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。請確定您也將 CSV 檔案上傳到 Amazon S3 儲存貯體。

使用 Amazon Fraud Detector 主控台

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，然後導覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中，選擇事件。
3. 選擇您的事件類型。
4. 選取儲存的事件索引標籤。
5. 在儲存的事件詳細資訊窗格中，確定事件擷取為 ON。
6. 在匯入事件資料窗格中，選擇新匯入。
7. 在新事件匯入頁面中，提供下列資訊：
   - 【建議】 保留此資料集的啟用智慧資料驗證 - 將新設定為預設設定。
   - 針對資料的 IAM 角色，選取您為 Amazon S3 儲存貯體建立的 IAM 角色，該儲存貯體包含您計劃匯入的 CSV 檔案。
   - 針對輸入資料位置，輸入您擁有 CSV 檔案的 S3 位置。
   - 如果您想要指定個別位置來存放匯入結果，請按一下用於輸入和結果的個別資料位置按鈕，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，並將許可寫入輸出 Amazon S3 儲存貯體。

8. 選擇 開始使用。
9. 匯入事件資料窗格中的狀態欄會顯示驗證和匯入任務的狀態。當您的資料集先通過驗證，然後匯入時，頂端的橫幅會提供狀態的高階描述。
10. 遵循提供給 的指引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 預設會在匯入之前驗證您的資料集。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。頁面頂端的橫幅提供驗證問題清單和匯入任務狀態的簡短描述。根據驗證問題清單和匯入任務的狀態，您可能需要採取動作，以確保成功驗證和匯入資料集。

下表根據驗證和匯入操作的結果，提供您必須採取之動作的詳細資訊。

橫幅訊息	Status	代表什麼意思	我應該做什麼
資料驗證已開始	驗證進行中	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。修正資料檔案中的錯誤，並啟動新的匯入任務。如需詳細資訊，請參閱驗證報告	驗證失敗	SDV 已識別資料檔案中的問題。必須解決這些問題，才能成功匯入您的資料集。	在匯入事件資料窗格中，選取任務 ID 並檢視驗證報告。遵循報告中的建議來解決所有列出的錯誤。如需詳細資訊，請參閱使用驗證報告。
資料匯入已開始。驗證已成功完成	匯入進行中	您的資料集已通過驗證。AFD 已開始匯入您的資料集	等待狀態變更
驗證已完成，並出現警告。資料匯入已開始	匯入進行中	資料集中的部分資料驗證失敗。不過，通過驗證的資料符合匯入的最低資料大小要求。	監控橫幅中的訊息，並等待狀態變更
您的資料已部分匯入。部分資料未通過驗證且未匯入。如需詳細資訊，請參閱驗證報告。	已匯入。狀態會顯示警告圖示。	資料檔案中失敗驗證的部分資料並未匯入。已匯入通過驗證的其餘資料。	在匯入事件資料窗格中，選取任務 ID 並檢視驗證報告。請遵循資料層級警告表格中的建議，以處理列出的警告。您不需要處理所有警告。不過，請確定您的資料集有超過 50% 的資料通過驗證才能成功匯

橫幅訊息	Status	代表什麼意思	我應該做什麼
			入。解決警告之後，請啟動新的匯入任務。如需詳細資訊，請參閱使用驗證報告。
由於處理錯誤，資料匯入失敗。啟動新的資料匯入任務	匯入失敗	由於暫時性執行時間錯誤，匯入失敗	啟動新的匯入任務
已成功匯入資料	已匯入	驗證和匯入都成功完成	選取匯入任務的任務 ID 以檢視詳細資訊，然後繼續模型訓練

> **Note**
>
> 我們建議您在資料集成功匯入 Amazon Fraud Detector 後等待 10 分鐘，以確保系統完全擷取它們。

智慧資料驗證報告

智慧資料驗證會在驗證完成後建立驗證報告。驗證報告提供 SDV 在資料集中識別的所有問題的詳細資訊，並提供建議的動作來修正最具影響力的問題。您可以使用驗證報告來判斷問題是什麼、問題在資料集中的位置、問題的嚴重性，以及如何修正這些問題。即使驗證成功完成，也會建立驗證報告。在這種情況下，您可以檢視報告，以查看是否有任何列出的問題，如果有的話，請決定您是否要修正其中任何問題。

> **Note**
>
> 目前版本的 SDV 會掃描資料集，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，您的資料集仍有可能導致模型訓練失敗的問題。即使驗證和匯入成功，仍建議您檢視驗證報告，並解決報告中列出的任何問題，以成功訓練模型。解決問題後，請建立新的批次匯入任務。

存取驗證報告

您可以在驗證完成後，使用下列其中一個選項隨時存取驗證報告：

1. 驗證完成後，並在匯入任務進行時，在頂端橫幅中，選擇檢視驗證報告。
2. 匯入任務完成後，在匯入事件資料窗格中，選擇剛完成之匯入任務的任務 ID。

使用驗證報告

匯入任務的驗證報告頁面提供此匯入任務的詳細資訊、找到任何重大錯誤的清單、找到資料集中特定事件（資料列）的警告清單，以及包含無效值和每個變數缺少值等資訊的資料集簡短摘要。

- 匯入任務詳細資訊

  提供匯入任務的詳細資訊。如果您的匯入任務失敗或資料集已部分匯入，請選擇移至結果檔案，以檢視無法匯入之事件的錯誤日誌。

- 嚴重錯誤

  提供 SDV 所識別之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，才能繼續匯入。如果您嘗試匯入資料集而不解決關鍵問題，匯入任務可能會失敗。

  若要解決關鍵問題，請遵循針對每個警告提供的建議。在您解決重大錯誤窗格中列出的所有問題之後，請建立新的批次匯入任務。

- 資料層級警告

  提供資料集中特定事件（資料列）的警告摘要。如果已填入資料層級警告窗格，表示資料集中的某些事件驗證失敗，且未匯入。

  對於每個警告，描述欄會顯示有問題的事件數量。而範例事件 IDs 會提供範例事件 IDs的部分清單，您可以用來做為起點，以找出有問題的其餘事件。使用針對警告提供的建議來修正問題。也請使用輸出檔案中的錯誤日誌，以取得有關問題的其他資訊。錯誤日誌會針對批次匯入失敗的所有事件產生。若要存取錯誤日誌，請在匯入任務詳細資訊窗格中，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，匯入任務也會失敗。在此情況下，您必須先修正資料，才能開始新的匯入任務。

- 資料集摘要

  提供資料集的驗證報告摘要。如果警告數目欄顯示超過 0 個警告，請決定您是否需要修正這些警告。如果警告數目欄顯示 0 秒，請繼續訓練您的模型。

使用適用於 Python 的 AWS 開發套件 (Boto3) 批次匯入事件資料

下列範例顯示 CreateBatchImportJob API 的範例請求。批次匯入任務必須包含 jobID、inputPath、outputPath、 eventTypeName 和 iamRoleArn。除非任務處於 CREATE_FAILED 狀態，否則 jobID 不能包含過去任務的相同 ID。inputPath 和 outputPath 必須是有效的 S3 路徑。您可以選擇不在 outputPath 中指定檔案名稱，不過，您仍然需要提供有效的 S3 儲存貯體位置。eventTypeName 和 iamRoleArn 必須存在。IAM 角色必須授予輸入 Amazon S3 儲存貯體的讀取許可，以及輸出 Amazon S3 儲存貯體的寫入許可。

```
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-*************'
)
```

取消批次匯入任務

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

若要在主控台中取消批次匯入任務，

1. 開啟 AWS 主控台並登入您的帳戶，然後導覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中，選擇事件。
3. 選擇您的事件類型。
4. 選取儲存的事件索引標籤。
5. 在匯入事件資料窗格中，選擇您要取消之進行中匯入任務的任務 ID。

6. 在事件任務頁面中，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任務。

使用適用於 Python 的 AWS 開發套件 (Boto3) 取消批次匯入任務

下列範例顯示 CancelBatchImportJob API 的範例請求。取消匯入任務必須包含進行中批次匯入任務的任務 ID。

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

使用 GetEventPredictions API 操作存放事件資料

根據預設，傳送至 GetEventPrediction API 進行評估的所有事件都會存放在 Amazon Fraud Detector 中。這表示當您產生預測時，Amazon Fraud Detector 會自動儲存事件資料，並使用該資料近乎即時地更新計算的變數。您可以在 Amazon Fraud Detector 主控台中導覽至事件類型，並使用 PutEventType API 操作設定事件擷取關閉或將 EventIngestion 值更新為 DISABLED，以停用資料儲存。如需 GetEventPrediction API 操作的詳細資訊，請參閱 詐騙預測。

> **Important**
>
> 我們強烈建議您為事件類型啟用事件擷取後，請保持啟用狀態。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 操作存放事件資料

您可以使用 SendEvent API 操作在 Amazon Fraud Detector 中存放事件，而無需產生這些事件的詐騙預測。例如，您可以使用 SendEvent操作上傳歷史資料集，以供稍後用來訓練模型。

SendEvent API 的事件時間戳記格式

使用 SendEvent API 儲存事件資料時，您必須確保事件時間戳記的格式為必要。Amazon Fraud Detector 支援下列日期/時間戳記格式：

- %yyyy-%mm-%ddT%hh：%mm：%ssZ（僅限無毫秒的 UTC 中的 ISO 8601 標準）

  範例：2019-11-30T13：01：01Z

- %yyyy/%mm/%dd %hh：%mm：%ss (AM/PM)

  範例：2019/11/30 下午 1：01：01 或 2019/11/30 13：01：01

- %mm/%dd/%yyyy %hh：%mm：%ss

  範例：11/30/2019 下午 1：01：01、11/30/2019 13：01：01

- %mm/%dd/%yy %hh：%mm：%ss

  範例：11/30/19 下午 1：01：01、11/30/19 13：01：01

剖析事件時間戳記的日期/時間戳記格式時，Amazon Fraud Detector 會做出下列假設：

- 如果您使用的是 ISO 8601 標準，則必須完全符合上述規格
- 如果您使用其他其中一種格式，還有其他彈性：
  - 對於月和日，您可以提供單位數或雙位數。例如，1/12/2019 是有效的日期。
  - 如果您沒有 hh：mm：ss（也就是說，您可以直接提供日期），則不需要包含 hh：mm：ss。您也可以提供僅小時和分鐘的子集（例如，hh：mm)。不支援僅提供小時。也不支援毫秒。
  - 如果您提供 AM/PM 標籤，則會假設 12 小時制。如果沒有 AM/PM 資訊，則會假設 24 小時制。
  - 您可以使用 "/" 或 "-" 做為日期元素的分隔符號。時間戳記元素會採用 "："。

以下是 SendEvent API 呼叫的範例。

```
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'}],

)
```

取得預存事件資料的詳細資訊

在 Amazon Fraud Detector 中存放事件資料之後，您可以使用 GetEvent API 檢查為事件存放的最新資料。下列範例程式碼會檢查為sample_registration事件存放的最新資料。

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

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

檢視預存事件資料集的指標

對於每個事件類型，您可以在 Amazon Fraud Detector 主控台中檢視指標，例如儲存事件的數量、儲存事件的總大小，以及最早和最新儲存事件的時間戳記。

若要檢視 事件類型的預存事件指標，

1. 開啟 AWS 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，選擇事件。
3. 選擇您的事件類型。
4. 選取儲存的事件索引標籤。
5. 儲存的事件詳細資訊窗格會顯示指標。這些指標每天會自動更新一次。
6. 或者，按一下重新整理事件指標以手動更新您的指標。

> **Note**
>
> 如果您剛匯入資料，建議您在完成匯入資料後等待 5 到 10 分鐘，以重新整理和檢視指標。

事件協調

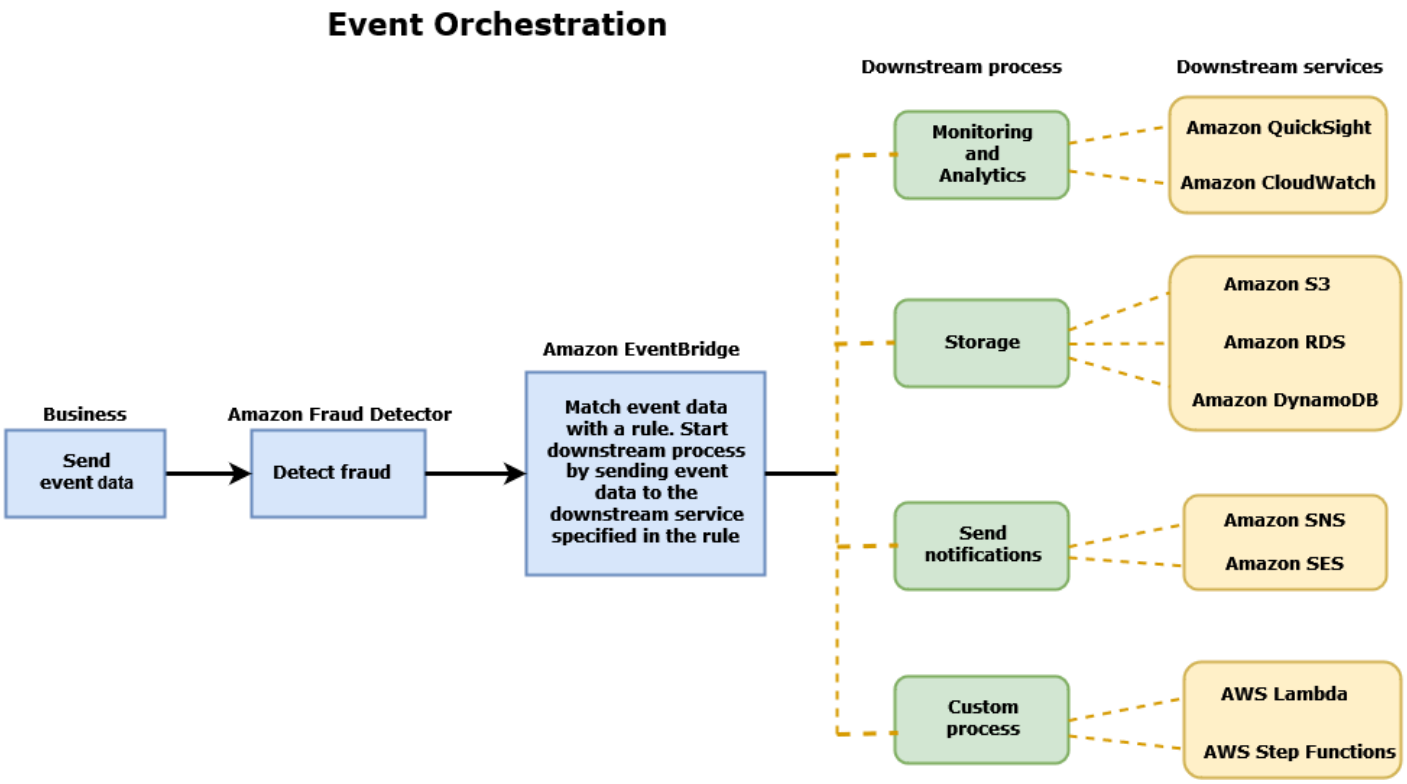
事件協調可讓您使用 Amazon EventBridge 輕鬆將事件傳送至 AWS 服務 以進行下游處理。Amazon Fraud Detector 為您提供簡單的規則，您可以在詐騙偵測後自動處理事件。透過事件協調，您可以自動化下游事件程序，例如，將事件傳送至儀表板，從事件資料中取得洞見、根據詐騙偵測結果產生通知，以及根據從詐騙偵測中學習來更新事件標籤。

事件協調可透過 Amazon EventBridge 輕鬆存取 AWS 環境中的服務。您可以設定 Amazon EventBridge 以直接傳送事件至 API 目的地 AWS 服務 ，或使用 API 目的地間接傳送事件。 https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-api-destinations.html AWS 服務 您用來協調下游程序的 也稱為目標。您可以使用 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
- 儲存：Amazon S3、Amazon RDS、Amazon DynamoDB
- 用於傳送通知 — Amazon SNS、Amazon SES
- 用於自訂處理：AWS Lambda、AWS Step Functions

如需 Amazon EventBridge 支援之協調目標的詳細資訊，請參閱 Amazon EventBridge 目標。

下圖提供事件協調運作方式的高階檢視。



設定事件協調

為事件設定事件協調需要您在目標服務中設定程序、設定 Amazon EventBridge 接收和傳送事件資料，以及在 Amazon EventBridge 中建立規則，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：

設定事件協調

1. 前往 Amazon EventBridge 使用者指南，了解如何使用 Amazon EventBridge。請務必了解如何在 Amazon EventBridge 中為您的使用案例建立規則。
2. 請遵循 的指示在 Amazon Fraud Detector 中啟用事件協調。

   > **Note**
   >
   > 事件的事件協調預設為停用。

3. 設定您的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. 遵循建立 Amazon EventBridge 規則的指示。

> **Important**
>
> 在 Amazon EventBridge 中建置事件模式時，請務必`aws.frauddetector`為來源欄位和`Event Prediction Result Returned`詳細資訊類型欄位提供 。

在 Amazon Fraud Detector 中啟用事件協調

您可以在建立事件類型時或建立事件類型之後，為事件啟用事件協調。您可以在 Amazon Fraud Detector 主控台、使用 `put-event-type`命令、使用 `PutEventType` API 或使用 來啟用事件協調 適用於 Python (Boto3) 的 AWS SDK。

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。如果您要建立新的事件類型並想要啟用協調，請遵循的指示建立事件類型。

啟用事件協調

1. 開啟 AWS 管理主控台並登入您的帳戶。導覽至 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。
5. 繼續執行 的步驟 3 說明設定事件協調。

使用 啟用事件協調 適用於 Python (Boto3) 的 AWS SDK

下列範例顯示更新事件類型`sample_registration`以啟用事件協調的範例請求。此範例使用 `PutEventType` API，並假設您已建立變數 `ip_address`和 `email_address`、標籤 `legit`和 `fraud`，以及實體類型 `sample_customer`。如需如何建立這些資源的資訊，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'])
```

在 Amazon Fraud Detector 中停用事件協調

您可以在 Amazon Fraud Detector 主控台、使用 `put-event-type`命令、使用 `PutEventType` API 或使用 ，隨時停用事件的事件協調 適用於 Python (Boto3) 的 AWS SDK。

在 Amazon Fraud Detector 主控台中停用事件協調

停用事件協調

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。

使用 停用事件協調 適用於 Python (Boto3) 的 AWS SDK

下列範例顯示使用 `PutEventType` API 更新事件類型`sample_registration`以停用事件協調的範例請求。

```
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，然後準備和提供將用於訓練模型的資料。

選擇模型類型

Amazon Fraud Detector 提供下列模型類型。選擇適用於您的使用案例的模型類型。

- 線上詐騙洞見

  Online Fraud Insights 模型類型經過最佳化，可在幾乎沒有評估實體的歷史資料時偵測詐騙，例如，新客戶在線上註冊新帳戶。
- 交易詐騙洞見

  Transaction Fraud Insights 模型類型最適合用於偵測詐騙使用案例，其中正在評估的實體可能有互動歷史記錄，而模型可以分析這些歷史記錄，以改善預測準確性 （例如，過去購買歷史記錄的現有客戶）。
- 帳戶接管洞見

  Account Takeover Insights 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。遭盜用帳戶的登入資料，例如用於登入的瀏覽器和裝置，與與帳戶相關聯的歷史登入資料不同。

線上詐騙洞見

Online Fraud Insights 是一種受監督的機器學習模型，這表示它使用詐騙和合法交易的歷史範例來訓練模型。線上詐騙洞見模型可以根據很少的歷史資料偵測詐騙。模型的輸入具有彈性，因此您可以進行調整，以偵測各種詐騙風險，包括仿造評論、促銷濫用和訪客結帳詐騙。

Online Fraud Insights 模型使用機器學習演算法的集合，以進行資料擴充、轉換和詐騙分類。作為模型訓練程序的一部分，Online Fraud Insights 會使用第三方資料來豐富原始資料元素，例如 IP 地址和 BIN 號碼，例如 IP 地址的地理位置或信用卡的發行銀行。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，將 Amazon 和 所見的詐騙模式納入考量 AWS。這些詐騙模式會使用漸層樹增強演算法，成為模型的輸入功能。

為了提高效能，線上 Fraud Insights 會透過貝葉斯最佳化程序來最佳化漸層樹狀增強演算法的超參數。它會依序訓練數十種具有不同模型參數的不同模型（例如樹的數量、樹的深度，以及每個分葉的樣本數量）。它也使用不同的最佳化策略，例如增加少數族群詐騙人口的權重，以處理極低的詐騙率。

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 目前支援的外部儲存體是 Amazon Simple Storage Service (Amazon S3)。如果您的 使用外部儲存，您的事件資料集必須以逗號分隔值 (CSV) 格式上傳至 Amazon S3 儲存貯體。在模型訓練組態中，這些資料儲存選項稱為 EXTERNAL_EVENTS（適用於外部儲存） 和 INGESTED_EVENTS（適用於內部儲存）。如需可用資料來源以及如何將資料存放在其中的詳細資訊，請參閱事件資料儲存。

準備資料

無論您選擇存放事件資料的位置為何 (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頭 EVENT_LABEL。此變數會將事件分類為詐騙或合法。使用 CSV 檔案（外部儲存） 時，您必須為檔案中的每個事件包含 EVENT_LABEL。對於內部儲存，EVENT_LABEL 欄位是選用的，但所有事件都必須加上標籤，才能包含在訓練資料集內。設定模型訓練時，您可以選擇是否忽略未標記的事件、擔任未標記事件的合法標籤，或擔任所有未標記事件的詐騙標籤。

選取資料

請參閱收集事件資料，以取得選擇資料以訓練線上詐騙洞見模型的相關資訊。

Online Fraud Insights 訓練會根據 EVENT_TIMESTAMP 處理範例和分割歷史資料。您不需要手動取樣資料，這樣做可能會對您的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之外，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，每個模型最多允許 100 個變數。一般而言，您提供的變數越多，模型越能區分詐騙和合法事件。雖然 Online Fraud Insights 模型可以支援數十個變數，包括自訂變數，但我們建議您包含 IP 地址和電子郵件地址，因為這些變數通常最有效地識別要評估的實體。

驗證資料

在訓練程序中，線上詐騙洞見會驗證資料集，找出可能影響模型訓練的資料品質問題。驗證資料之後，Amazon Fraud Detector 將採取適當的動作來建置最佳的模型。這包括發出潛在資料品質問題的警

告、自動移除具有資料品質問題的變數，或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。

交易詐騙洞見

Transaction Fraud Insights 模型類型旨在偵測線上或card-not-present交易詐騙。Transaction Fraud Insights 是受監督的機器學習模型，這表示它使用詐騙和合法交易的歷史範例來訓練模型。

Transaction Fraud Insights 模型使用機器學習演算法的集合，以進行資料擴充、轉換和詐騙分類。它利用特徵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， Transaction Fraud Insights 會使用第三方資料來豐富原始資料元素，例如 IP 地址和 BIN 號碼，例如 IP 地址的地理位置或信用卡的發行銀行。除了第三方資料之外， Transaction Fraud Insights 還使用深度學習演算法，將 Amazon 所見的詐騙模式納入考量，而 AWS 這些詐騙模式會使用漸層樹增強演算法，成為模型的輸入功能。

為了提高效能， Transaction Fraud Insights 會透過貝葉斯最佳化程序最佳化漸層樹增強演算法的超參數、使用不同的模型參數（例如樹木數量、樹木深度、每個分葉的樣本數量）依序訓練數十種不同的模型，以及諸如將少數族群權重化以處理極低的詐騙率等不同的最佳化策略。

作為模型訓練程序的一部分，交易詐騙模型的特徵工程引擎會計算訓練資料集內每個唯一實體的值，以協助改善詐騙預測。例如，在訓練過程中，Amazon Fraud Detector 會計算和存放實體上次進行購買的時間，並在每次呼叫 `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，以預測交易是否詐騙。

選取資料來源

Transaction Fraud Insights 模型僅針對使用 Amazon Fraud Detector (INGESTED_EVENTS) 內部存放的資料集進行訓練。這可讓 Amazon Fraud Detector 持續更新您正在評估之實體的計算值。如需可用資料來源的詳細資訊，請參閱 事件資料儲存

準備資料

在您訓練 Transaction Fraud Insights 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。Transaction Fraud Insights 模型會將收到的新實體與資料集中的詐騙和合法實體範例進行比較，因此為每個實體提供許多範例很有幫助。

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

選取資料

根據預設， Transaction Fraud Insights 會針對您選取的事件類型，針對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成熟。也就是說，已過足夠的時間，以確保合法和詐騙記錄已正確識別。例如，針對扣款詐騙，通常需要 60 天或更久的時間才能正確識別詐騙事件。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。

您不需要選取代表理想詐騙率的時間範圍。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。

如果您選擇的事件不足而無法成功訓練模型的時間範圍，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 欄位是選用的，但事件必須加上標籤，才能包含在訓練資料集中。設定模型訓練時，您可以選擇是否忽略未標記的事件、擔任未標記事件的合法標籤，或擔任未標記事件的詐騙標籤。

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，模型越能區分詐騙和合法事件。雖然 Transaction Fraud Insight 模型可以支援數十個變數，包括自訂變數，但我們建議您包含 IP 地址、電子郵件地址、付款工具類型、訂單價格和卡片 BIN。

驗證資料

在訓練過程中， Transaction Fraud Insights 會驗證訓練資料集是否有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置最佳的模型。這包括發出潛在資料品質問題的警告、自動移除具有資料品質問題的變數，或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。

如果唯一實體的數量小於 1，500，Amazon Fraud Detector 會發出警告，但會繼續訓練模型，因為這可能會影響訓練資料的品質。如果您收到警告，請檢閱效能指標。

帳戶接管洞察

帳戶接管洞察 (ATI) 模型類型透過偵測帳戶是否透過惡意接管、網路釣魚或遭竊的登入資料入侵，來識別詐騙線上活動。Account Takeover Insights 是一種機器學習模型，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嵌入訓練過的 Account Takeover Insights 模型，以偵測帳戶是否遭到入侵。此模型會評估各種身分驗證和登入類型。其中包括 Web 應用程式登入、API 型身分驗證和

single-sign-on(SSO)。若要使用 Account Takeover Insights 模型，請在顯示有效的登入憑證後呼叫 GetEventPrediction API。API 會產生分數，以量化帳戶遭到入侵的風險。Amazon Fraud Detector 會使用分數和您定義的規則，來傳回一或多個登入事件的結果。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動作。也就是說，您可以核准或挑戰為登入提供的登入資料。例如，您可以要求帳戶 PIN 做為額外的驗證，來挑戰登入資料。

您也可以使用 Account Takeover Insights 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，供人工審核人員判斷是否需要採取進一步動作，例如暫停帳戶。

Account Takeover Insights 模型使用包含您業務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詐騙。不過，這並非訓練模型的必要條件。帳戶接管洞見模型會根據帳戶成功登入的歷史記錄偵測異常。其也會了解如何偵測使用者行為中的異常情況，而這些異常情況顯示惡意帳戶接管事件的風險增加。例如，通常從相同裝置集和 IP 地址登入的使用者。詐騙者通常會從不同的裝置和地理位置登入。此技術會產生異常活動的風險分數，通常是惡意帳戶接管的主要特徵。

在訓練 Account Takeover Insights 模型之前，Amazon Fraud Detector 會使用機器學習技術的組合來執行資料擴充、資料彙總和資料轉換。然後，在訓練過程中，Amazon Fraud Detector 會充實您提供的原始資料元素。原始資料元素的範例包括 IP 地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 地址登入的次數。Amazon Fraud Detector 可以使用這些額外的擴充功能和彙總功能，從登入事件的一小組輸入產生強大的模型效能。

Account Takeover Insights 模型會偵測由不良行為者存取合法帳戶的執行個體，無論該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記為高風險帳戶。您可以透過兩種方式之一來處理高風險帳戶。您可以強制執行額外的身分驗證。或者，您可以將帳戶傳送至佇列以進行手動調查。

選取資料來源

Account Takeover Insights 模型是在 Amazon Fraud Detector 內部存放的資料集上進行訓練。若要使用 Amazon Fraud Detector 存放您的登入事件資料，請使用 使用者的登入事件建立 CSV 檔案。對於每個事件，請包含登入資料，例如事件時間戳記、使用者 ID、IP 地址、使用者代理程式，以及登入資料是否有效。建立 CSV 檔案後，請先將檔案上傳至 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 存放事件資料集的詳細資訊，請參閱 使用 Amazon Fraud Detector 在內部存放事件資料

準備資料

Amazon Fraud Detector 要求您以以 UTF-8 格式編碼的逗號分隔值 (CSV) 檔案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。檔案標頭包含事件中繼資料和描述每個資料元素的事件變數。事件資料遵循 標頭。事件資料中的每行都包含來自單一登入事件的資料。

對於帳戶接管洞見模型，您必須在 CSV 檔案的標頭列中提供下列事件中繼資料和事件變數。

事件中繼資料

建議您在 CSV 檔案標頭中提供下列中繼資料。事件中繼資料必須為大寫字母。

- EVENT_ID - 登入事件的唯一識別符。
- 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符。
- EVENT_TIMESTAMP - 發生登入事件時的時間戳記。時間戳記必須在 UTC 中為 ISO 8601 標準。
- EVENT_LABEL （建議） - 將事件分類為詐騙或合法的標籤。您可以使用任何標籤，例如「詐騙」、「合法」、「1」或「0」。

> **Note**
>
> - 事件中繼資料必須為大寫字母。區分大小寫。
> - 登入事件不需要標籤。不過，我們建議您包含 EVENT_LABEL 中繼資料，並提供登入事件的標籤。如果標籤不完整或偶發，沒問題。如果您提供標籤，Amazon Fraud Detector 將使用它們自動計算帳戶接管探索率，並將其顯示在模型效能圖表和資料表中。

事件變數

對於帳戶接管洞見模型，您必須提供必要 （強制性） 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。作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特徵工程。

> **Note**
>
> 事件變數名稱必須以小寫字母表示。它們區分大小寫。

強制性變數

訓練 Accounts Takeover Insights 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 地址
瀏覽器和裝置	USERAGENT	登入事件中使用的瀏覽器、裝置和作業系統
有效的登入資料	VALIDCRED	指示用於登入的登入資料是否有效

選用變數

下列變數是訓練 Accounts Takeover Insights 模型的選用變數。

類別	Type	描述
瀏覽器和裝置	FINGERPRINT	瀏覽器或裝置指紋的唯一識別符
工作階段 ID	SESSION_ID	驗證工作階段的識別符
標籤	EVENT_LABEL	將事件分類為詐騙或合法的標籤。您可以使用任何標籤，例如「詐騙」、「合法」、「1」或「0」。
時間戳記	LABEL_TIMESTAMP	上次更新標籤時的時間戳記。如果提供 EVENT_LABEL，則此為必要項目。

> **Note**
>
> - 您可以為兩個強制性變數選用變數提供任何變數名稱。請務必將每個強制和選用變數指派給正確的變數類型。
> - 您可以提供額外的變數。不過，Amazon Fraud Detector 不會包含這些變數來訓練 Account Takeover Insights 模型。

選取資料

收集資料是建立帳戶接管洞見模型的重要步驟。當您開始收集登入資料時，請考慮下列要求和建議：

必要

- 提供至少 1，500 個使用者帳戶範例，每個帳戶至少有兩個相關聯的登入事件。
- 您的資料集必須至少涵蓋 30 天的登入事件。您可以稍後指定要用來訓練模型的事件特定時間範圍。

建議

- 您的資料集包含失敗登入事件的範例。您可以選擇將這些失敗的登入標記為「詐騙」或「合法」。
- 使用跨超過六個月的登入事件準備歷史資料，並包含 100K個實體。

如果您沒有已符合最低需求的資料集，請考慮呼叫 SendEvent API 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 會檢查您資料集中包含的中繼資料和變數，以訓練模型是否符合大小和格式需求。如需詳細資訊，請參閱資料集驗證。它也會檢查其他要求。如果資料集未通過驗證，則不會建立模型。若要成功建立模型，請務必在再次訓練之前修正未通過驗證的資料。

常見的資料集錯誤

驗證資料集以訓練 Account Takeover Insights 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 UTF-8 格式。

- CSV 檔案標頭至少不包含下列其中一個中繼資料：EVENT_ID、 ENTITY_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_ADDRESS、 USERAGENT或 VALIDCRED。
- 有一個以上的變數與相同的變數類型相關聯。
- 中超過 0.1% 的值EVENT_TIMESTAMP包含 null 或值，而非支援的日期和時間戳記格式。
- 第一個事件和最後一個事件之間的天數少於 30 天。
- 超過 10% 的變數IP_ADDRESS類型是無效或 null。
- 超過 50% 的變數USERAGENT類型包含 null。
- VALIDCRED 變數類型的所有變數都會設定為 false。

建立模型

Amazon Fraud Detector 模型會學習偵測特定事件類型的詐騙。在 Amazon Fraud Detector 中，您會先建立模型，做為模型版本的容器。每次訓練模型時，都會建立新的版本。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。當您建立模型時，Amazon Fraud Detector 會代表您建立此變數。您可以在規則表達式中使用此變數，以在詐騙評估期間解譯模型分數。

使用 訓練和部署模型 適用於 Python (Boto3) 的 AWS SDK

模型版本是透過呼叫 CreateModel和 CreateModelVersion操作來建立。 會CreateModel啟動模型，做為模型版本的容器。 會CreateModelVersion啟動訓練程序，進而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 的範例請求。此範例會建立 Online Fraud Insights 模型類型，並假設您已建立事件類型 sample_registration。如需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 CreateModelVersion API 訓練您的第一個版本。針對 TrainingDataSource和 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，以及如何分類事件標籤。根據預設，Amazon Fraud Detector 會忽略未標記的事件。此範例程式碼使用 AUTO unlabeledEventsTreatment來指定 Amazon Fraud Detector 決定如何使用未標記的事件。

```
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'
}
)
```

成功的請求將產生狀態為 的新模型版本TRAINING_IN_PROGRESS。在訓練期間，您可以隨時呼叫 UpdateModelVersionStatus 並將狀態更新為 來取消訓練TRAINING_CANCELLED。訓練完成後，模型版本狀態會更新為 TRAINING_COMPLETE。您可以使用 Amazon Fraud Detector 主控台或呼叫 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，請啟用模型，讓偵測器可在即時詐騙預測中使用模型。Amazon Fraud Detector 會在開啟自動擴展的多個可用區域中部署模型，以確保模型隨著您正在進行的詐騙預測數量而擴展。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 會以不同的方式產生不同模型類型的模型分數。

對於 Account Takeover Insights (ATI) 模型，Amazon Fraud Detector 只會使用彙總值 （透過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，指出未知風險。這是因為對於新的實體，用於計算彙總的值將為零或 null。Account Takeeover Insights (ATI) 模型會針對相同實體和現有實體的所有後續事件產生介於 0 到 1000 之間的模型分數，其中 0 表示低詐騙風險，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 對應於預估的 5% 挑戰率，而分數 900 對應於預估的 0.1% 挑戰率。

對於線上詐騙詳情 (OFI) 和交易詐騙詳情 (TFI) 模型，Amazon Fraud Detector 會使用彙總值 （結合一組原始變數計算的值） 和原始值 （為變數提供的值） 來產生模型分數。模型分數可以介於 0 到 1000 之間，0 表示低詐騙風險，1000 表示高詐騙風險。對於 OFI 和 TFI 模型，模型分數與偽陽性率 (FPR) 直接相關。例如，分數 600 對應於估計的 10% 偽陽性率，而分數 900 對應於估計的 2% 偽陽性率。下表提供特定模型分數如何與預估誤報率關聯的詳細資訊。

模型分數	預估 FPR
975	0.50%
950	1%
900	2%
860	3%
775	5%
700	7%

模型分數	預估 FPR
600	10%

模型效能指標

模型訓練完成後，Amazon Fraud Detector 會使用 15% 的資料來驗證模型效能，而這些資料並非用來訓練模型。您可以預期已訓練的 Amazon Fraud Detector 模型具有與驗證效能指標類似的實際詐騙偵測效能。

身為企業，您必須在偵測更多詐騙，以及為合法客戶增加更多摩擦之間取得平衡。為了協助選擇正確的平衡，Amazon Fraud Detector 提供下列工具來評估模型效能：

- 分數分佈圖 – 模型分數分佈的長條圖假設 100，000 個事件的範例群體。左側 Y 軸代表合法事件，右側 Y 軸代表詐騙事件。您可以按一下圖表區域來選取特定的模型閾值。這將更新混淆矩陣和 ROC 圖表中的對應檢視。
- 混淆矩陣 – 透過比較模型預測與實際結果，摘要指定分數閾值的模型準確性。Amazon Fraud Detector 會假設 100，000 個事件的範例人口。詐騙和合法事件的分佈會模擬您企業中的詐騙率。
  - 真陽性 – 此模型可預測詐騙，而事件實際上是詐騙。
  - 誤報 – 此模型預測詐騙，但事件實際上是合法的。
  - 真正的負面：模型預測合法，而事件實際上是合法的。
  - 錯誤負面：模型預測合法，但事件實際上是詐騙。
  - 真陽性率 (TPR) – 模型偵測到的總詐騙百分比。也稱為擷取速率。
  - 偽陽性率 (FPR) – 錯誤預測為詐騙的總合法事件百分比。
- 接收者運算子曲線 (ROC) – 在所有可能的模型分數閾值中，以偽陽性率函數繪製真正的陽性率。選擇進階指標來檢視此圖表。
- 曲線下面積 (AUC) – 總結所有可能模型分數閾值的 TPR 和 FPR。沒有預測能力的模型 AUC 為 0.5，而完美模型的分數為 1.0。
- 不確定範圍 – 它會顯示模型預期 AUC 的範圍。範圍較大 (AUC 上限和下限的差異 > 0.1) 表示模型不確定性較高。如果不確定性範圍很大 (>0.1)，請考慮提供更多已標記的事件並重新訓練模型。

使用模型效能指標

1. 從分數分佈圖表開始，檢閱詐騙和合法事件模型分數的分佈。理想情況下，您會在詐騙和合法事件之間有明確的區隔。這表示模型可以準確識別哪些事件是詐騙事件，哪些是合法的事件。按一下圖表區域以選取模型閾值。您可以看到調整模型分數閾值如何影響您的真陽性和偽陽性率。

   > **Note**
   >
   > 分數分佈圖表會在兩個不同的 Y 軸上繪製詐騙和合法事件。左側 Y 軸代表合法事件，右側 Y 軸代表詐騙事件。

2. 檢閱混淆矩陣。根據您選取的模型分數閾值，您可以根據 100，000 個事件的範例看到模擬的影響。詐騙和合法事件的分佈會模擬您企業中的詐騙率。使用此資訊尋找真陽性率和偽陽性率之間的正確平衡。
3. 如需其他詳細資訊，請選擇進階指標。使用 ROC 圖表來了解任何模型分數閾值的真陽性率和偽陽性率之間的關係。ROC 曲線可協助您微調真陽性率和偽陽性率之間的權衡。

   > **Note**
   >
   > 您也可以選擇資料表，以資料表形式檢閱指標。
   > 資料表檢視也會顯示指標精確度。精確度是與預測為詐騙的所有事件相比，正確預測為詐騙事件的百分比。

4. 使用效能指標，根據您的目標和詐騙偵測使用案例，判斷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風險、中等風險或低風險，則需要識別兩個閾值分數，以便您可以草擬三個規則條件，如下所示：

   - 分數 > X 是高風險
   - 分數 < X 但 > Y 為中等風險
   - 分數 < Y 為低風險

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您模型整體效能的相對重要性提供值。具有最高值的模型變數對於模型而言比該模型版本資料集中的其他模型變數更重要，預設會列在頂端。同樣地，具有最低值的模型變數預設會列

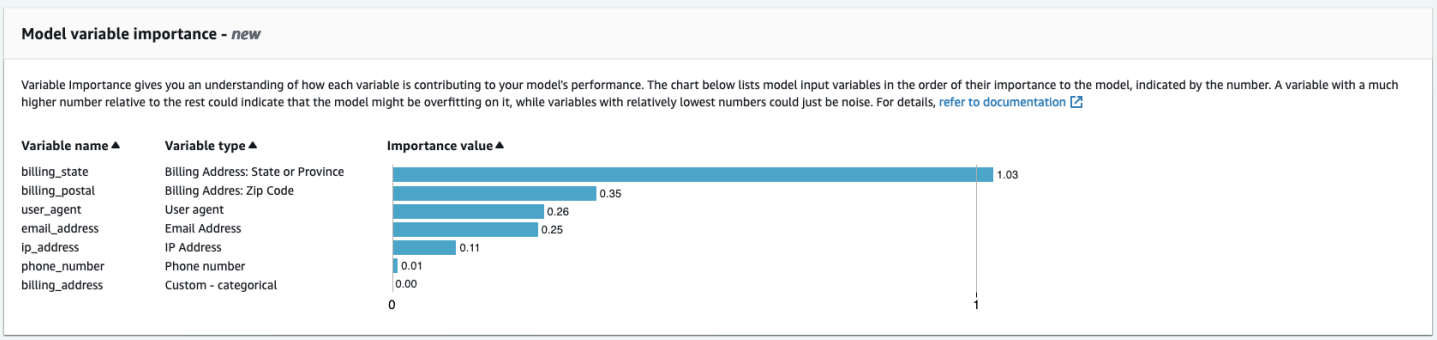
在底部，與其他模型變數相較之下，其重要性最低。使用模型變數重要性值，您可以深入了解哪些輸入驅動了模型的效能。

您可以在 Amazon Fraud Detector 主控台或使用 DescribeModelVersion API 來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 地址或電子郵件）。如需詳細資訊，請參閱變數類型。對於 Account Takeover Insights (ATI) 模型，Amazon Fraud Detector 為原始和彙總變數類型提供變數重要性值。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一組 Amazon Fraud Detector 合併的原始變數，以計算彙總重要性值。
- 變數名稱：用於訓練模型版本的事件變數名稱（例如 `ip_address`、`email_address`、)`are_creadentials_valid`。對於彙總變數類型，會列出用於計算彙總變數重要性值的所有變數名稱。
- 變數重要性值：代表原始變數或彙總變數對模型效能相對重要性的數字。典型範圍：0–10

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。帳戶接管洞見 (ATI) 模型除了原始變數的重要性值之外，還會提供彙總的變數重要性值。視覺化圖表可讓您輕鬆地查看具有垂直虛線的變數之間的相對重要性，並提供最高排名變數重要性值的參考。



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**
>
> 2021 年 7 月 9 日之前建立的模型版本沒有可變重要性值。您必須訓練新版本的模型，才能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來深入了解哪些因素推動模型的效能提升或降低，以及哪些變數貢獻最大。然後調整您的模型以改善整體效能。

更具體地說，為了改善模型效能，請針對訓練資料中的網域知識和偵錯問題檢查可變重要性值。例如，如果使用帳戶 ID 做為模型的輸入，且其列在頂端，請查看其可變重要性值。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適應特定的詐騙模式（例如，所有詐騙事件都來自相同的帳戶 ID)。不過，如果變數取決於詐騙標籤，也可能發生標籤洩漏的情況。根據您的網域知識分析結果，您可能想要移除變數並使用更多樣化的資料集進行訓練，或保持模型不變。

同樣地，請查看上次排名的變數。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。您可以考慮移除變數來訓練更簡單的模型版本。如果您的模型只有幾個變數，例如只有兩個變數，Amazon Fraud Detector 仍會提供變數重要性值，並對變數進行排名。不過，在此情況下，洞察會受到限制。

Important

1. 如果您注意到模型變數重要性圖表中缺少變數，可能是下列其中一個原因所造成。請考慮修改資料集中的變數，並重新訓練模型。
   - 訓練資料集中變數的唯一值計數低於 100。
   - 訓練資料集缺少大於 0.9 的變數值。
2. 每次您想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：

- 可變重要性值必須一律與網域知識結合評估。
- 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。請勿單獨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。請勿比較不同模型版本中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排名

模型訓練完成後，您可以在 Amazon Fraud Detector 主控台或使用 DescribeModelVersion API 來檢視已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 AWS 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 Models (模型)。
3. 選擇您的模型，然後選擇您的模型版本。
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。

了解模型變數重要性值的計算方式

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 SHapley Additive exPlanations (SHAP)。SHAP 基本上是在考慮所有模型變數的所有可能組合之後，模型變數的平均預期貢獻。

SHAP 會先指派每個模型變數的貢獻，以預測事件。然後，它會彙總這些預測，以在模型層級建立變數的排名。若要為預測指派每個模型變數的貢獻，SHAP 會考慮所有可能的變數組合之間模型輸出的差異。透過包含包含或移除特定變數集以產生模型輸出的所有可能性，SHAP 可以準確存取每個模型變數的重要性。當模型變數彼此高度相關時，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。您可以改為將模型中已移除或遺失的變數取代為一或多個基準的對應變數值（例如非詐騙事件）。選擇適當的基準執行個體可能很困難，但 Amazon Fraud Detector 將此基準設定為您的人口平均值，讓這項操作變得簡單。

匯入 SageMaker AI 模型

您可以選擇將 SageMaker AI 託管模型匯入至 Amazon Fraud Detector。與模型類似，SageMaker AI 模型可以新增至偵測器，並使用 `GetEventPrediction` API 產生詐騙預測。在`GetEventPrediction`請求中，Amazon Fraud Detector 將調用您的 SageMaker AI 端點，並將結果傳遞給您的規則。

您可以設定 Amazon Fraud Detector 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 將使用此範本將您的事件變數

轉換為必要的輸入承載，以叫用 SageMaker AI 端點。或者，您可以將 SageMaker AI 模型設定為使用作為`GetEventPrediction`請求一部分傳送的 byteBuffer。

Amazon Fraud Detector 支援匯入使用 JSON 或 CSV 輸入格式和 JSON 或 CSV 輸出格式的 SageMaker AI 演算法。支援的 SageMaker AI 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 AI 模型 適用於 Python (Boto3) 的 AWS SDK

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

輸入組態指定 將使用事件變數來建構模型輸入 (`useEventVariables` 設定為 `TRUE`)。輸入格式為 TEXT_CSV，因為 XGBoost 需要 CSV 輸入。csvInputTemplate 指定如何從作為`GetEventPrediction`請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_amthist_amt`和 `payment_type`。

輸出組態會指定 SageMaker AI 模型的回應格式，並將適當的 CSV 索引映射至 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 AI 模型的輸出必須映射至具有來源 的變數`EXTERNAL_MODEL_SCORE`。您無法在主控台中使用變數建立這些變數。您必須在設定模型匯入時建立它們。

```
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。當您刪除模型時，Amazon Fraud Detector 會永久刪除該模型，且資料不會再存放在 Amazon Fraud Detector 中。

如果 Amazon SageMaker AI 模型未與偵測器版本相關聯，您也可以將其移除。移除 SageMaker AI 模型會中斷與 Amazon Fraud Detector 的連線，但 SageMaker AI 中仍提供該模型。

刪除模型版本

您只能刪除`Ready to deploy`處於 狀態的模型版本。若要將模型版本從 `ACTIVE` 變更為 `Ready to deploy` 狀態，請取消部署模型版本。

1. 登入 AWS Management Console 並開啟 Amazon Fraud Detector 主控台，網址為 https：//https://console.aws.amazon.com/frauddetector。
2. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇模型。
3. 選擇包含您要刪除之模型版本的模型。
4. 選擇您要刪除的模型版本。
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。

取消部署模型版本

您無法取消部署任何偵測器版本 (`ACTIVE`、`INACTIVE`、) 正在使用的模型版本`DRAFT`。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 主控台的左側導覽窗格中，選擇模型。
2. 選擇包含您要取消部署之模型版本的模型。

3. 選擇您要刪除的模型版本。
4. 選擇動作，然後選擇取消部署模型版本。

刪除模型

刪除模型之前，您必須先刪除所有模型版本，並與模型相關聯。

1. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇模型。
2. 選擇您要刪除的模型。
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。

移除 Amazon SageMaker AI 模型

1. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇模型。
2. 選擇您要移除的 SageMaker AI 模型。
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 AI 模型。

偵測器

偵測器是包含詐騙偵測邏輯的容器，例如模型和規則，適用於您想要評估詐騙的特定商業事件。您首先要透過指定您已定義的事件來建立偵測器，並選擇性地新增 Amazon Fraud Detector 為事件建立和訓練的模型版本。

然後，您將規則和規則執行順序新增至偵測器，以建立偵測器版本。偵測器版本會定義規則，並選擇性地定義模型，該模型將在產生詐騙預測的請求中執行。您可以將偵測器中定義的任何規則新增至偵測器版本。您也可以將針對評估事件類型訓練的任何模型新增至偵測器版本。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，以滿足多個使用案例。

每個偵測器版本的狀態必須為 `DRAFT`、 `ACTIVE`或 `INACTIVE`。一次只能有一個偵測器版本處於 `ACTIVE` 狀態。Amazon Fraud Detector 使用具有 `ACTIVE` 狀態的偵測器版本來產生詐騙預測。

建立偵測器

您可以透過指定您已定義的事件類型來建立偵測器。您可以選擇新增已由 Amazon Fraud Detector 訓練和部署的模型。如果您新增模型，您可以在建立規則時，在規則表達式中使用 Amazon Fraud Detector 產生的模型分數 (例如 `$model score < 90`)。

您可以在 Amazon Fraud Detector 主控台、使用 PutDetector API、使用 put-detector 命令或使用 AWS SDK 建立偵測器。如果您使用 API、命令或 SDK 來建立偵測器，則在建立偵測器之後，請遵循的指示建立偵測器版本。

在 Amazon Fraud Detector 主控台中建立偵測器

此範例假設您已建立事件類型，也已建立並部署您想要用於詐騙預測的模型版本。

步驟 1：建置偵測器

1. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇 Detectors。
2. 選擇建立偵測器。
3. 在定義偵測器詳細資訊頁面中，輸入`sample_detector`偵測器名稱。或者，輸入偵測器的描述，例如 `my sample fraud detector`。
4. 針對事件類型，選取您為詐騙預測建立的事件類型。
5. 選擇 Next (下一步)。

步驟 2：新增部署的模型版本

1. 請注意，這是選用步驟。您不需要將模型新增至偵測器。若要略過此步驟，選擇下一步。
2. 在新增模型 - 選用中，選擇新增模型。
3. 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 模型名稱。針對選取版本，選擇已部署模型的模型版本。
4. 選擇 Add model (新增模型)。
5. 選擇 Next (下一步)。

步驟 3：新增規則

規則是告訴 Amazon Fraud Detector 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`和 `low_fraud_risk`。若要建立您自己的規則、規則表達式、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. 在新增規則頁面中，定義規則下，輸入 `high_fraud_risk` 表示規則名稱，在描述 - 選擇性下，輸入 **`This rule captures events with a high ML model score`**表示規則的描述。
2. 在表達式中，使用 Amazon Fraud Detector 簡化規則表達式語言輸入下列規則表達式：

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```

3. 在結果中，選擇建立新結果。結果是詐騙預測的結果，如果規則在評估期間相符，則會傳回結果。
4. 在建立新的結果中，輸入 `verify_customer`做為結果名稱。或者，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。建立之後，Amazon Fraud Detector 會讓規則可用於偵測器。
7. 選擇新增另一個規則，然後選擇建立規則索引標籤。
8. 再重複此程序兩次，使用下列`low_fraud_risk`規則詳細資訊建立您的 `medium_fraud_risk`和規則：

   - medium_fraud_risk

     規則名稱： `medium_fraud_risk`

     結果： `review`

表達式：

```
$sample_fraud_detection_model_insightscore <= 900 and

$sample_fraud_detection_model_insightscore > 700
```

- low_fraud_risk

  規則名稱： `low_fraud_risk`

  結果： `approve`

  表達式：

  ```
  $sample_fraud_detection_model_insightscore <= 700
  ```

9. 建立使用案例的所有規則後，請選擇下一步。

   如需建立和撰寫規則的詳細資訊，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判斷是否評估您定義的所有規則，或規則評估是否停止在第一個相符規則。而規則順序會決定您希望規則在其中執行的順序。

預設規則執行模式為 `FIRST_MATCHED`。

第一個相符項目

第一個相符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。

您在 中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。這會`high_fraud_risk`移至第一個位置。

重複此程序，讓您的`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。

所有相符項目

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

針對此教學課程選取 FIRST_MATCHED ，然後選擇下一步。

步驟 5：檢閱並建立偵測器版本

偵測器版本定義用於產生詐騙預測的特定模型和規則。

1. 在檢閱和建立頁面中，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，請選擇對應區段旁的編輯。
2. 選擇建立偵測器。建立後，偵測器的第一個版本會出現在偵測器版本資料表中，其中包含Draft狀態。

   您可以使用草稿版本來測試您的偵測器。

使用 建立偵測器 適用於 Python (Boto3) 的 AWS SDK

下列範例顯示 PutDetector API 的範例請求。偵測器可做為偵測器版本的容器。PutDetector API 會指定偵測器將評估的事件類型。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，以及可選的模型版本，這些版本將做為產生詐騙預測請求的一部分。您可以將偵測器中定義的任何規則新增至偵測器版本。您也可以新增任何已針對評估事件類型訓練的模型。

每個偵測器版本的狀態為 DRAFT、 ACTIVE或 INACTIVE。一次只能有一個偵測器版本處於 ACTIVE 狀態。在GetEventPrediction請求期間，如果DetectorVersion未指定偵測器，Amazon Fraud Detector 將使用ACTIVE偵測器。

規則執行模式

Amazon Fraud Detector 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 Fraud Detector 會依序評估規則，從第一個相符的規則停止，直到持續為止。然後，Amazon Fraud Detector 會提供該單一規則的結果。如果規則評估為 false （不相符），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 Fraud Detector 會執行所有規則，並傳回每個相符規則的定義結果。

使用 建立偵測器版本 適用於 Python (Boto3) 的 AWS SDK

下列範例顯示 CreateDetectorVersion API 的範例請求。規則執行模式設定為 FIRST_MATCHED，因此 Amazon Fraud Detector 會依序評估規則，從第一個相符規則停止，以先到持續。然後，Amazon Fraud Detector 會在 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 UpdateDetectorVersionStatus API。下列範例會將偵測器版本狀態從 更新DRAFT為 ACTIVE。在GetEventPrediction請求期間，如果未指定偵測器 ID，Amazon Fraud Detector 將使用偵測器的 ACTIVE 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

在 Amazon Fraud Detector 中刪除偵測器之前，您必須先刪除與偵測器相關聯的所有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，且資料不會再存放在 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 AWS Management Console 並開啟 Amazon Fraud Detector 主控台，網址為 https：//https://console.aws.amazon.com/frauddetector。
2. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇 Detectors。
3. 選擇包含您要刪除之偵測器版本的偵測器。
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 ACTIVE或INACTIVE偵測器版本未使用規則版本時，您才能將其刪除。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 Detectors。
2. 選擇包含您要刪除之規則版本的偵測器。
3. 選擇關聯的規則索引標籤，然後選擇要刪除的規則。
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，您必須先刪除與偵測器相關聯的所有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 Detectors。
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的詐騙風險。本節提供有關建立和管理 資源的資訊。

主題

Variables

變數代表您想要在詐騙預測中使用的資料元素。這些變數可以從您準備訓練模型的事件資料集、Amazon Fraud Detector 模型的風險分數輸出，或從 Amazon SageMaker AI 模型取得。如需從事件資料集取得變數的詳細資訊，請參閱使用 Data Model Explorer 取得事件資料集需求。

建立事件類型時，必須先建立您要用於詐騙預測的變數，然後新增至事件。您建立的每個變數都必須指派資料類型、預設值，以及選用的變數類型。Amazon Fraud Detector 會充實您提供的部分變數，例如 IP 地址、銀行識別號碼 (BINs) 和電話號碼，為使用這些變數的模型建立額外的輸入和提升效能。

資料類型

變數必須具有變數代表的資料元素資料類型，並且可以選擇指派其中一個預先定義的 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	< 空 >	abc、123、1D3B
Integer	正整數或負整數	0	1、-1

資料類型	描述	預設值	範例值
Boolean	是非題	False	對、錯
DateTime	僅限以 ISO 8601 標準 UTC 格式指定的日期和時間	< 空 >	2019-11-30T13：01：01Z
Float	含小數點的數字	0.0	4.01、0.10

預設值

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

變數類型

建立變數時，您可以選擇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用資料元素。只有具有相關聯變數類型的變數才能用於模型訓練。作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、特徵工程和風險評分。

Amazon Fraud Detector 已預先定義下列變數類型，可用來指派給變數。

類別	變數類型	描述	資料類型	範例
Se (工作階段	IP_ADDRES S	在事件期間收集的 IP 地址	字串	192.0.2.0 注意：Amazon Fraud Detector 會充實

類別	變數類型	描述	資料類型	範例
				此資料。如需詳細資訊，請參閱地理位置擴充功能
	USERAGEN	在事件期間收集的使用者代理程式	字串	Mozilla 5.0 (Windows NT 10.0、Win64、x64、rv：68.0) Gecko 20100101

類別	變數類型	描述	資料類型	範例
	FINGERPRINT	用於事件之裝置的唯一識別符	字串	sadfow987u234
	SESSION_ID	事件作用中工作階段的工作階段 ID	字串	sid123456789
	ARE_CREDENTIALS_VALID	指出用於事件登入的登入資料是否有效	Bool	True
使用者	EMAIL_ADDRESS	在事件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	在事件期間收集的電話號碼	字串	+1 555-0100 注意：Amazon Fraud Detector 會充實此資料。如需詳細資訊，請參閱電話號碼擴充功能

類別	變數類型	描述	資料類型	範例
帳單	BILLING_NAME	與帳單地址相關聯的名稱	字串	John Doe

類別	變數類型	描述	資料類型	範例
	BILLING_PHONE	與帳單地址相關聯的電話號碼	字串	+1 555-0100 注意：Amazon Fraud Detector 會充實此資料。如需詳細資訊，請參閱電話號碼擴充功能

類別	變數類型	描述	資料類型	範例
	BILLING_ADDRESS_L	帳單地址的第一行	字串	任何街道
	BILLING_ADDRESS_L	帳單地址的第二行	字串	任何單位 123
	BILLING_CITY	帳單地址中的城市	字串	任何城市
	BILLING_STATE	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
	BILLING_COUNTRY	帳單地址中的國家/地區	字串	任何國家 注意：Amazon Fraud Detector 會充實此資料。如需詳細資訊，請參閱地理位置擴充

類別	變數類型	描述	資料類型	範例
				功能
	BILLING_ZIP	帳單地址中的郵遞區號	字串	01234 注意：Amazon Fraud Detector 會充實此資料。如需詳細資訊，請參閱地理位置擴充功能

類別	變數類型	描述	資料類型	範例
運送	SHIPPING_NAME	與運送地址相關聯的名稱	字串	John Doe

類別	變數類型	描述	資料類型	範例
	SHIPPING_PHONE	與運送地址相關聯的電話號碼	字串	+1 555-0100 注意：Amazon Fraud Detector 會充實此資料。如需詳細資訊，請參閱電話號碼擴充功能

類別	變數類型	描述	資料類型	範例
	SHIPPING_ADDRESS_1	運送地址的第一行	字串	123 任何街道
	SHIPPING_ADDRESS_2	運送地址的第二行	字串	單元 123
	SHIPPING_CITY	運送地址中的城市	字串	任何城市
	SHIPPING_STATE	運送地址中的州或省	字串	任何狀態

類別	變數類型	描述	資料類型	範例
	SHIPPING_COUNTRY	位於運送地址中的國家/地區	字串	任何國家 注意：Amazon Fraud Detector 會充實此資料。如需詳細資訊，請參閱地理位置擴充

類別	變數類型	描述	資料類型	範例
				功能
	SHIPPING_ZIP	運送地址中的郵遞區號	字串	01234 注意：Amazon Fraud Detector 會充實此資料。如需詳細資訊，請參閱地理位置擴充功能

類別	變數類型	描述	資料類型	範例
付款	ORDER_ID	交易的唯一識別符	字串	LUX60
	價格	總訂單價格	字串	560.00
	CURRENCY_CODE	ISO 4217 貨幣代碼	字串	美元
	PAYMENT_TYPE	在事件期間用於付款的付款方式	字串	信用卡
	AUTH_COD	信用卡發行者或發行銀行傳送的英數代碼	字串	0000
	AVS	來自卡片處理器的地址驗證系統 (AVS) 回應碼	字串	Y
產品	PRODUCT_ATEGORY	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
	CATEGORIAL	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
	FREE_FORM_TEXT	擷取為事件一部分的任何任意格式文字（例如，客戶評論或評論）	字串	任意格式文字輸入的範例

將變數指派給變數類型

如果您打算使用變數來訓練模型，請務必選擇要指派給變數的正確變數類型。不正確的變數類型指派可能會對模型效能造成負面影響。您稍後變更指派也會變得非常困難，特別是在多個模型和事件已使用變數時。

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

將變數指派給正確變數類型的重要備註

1. 如果變數符合其中一個預先定義的變數類型，請使用它。請確定變數類型對應至變數。例如，如果您將 ip_address 變數指派給EMAIL_ADDRESS變數類型，則 ip_address 變數不會充實 ASN、ISP、地理位置和風險分數等豐富功能。如需詳細資訊，請參閱變數擴充功能。
2. 如果變數不符合任何預先定義的變數類型，請依照下列建議來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排序的變數，並且可以放入類別、區段或群組。您用來訓練模型的資料集可能有 ID 變數，例如 merchant_id、acampaency_id 或 policy_id。這些變數代表群組（例如，具有相同 policy_id 的所有客戶代表群組）。必須指派具有下列資料的變數 CATEGORICAL 變數類型 -
   - 包含 customer_ID、Segment_ID、color_ID、compartment_code 或 product_ID 等資料的變數。

- 包含具有 true、false 或 null 值的布林值的變數。
- 可以放入群組或類別的變數，例如公司名稱、產品類別、卡片類型或推薦媒體。

> **Note**
>
> ENTITY_ID 是 Amazon Fraud Detector 用來指派給 ENTITY_ID 變數的預留變數類型。ENTITY_ID 變數是啟動您要評估之動作的實體 ID。如果您要建立交易詐騙洞見 (TFI) 模型類型，則需要提供 ENTITY_ID 變數。您需要決定資料中的哪個變數可唯一識別啟動動作的實體，並將其傳遞為 ENTITY_ID 變數。將 CATEGORICAL 變數類型指派給資料集中的所有其他 IDs，如果這些 ID 存在且您使用它們進行模型訓練。其他 IDs 範例不是您資料集中的實體，可以是 merchant_ID、 policy_ID 和 campaign_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 變數類型的範例為：使用者檢閱、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字符。分隔符號可以是英數字元和底線符號以外的任何字元。例如，使用者檢閱和註解可以用「空格」分隔符號分隔，日期和引號可以使用連字號做為分隔符號，以分隔字首、尾碼和中繼部分。Amazon Fraud Detector 使用分隔符號從 FREE_FORM_TEXT 變數擷取資料。
5. 將 NUMERIC 變數類型指派給真實數字且具有固有排序的變數。NUMERIC 變數的範例包括 day_of_the_week、invent_severity、Customer_rating。雖然您可以為這些變數指派 CATEGORICAL 變數類型，但我們強烈建議將具有固有順序的所有實數變數指派給 NUMERIC 變數類型。

變數擴充功能

Amazon Fraud Detector 會充實您提供的一些原始資料元素，例如 IP 地址、銀行識別號碼 (BINs) 和電話號碼，為使用這些資料元素的模型建立額外的輸入並提升效能。擴充功能有助於識別潛在的可疑情況，並協助模型擷取更多詐騙。

電話號碼擴充功能

Amazon Fraud Detector 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額外資訊來充實電話號碼資料。2021 年 12 月 13 日或之後訓練的所有模型，其電話號碼都會自動啟用電話號碼擴充功能，並包含國家/地區碼 (+xxx)。如果您已在模型中包含電話號碼變數，並在 2021 年 12 月 13 日之前進行訓練，請重新訓練您的模型，以便充分利用此擴充功能。

強烈建議您針對電話號碼變數使用下列格式，以確保您的資料能夠成功擴充。

變數	格式	描述
PHONE_NUMBER	E.164 標準	請務必將國家/地區代碼 (+xxx) 與電話號碼一起包含。
BILLING_PHONE 和 SHIPPING_PHONE	E.164 標準	請務必將國家/地區代碼 (+xxx) 與電話號碼一起包含。

地理位置擴充功能

從 2022 年 2 月 8 日開始，Amazon Fraud Detector 會計算您為事件提供的 IP_ADDRESS、BILLING_ZIP 和 SHIPPING_ZIP 值之間的實體距離。計算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三個變數中的兩個：IP_ADDRESS、BILLING_ZIP 或 SHIPPING_ZIP。此外，每個 BILLING_ZIP 和 SHIPPING_ZIP 值必須分別有有效的 BILLING_COUNTRY 代碼和 SHIPPING_COUNTRY 代碼。如果您有在 2022 年 2 月 8 日之前訓練的模型，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功能。

如果由於資料無效，Amazon Fraud Detector 無法判斷事件與 IP_ADDRESS、BILLING_ZIP 或 SHIPPING_ZIP 值相關聯的位置，則會改用特殊預留位置值。例如，假設事件具有有效的 IP_ADDRESS 和 BILLING_ZIP 值，但 SHIPPING_ZIP 值無效。在這種情況下，僅針對 IP_ADDRESS–> BILLING_ZIP 完成擴充。IP_ADDRESS–>SHIPPING_ZIP 和 BILLING_ZIP–>SHIPPING_ZIP 不會完成擴充。相反地，預留位置值會用於其位置。無論您的模型是否啟用地理位置擴充，模型的效能都不會變更。

您可以將 BILLING_ZIP 和 SHIPPING_ZIP 變數映射至 CUSTOM_CATEGORICAL 變數類型，以選擇不增加地理位置。變更變數類型不會影響您模型的效能。

地理位置變數格式

強烈建議您針對地理位置變數使用下列格式，以確保您的位置資料已成功擴充。

變數	格式	描述
IP_ADDRESS	IPv4 地址	例如 - 1.1.1.1
BILLING_ZIP 和 SHIPPING_ZIP	指定國家/地區的 ISO 3166-1 alpha-2 郵遞區號	如需詳細資訊，請參閱本主題中的國家和區域代碼一節。
BILLING_COUNTRY 和 SHIPPING_COUNTRY	ISO 3166-1 alpha-2 雙字母標準國家/地區碼	如需詳細資訊，請參閱本主題中的國家和區域代碼一節。Amazon Fraud Detector 會嘗試將國家/地區名稱的所有常見變化與其 ISO 3166-1 雙字母標準國家/地區碼進行比對。不過，我們無法保證它們會正確配對。

國家和區域代碼

下表提供 Amazon Fraud Detector 支援用於地理位置擴充的國家和地區的完整清單。每個國家和區域都有一個指派的國家/地區代碼（特別是 ISO 3166-1 alpha-2 雙字母國家/地區代碼）和郵遞區號。

郵遞區號格式

- 9 - 數字
- a - 字母
- 【X】 - X 是選用項目。例如，Guersney "GY9【9】 9aa" 表示 "GY9 9aa" 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，「aa【aa/99】」表示「aaa」和「aa 99」都是有效的。使用其中一種格式，但請勿使用這兩種格式。
- 有些國家具有固定字首。例如，Andorra 的郵遞區號為 AD999。這表示國家/地區代碼必須以字母 AD 開頭，後面接著三個數字。

Code	名稱	郵遞區號
.ade	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 9999
BD	孟加拉	9999
BE	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 9a9
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
CZ	捷克	999 99
DE	德國	99999
DK	丹麥	9999
DO	多明尼加共和國	99999

Code	名稱	郵遞區號
DZ	阿爾及利亞	99999
EE	愛沙尼亞	99999
ES	西班牙	99999
FI	芬蘭	99999
FM	密克羅尼西亞聯合狀態	99999
FO	法羅群島	999
法國	法國	99999
GB	英國	a【a】9【a/9】 9aa
GG	根西島	GY9【9】 9aa
GL	格陵蘭	9999
GP	瓜地洛普	99999
GT	瓜地馬拉	99999
GU	關島	99999
HR	克羅埃西亞	99999
HU	匈牙利	9999
IE	愛爾蘭	a99【a/9】【a/9】【a/9】【a/9】【a/9】
IM	曼島	IM9【9】9aa
IN	印度	999999
IS	冰島	999
IT	義大利	99999

Code	名稱	郵遞區號
JE	澤西島	JE9【9】9aa
JP	日本	999-9999
KR	韓國	99999
LI	列支敦斯登	9999
LK	斯里蘭卡	99999
LT	立陶宛	99999
LU	盧森堡	L-9999
LV	拉脫維亞	LV-9999
MC	摩納哥	99999
MD	摩爾多瓦共和國	9999
MH	馬紹爾群島	99999
MK	北馬其頓	9999
MP	北馬里亞納群島	99999
MQ	Matinique	99999
MT	馬爾他	aaa 9999
MX	墨西哥	99999
MY	馬來西亞	99999
NL	荷蘭	9999 aa
NO	挪威	9999
NZ	紐西蘭	9999

Code	名稱	郵遞區號
PH	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
RE	團圓	99999
RO	羅馬尼亞	999999
RU	俄羅斯聯邦	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
TH	泰國	99999
TR	土耳其	99999
UA	烏克蘭	99999
美國	美國	99999
UY	烏拉圭	99999
VI	美屬維京群島	99999

Code	名稱	郵遞區號
WF	瓦利斯和富圖那	99999
YT	馬約特島	99999
ZA	南非	9999

使用者代理程式擴充功能

如果您建立 Account Takeover Insights (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 Fraud Detector 會使用其他資訊來充實使用者代理程式資料，例如 user_agent_family OS_family、 和 device_family。

建立變數

您可以在 Amazon Fraud Detector 主控台中使用 create-variable 命令、使用 CreateVariable 或使用 適用於 Python (Boto3) 的 AWS SDK

使用 Amazon Fraud Detector 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)。這些變數會用作範例。如果您要建立變數以用於模型訓練，請使用您資料集中適合您使用案例的變數。建立變數變數擴充功能之前，請務必閱讀 變數類型和 。

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 Fraud Detector，在左側導覽中選擇變數，然後選擇建立。
3. 在新增變數頁面中，輸入 email_address做為變數名稱。或者，輸入變數的描述。
4. 在變數類型中，選擇電子郵件地址。
5. Amazon Fraud Detector 會自動選取此變數類型的資料類型，因為已預先定義此變數類型。如果您的變數未自動指派變數類型，請從清單中選擇變數類型。如需詳細資訊，請參閱變數類型。
6. 如果您想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。如果您遵循此範例，請略過此步驟。
7. 選擇 Create (建立)。
8. 在 email_address 概觀頁面中，確認您剛建立之變數的詳細資訊。

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. 重複此程序來建立另一個變數ip_address，並選擇變數類型的 IP 地址。
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。您可以在建立事件類型時，稍後決定要包含哪些變數來訓練模型以偵測詐騙並產生詐騙偵測。

使用 建立變數 適用於 Python (Boto3) 的 AWS SDK

下列範例顯示 CreateVariable API 的請求。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)。

這些變數會用作範例。如果您要建立變數以用於模型訓練，請使用您資料集中適用於您的使用案例的變數。建立變數變數擴充功能之前，請務必閱讀 變數類型和 。

請務必指定變數來源。它有助於識別變數值衍生的位置。如果變數來源是 EVENT，則變數值會作為 GetEventPrediction 請求的一部分傳送。如果變數值為 MODEL_SCORE，則會由 Amazon Fraud Detector 填入。如果 EXTERNAL_MODEL_SCORE，變數值會由匯入的 SageMaker AI 模型填入。

```
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

當您刪除變數時，Amazon Fraud Detector 會永久刪除該變數，且資料不會再存放在 Amazon Fraud Detector 中。

您無法刪除包含在 Amazon Fraud Detector 中事件類型的變數。您必須先刪除變數相關聯的事件類型，然後刪除變數。

您無法手動刪除 Amazon Fraud Detector 模型輸出變數和 SageMaker AI 模型輸出變數。當您刪除模型時，Amazon Fraud Detector 會自動刪除模型輸出變數。

您可以在 Amazon Fraud Detector 主控台中使用 delete-variable CLI 命令、使用 DeleteVariable API，或使用 適用於 Python (Boto3) 的 AWS SDK

使用主控台刪除變數

若要刪除變數，

1. 登入 AWS Management Console 並開啟 Amazon Fraud Detector 主控台，網址為 https://console.aws.amazon.com/frauddetector：//。
2. 在 Amazon Fraud Detector 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 適用於 Python (Boto3) 的 AWS SDK

下列程式碼範例會使用 DeleteVariable API 刪除變數 customer_name。

```
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，並用於訓練 Amazon Fraud Detector 中的機器學習模型。如果您打算訓練線上詐騙洞見 (OFI) 或交易詐騙洞見 (TFI) 模型，則訓練資料集中至少 400 個事件必須分類為詐欺或合法。您可以使用任何標籤，例如詐騙、正當、1 或 0 來分類訓練資料集中的事件。訓練完成後，訓練模型會評估事件是否發生詐騙，並使用這些值將事件分類為詐騙或合法。

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置和訓練詐騙偵測模型的事件類型建立關聯。

建立標籤

您可以在 Amazon Fraud Detector 主控台中使用 put-label 命令、 PutLabel API 或使用 建立標籤 適用於 Python (Boto3) 的 AWS SDK。

使用 Amazon Fraud Detector 主控台建立標籤

若要建立標籤，

1. 開啟 AWS 管理主控台並登入您的帳戶。
2. 導覽至 Amazon Fraud Detector，選擇左側導覽中的標籤，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做為標籤名稱。標籤名稱必須與訓練資料集中代表詐騙活動的標籤相對應。或者，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至代表訓練資料集中合法活動的值。

使用 建立標籤 適用於 Python (Boto3) 的 AWS SDK

下列 適用於 Python (Boto3) 的 AWS SDK 範例程式碼會使用 PutLabel API 建立兩個標籤 （ 詐騙、合法 ）。建立標籤後，您可以將它們新增至事件類型，以分類特定事件。

```
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存放在 Amazon Fraud Detector 中，您可能需要新增或更新所儲存事件的標籤，例如當您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。

您可以使用 update-event-label 命令、UpdateEventLabel API 或使用 來新增或更新預存事件的標籤 適用於 Python (Boto3) 的 AWS SDK

下列 適用於 Python (Boto3) 的 AWS SDK 範例程式碼新增與使用 `UpdateEventLabel` API 註冊的事件類型相關聯的標籤詐騙。

```
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'
)
```

更新存放在 Amazon Fraud Detector 的事件資料中的事件標籤

您可能需要為已存放在 Amazon Fraud Detector 的事件新增或更新詐騙標籤，例如當您執行事件的離線詐騙調查，並想要關閉機器學習回饋迴圈時。若要更新已存放在 Amazon Fraud Detector 的事件標籤，請使用 `UpdateEventLabel` API 操作。以下顯示 UpdateEventLabel API 呼叫的範例。

```
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

當您刪除標籤時，Amazon Fraud Detector 會永久刪除該標籤，且資料不會再存放在 Amazon Fraud Detector 中。

您無法刪除包含在 Amazon Fraud Detector 中事件類型的標籤。您也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 主控台中使用 delete-label 命令、使用 DeleteLabel API，或使用 適用於 Python (Boto3) 的 AWS SDK

使用主控台刪除標籤

刪除標籤

1. 登入 AWS Management Console 並開啟 Amazon Fraud Detector 主控台，網址為 https://console.aws.amazon.com/frauddetector：//。
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. 選擇您要刪除的標籤。
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 適用於 Python (Boto3) 的 AWS SDK

下列 適用於 Python (Boto3) 的 AWS SDK 範例程式碼會使用 DeleteLabel API 刪除標籤正當性。

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

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

規則

規則是告訴 Amazon Fraud Detector 如何在詐騙預測期間解譯變數值的條件。規則是偵測器邏輯的一部分，由下列元素組成：

- 變數或清單 – 變數代表事件資料集中的資料元素，您想要在詐騙預測中使用。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 和 清單。
- 表達式 – 規則中的表達式會擷取您的商業邏輯。如果您在規則中使用變數，則會使用變數、比較運算子，例如 >、 < 、<=、>=. == 來建構簡單的規則表達式，以及 值。如果您使用的是清單，規則表達式會建構為清單項目in、 和清單名稱。如需詳細資訊，請參閱規則語言參考。您可以使用 and和將多個表達式結合在一起or。所有表達式都必須評估為布林值 (true 或 false)，且長度小於 4，000 個字元。不支援 If-else 類型條件。
- 結果 – 結果是 Amazon Fraud Detector 在規則相符時傳回的回應。結果指出詐騙預測的結果。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，請參閱結果。

偵測器必須至少有一個相關聯的規則。規則最多可以有 3 個清單，而偵測器最多可以有 30 個清單。您可以在偵測器建立程序中建立規則。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

下節概述 Amazon Fraud Detector 中的表達式 （ 即規則撰寫 ） 功能。

使用變數

您可以使用評估事件類型中定義的任何變數做為表達式的一部分。使用美元符號來表示變數：

```
$example_variable < 100
```

使用清單

您可以使用與變數類型相關聯的任何清單，並將項目填入規則表達式中。使用美元符號來表示清單項目值：

```
$example_list_variable in @list_name
```

比較、成員資格和身分運算子

Amazon Fraud Detector 包含下列比較運算子： **>** 、**>=**、 **<** 、**<=**、 **！=**、**==**、in、not in

範例如下：

範例： <

```
$variable < 100
```

範例： in， not in

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

範例： ！=

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

範例：==

```
$variable == 1000
```

運算子資料表

運算子	Amazon Fraud Detector Operator
等於	==
不等於	!=
大於	>
小於	<
大於或等於	>=
小於或等於	<=

運算子	Amazon Fraud Detector Operator
In (入)	in
及	以及
或	或
Not	!

基本數學

您可以在表達式中使用基本數學運算子（例如 +、-、* 、/)。典型的使用案例是在評估期間需要合併變數時。

在下面的規則中，我們將`$variable_1`使用 新增變數`$variable_2`，並檢查總數是否小於 10。

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

基本數學資料表資料

運算子	Amazon Fraud Detector Operator
Plus	+
最小值	-
乘	*
除	/
Modulo	%

規則運算式 (regex)

您可以使用 regex 來搜尋特定模式，做為表達式的一部分。如果您想要比對其中一個變數的特定字串或數值，這特別有用。Amazon Fraud Detector 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)。Amazon Fraud Detector 的規則表達式支援是以

Java 中的 .matches() 為基礎 （使用 RE2J 規則表達式程式庫）。網際網路上有數個實用的網站，可用於測試不同的規則表達式模式。

在下面的第一個範例中，我們首先將變數轉換為email小寫。然後，我們會檢查模式是否@gmail.com在 email變數中。請注意，第二個期間會逸出，以便我們可以明確檢查字串 .com。

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

在第二個範例中，我們會檢查變數是否phone_number包含國家/地區碼+1，以判斷電話號碼是否來自美國。加號會逸出，以便我們可以明確檢查字串 +1。

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

Regex 資料表

運算子	Amazon Fraud Detector 範例
比對開頭為 的任何字串	regex_match("^mystring"，$variable)
完全比對整個字串	regex_match("mystring"，$variable)
比對新行以外的任何字元	regex_match("."， $variable)
比對除「mystring」前的新行以外的任意數量字元	regex_match(".*mystring"，$variable)
逸出特殊字元	\

檢查是否有遺失值

有時檢查值是否遺失會有幫助。在 Amazon Fraud Detector 中，這會以 null 表示。您可以使用下列語法來執行此操作：

```
$variable != null
```

同樣地，如果您想要檢查值是否存在，您可以執行下列動作：

```
$variable == null
```

多個條件

您可以使用 and和 將多個表達式結合在一起or。Amazon Fraud Detector 會在找到單一 true 值時在OR表達式中停止，並在找到單一 false 值AND時在 中停止。

在下面的範例中，我們使用 條件來檢查兩個and條件。在第一個陳述式中，我們正在檢查變數 1 是否小於 100。在第二個階段，我們會檢查變數 2 是否不是美國。

由於規則使用 and，因此整個條件都必須是 TRUE，才能評估為 TRUE。

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

您可以使用括號將布林值操作分組，如下所示：

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

其他表達式類型

DateTime 函數

函式	描述	範例
getcurrentdatetime()	以 ISO8601 UTC 格式提供規則執行的目前時間。您可以使用 getepochmilliseconds(getcurrentdatetime()) 來執行其他操作	getcurrentdatetime() == "2023-03-28T18：34：02Z"
isbefore(DateTime1、DateTime2)	如果發起人 DateTime1 早於 DateTime2，則傳回布林值 (True/False)	isbefore(getcurrentdatetime()，"2019-11-30T01：01：01Z") == "False" isbefore(getcurrentdatetime()，"2050-11-30T01：05：01Z") == "True"
isafter(DateTime1，DateTime2)	如果發起人 DateTime1 晚於 DateTime2，則傳回布林值 (True/False)	isafter(getcurrentdatetime()，"2019-11-30T01：01：01Z") == "True"

函式	描述	範例
		isafter(getcurrentdatetime()，"2050-11-30T01：05：01Z") == "False"
getepochmilliseconds(DateTime)	採用 DateTime，並以 epoch 毫秒傳回該 DateTime。適用於在日期執行數學操作	getepochmilliseconds("2019-11-30T01：01：01Z") == 1575032461

字串運算子

運算子	範例
將字串轉換為大寫	uppercase($variable)
將字串轉換為小寫	lowercase($variable)

其他

運算子	註解
新增註解	# 我的評論

建立 規則

您可以在 Amazon Fraud Detector 主控台、使用 create-rule 命令、使用 CreateRule API 或使用 建立規則 適用於 Python (Boto3) 的 AWS SDK。

每個規則都必須包含單一表達式，以擷取您的商業邏輯。所有表達式都必須評估為布林值 (true 或 false)，且長度小於 4，000 個字元。不支援 If-else 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、與可變類型相關聯，並填入項目。

下列範例會建立現有偵測器 `high_risk`的規則`payments_detector`。規則會將表達式和結果`verify_customer`與規則建立關聯。

先決條件

若要遵循下述步驟，請務必先完成下列步驟，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，請將範例偵測器名稱、規則名稱、規則表達式和結果名稱取代為與您使用案例相關的名稱和表達式。

在 Amazon Fraud Detector 主控台中建立新的規則

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，選擇偵測器，然後選取您為使用案例建立的偵測器，例如 payments_detector。
3. 在 payments_detector 頁面中，選擇關聯的規則索引標籤，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 - 選用中，選擇性地輸入規則描述，例如，**This rule captures events with a high ML model score**
   c. 在表達式中，使用表達式快速參考指南輸入使用案例的規則表達式。範例 `$sample_fraud_detection_model_insightscore >900`
   d. 在結果中，選擇您為使用案例建立的結果，例如 verify_customer。結果是詐騙預測的結果，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的規則。這是 Amazon Fraud Detector 自動提供偵測器使用的規則第 1 版。

使用 建立規則 適用於 Python (Boto3) 的 AWS SDK

下列範例程式碼使用 CreateRule API 來建立現有偵測器 `high_risk`的規則`payments_detector`。範例程式碼也會將規則表達式和結果新增至`verify_customer`規則。

先決條件

若要使用範例程式碼，請確定您已完成下列操作，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，請將範例偵測器名稱、規則名稱、規則表達式和結果名稱取代為與您使用案例相關的名稱和表達式。

```
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 Fraud Detector 會自動將其提供給偵測器使用。

更新規則

您可以隨時更新規則，方法是新增或更新規則描述、更新規則表達式，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 Fraud Detector 主控台中使用 update-rule-version 命令、使用 UpdateRuleVersion API 或使用 AWS SDK 來更新規則。

更新規則後，請務必更新您的偵測器版本，以使用新的規則版本。

在 Amazon Fraud Detector 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。導覽至 Amazon Fraud Detector。
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，選擇關聯的規則索引標籤，然後選取您要更新的規則。
5. 在規則頁面中，選擇動作，然後選擇建立版本。
6. 請注意，版本已變更。輸入更新的描述、表達式或結果。

7. 選擇儲存新版本

使用 更新規則 適用於 Python (Boto3) 的 AWS SDK

下列範例程式碼使用 UpdateRuleVersion API，將規則的閾值`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。規則是告訴 Amazon Fraud Detector 如何在詐騙預測期間解譯輸入資料的條件。例如，您可以建立 IP 地址清單，然後建立規則，以在特定 IP 地址位於清單中時拒絕存取。使用清單的規則會以 `$ip_address_value` `@list_name` 格式表示。

使用 Amazon Fraud Detector，您可以新增或移除資料來管理清單，而不需要更新相關聯的規則。與您的清單相關聯的規則會自動納入新新增或移除的資料。

清單最多可包含 100，000 個唯一項目，每個項目的長度最多可達 320 個字元。根據預設，您在規則中使用的每個清單都會與 Amazon Fraud Detector 的 變數類型 FREE_FORM_TEXT 相關聯。您可以隨時將變數類型指派給您的清單。您可以在規則中使用最多 3 個清單。

您可以使用 API、使用 或使用 AWS SDK，在 Amazon Fraud Detector 主控台中建立清單、將項目新增至清單 AWS CLI、刪除清單，或刪除清單中的一或多個項目，或將變數類型指派給清單。

建立清單

您可以在事件資料集中建立包含變數輸入資料的清單（項目），並在規則表達式中使用清單。清單中的項目可以動態管理，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 變數類型支援的建立關聯。根據預設，Amazon Fraud Detector 會假設清單為 FREE_FORM_TEXT 變數類型。

您可以在 Amazon Fraud Detector 主控台、使用 API、使用 AWS CLI或使用 AWS SDK 建立清單。

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. 在清單詳細資訊下
   a. 在清單名稱中，輸入清單的名稱。
   b. 在描述中，選擇性地輸入描述。
   c. （選用）在變數類型中，為您的清單選取變數類型。

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

4. 在新增清單資料中，新增清單項目，每行一個項目。您也可以從試算表複製和貼上項目。

> **Note**
> 請確定項目不是使用逗號分隔，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 Create (建立)。

使用 建立清單 適用於 Python (Boto3) 的 AWS SDK

您可以透過指定清單名稱來建立清單。建立清單時，您可以選擇提供描述、建立變數類型關聯，或將項目新增至清單。或者，您可以稍後透過新增項目或描述來更新清單。如果您在建立清單時尚未指派變數類型，則可以稍後將變數類型指派給清單。清單的變數類型在指派後就無法變更。

> **Important**
>
> 如果您的清單包含 IP 地址，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。

下列範例使用 CreateList API 操作，透過提供描述、變數類型和新增四個`allow_email_ids`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']
     )
```

在清單中新增項目

建立清單之後，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，您不需要更新與清單相關聯的規則。規則會自動納入新增的項目。

您的清單最多可包含 100，000 個唯一項目，每個項目最多可達 320 個字元。

您可以在 Amazon Fraud Detector 主控台中使用 API、 AWS CLI或使用 AWS SDK 新增項目。

使用 Amazon Fraud Detector 主控台在清單中新增項目

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. 在清單詳細資訊頁面中，選取列出資料索引標籤，然後選擇新增資料。
5. 在新增清單資料方塊中，在每個行上新增一個項目，或從試算表複製和貼上項目。請確定不要使用逗號分隔項目。

6. 選擇新增。

使用 在清單中新增項目 適用於 Python (Boto3) 的 AWS SDK

下列範例使用 UpdateList API 操作，在allow_email_ids清單中新增兩個新項目。請確定您正在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']
```

將變數類型指派給清單

您在規則中使用的每個清單都必須與 Amazon Fraud Detector 的變數類型變數類型相關聯。根據預設，Amazon Fraud Detector 會假設清單為 FREE_FORM_TEXT 變數類型。請務必注意，包含 IP 地址的清單必須與 IP_ADDRESS 變數類型相關聯。

您可以在建立清單時或稍後隨時將清單與變數類型建立關聯。如果您已將清單與變數類型建立關聯，並希望稍後再變更，則必須建立新的清單。您無法變更清單的變數類型。

您可以在 Amazon Fraud Detector 主控台中使用 API、 或使用 AWS SDK AWS CLI來指派變數類型。

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

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. 在清單詳細資訊頁面中，選擇動作，然後選取編輯清單。
5. 在編輯清單方塊中，選取您清單的變數類型。
6. 選擇 Save (儲存)。

使用 將變數類型指派給清單 適用於 Python (Boto3) 的 AWS SDK

下列範例使用 UpdateList API 操作來指派要allow_ip_address列出的變數類型。

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

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

刪除清單

您可以刪除未用於任何規則的清單。當您刪除清單時，Amazon Fraud Detector 會永久刪除該清單和清單中的所有項目。

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

使用 Amazon Fraud Detector 主控台刪除清單

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. 在清單詳細資訊頁面中，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 適用於 Python (Boto3) 的 AWS SDK

下列範例使用 DeleteList API 操作來刪除 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。當您刪除清單中的項目時，您不需要更新規則，清單會與之建立關聯。規則會自動合併更新的清單。

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

使用 Amazon Fraud Detector 主控台從清單中刪除項目

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. 在清單詳細資訊頁面中，選取列出資料索引標籤，然後選取要刪除的項目。
5. 選擇刪除，然後再次選擇刪除進行確認。

使用 從清單中刪除項目 適用於 Python (Boto3) 的 AWS SDK

在下列範例中，UpdateList API 操作會從`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']
)
```

從清單中刪除所有項目

如果規則中未使用清單，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，稍後再新增相同清單中的項目。

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

使用 Amazon Fraud Detector 主控台從清單中刪除所有項目

從清單中刪除所有項目

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. 在清單詳細資訊頁面中，選取列出資料索引標籤，然後選擇全部刪除。
5. 在刪除所有方塊中，輸入 `delete all` 進行確認，然後選擇刪除所有清單資料。

使用 從清單中刪除所有項目 適用於 Python (Boto3) 的 AWS SDK

在下列範例中，UpdateList API 操作會從`allow_email_ids`清單中刪除所有項目。

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

結果

結果是詐騙預測的結果。您可以為每個可能的詐騙預測結果建立結果。例如，您可能希望結果代表風險層級 (high_risk、mediad_risk 和 low_risk) 或動作（核准、檢閱）。建立結果之後，您可以將一或多個結果新增至規則。在 GetEventPrediction 回應中，Amazon Fraud Detector 會傳回任何相符規則的定義結果。

建立結果

您可以在 Amazon Fraud Detector 主控台、使用 put-outcome 命令、使用 PutOutcome API 或使用 建立結果 適用於 Python (Boto3) 的 AWS SDK。

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。導覽至 Amazon Fraud Detector。
2. 在左側導覽窗格中，選擇結果。
3. 在結果頁面中，選擇建立。
4. 在您的新結果頁面中，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，選擇性地輸入描述。
5. 選擇儲存結果。
6. 重複步驟 2 到 5 來建立其他結果。

使用 建立結果 適用於 Python (Boto3) 的 AWS SDK

下列範例使用 PutOutcome API 來建立三個結果。它們是 `verify_customer`、 `review`和 `approve`。建立結果之後，您可以將結果指派給規則。

```
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。

當您刪除結果時，Amazon Fraud Detector 會永久刪除該結果，且資料不會再存放在 Amazon Fraud Detector 中。

您可以在 Amazon Fraud Detector 主控台中使用 delete-outcome 命令、使用 DeleteOutcome API 或使用 適用於 Python (Boto3) 的 AWS SDK

在 Amazon Fraud Detector 主控台中刪除結果

刪除結果

1. 登入 AWS Management Console 並開啟 Amazon Fraud Detector 主控台，網址為 https://console.aws.amazon.com/frauddetector：//。
2. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇資源，然後選擇結果。
3. 選擇您要刪除的結果。
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 適用於 Python (Boto3) 的 AWS SDK

下列範例使用 DeleteOutcome API 刪除`verify_customer`結果。刪除結果後，您無法再將其指派給規則。

```
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。您會提供實體類型 (ENTITY_TYPE) 和實體識別符 (ENTITY_ID) 做為事件資料集的一部分，以指出執行事件的特定實體。

Amazon Fraud Detector 使用實體類型來產生事件的詐騙預測，以指出事件執行者。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 主控台中使用 put-entity-type 命令、 PutEntityType API 或使用 建立實體類型 適用於 Python (Boto3) 的 AWS SDK。以下範例會在 Amazon Fraud Detector 主控台`customer`中使用適用於 Python 的 SDK (Boto3) 建立實體類型。如果您要建立實體類型來與事件類型建立關聯，以訓練詐騙偵測模型，請使用適用於使用案例的事件資料集中的實體類型。

使用 Amazon Fraud Detector 主控台建立實體類型

若要建立實體類型，

1. 開啟 AWS 管理主控台並登入您的帳戶。
2. 導覽至 Amazon Fraud Detector，選擇左側導覽中的實體，然後選擇建立。
3. 在建立實體頁面中，輸入客戶做為實體類型名稱。或者，輸入實體的描述。
4. 選擇 Create entity (建立實體)。

使用 建立實體類型 適用於 Python (Boto3) 的 AWS SDK

下列 適用於 Python (Boto3) 的 AWS SDK 程式碼範例使用 `PutEntityType` API 來建立實體類型 `customer`。如果您要建立實體類型來與事件類型建立關聯，以訓練詐騙偵測模型，請使用您事件資料集中適用於您使用案例的實體。

```
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，您無法刪除事件類型中包含的實體類型。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。

當您刪除實體類型時，Amazon Fraud Detector 會永久刪除該實體類型，且資料不會再存放在 Amazon Fraud Detector 中。

您可以在 Amazon Fraud Detector 主控台中使用 delete-entity-type 命令、使用 DeleteEntityType API 或使用 適用於 Python (Boto3) 的 AWS SDK

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 AWS Management Console 並開啟 Amazon Fraud Detector 主控台，網址為 https：//https://console.aws.amazon.com/frauddetector。
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. 選擇您要刪除的實體類型。
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 適用於 Python (Boto3) 的 AWS SDK

下列 適用於 Python (Boto3) 的 AWS SDK 範例程式碼會使用 DeleteEntityType API 刪除實體類型客戶。

```
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 已與 整合 AWS CloudFormation，這項服務可協助您建立和設定 Amazon Fraud Detector 資源的模型，讓您可減少建立和管理資源和基礎設施的時間。您可以建立範本，描述您想要的所有 Amazon Fraud Detector 資源 （例如偵測器、變數、EntityType、EventType、結果和標

籤），並為您 AWS CloudFormation 佈建和設定這些資源。您可以重複使用範本，在多個 AWS 帳戶和區域中一致且重複地佈建和設定資源。

使用 AWS CloudFormation 無需額外費用。

建立 Amazon Fraud Detector 範本

若要佈建和設定 Amazon Fraud Detector 和相關服務的資源，您必須了解 AWS CloudFormation 範本。範本是以 JSON 或 YAML 格式化的文本檔案。這些範本說明您想要在 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 設計工具來協助您開始使用 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 設計工具？。

您也可以使用 AWS CloudFormation 範本建立、更新和刪除 Amazon Fraud Detector 資源。如需詳細資訊，包括 資源的 JSON 和 YAML 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。

如果您已使用 CloudFormation，則不需要管理其他 IAM 政策或 CloudTrail 記錄。

管理 Amazon Fraud Detector 堆疊

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 將包含哪些資源到您的堆疊中。您也可以將已建立的 Amazon Fraud Detector 資源匯入 CloudFormation 管理中，方法是將其匯入新的或現有的堆疊。

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

整理 Amazon Fraud Detector 堆疊

您組織 AWS CloudFormation 堆疊的方式完全由您決定。一般而言，最佳實務是依生命週期和擁有權來組織堆疊。這表示資源的分組方式是變更頻率，或由負責更新資源的團隊進行分組。

您可以選擇為每個偵測器及其偵測邏輯（例如規則、變數等）建立堆疊來組織堆疊。如果您使用的是其他服務，您應該考慮是否要將 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，以協助收集資料和處理資料的 Amazon Fraud Detector 資源。這可能是確保所有詐騙團隊產品一起運作的有效方法。

了解 Amazon Fraud Detector CloudFormation 參數

除了所有 CloudFormation 範本中提供的標準參數之外，Amazon Fraud Detector 還推出兩個額外的參數，可協助您管理部署行為。如果您不包含其中一個或兩個參數，CloudFormation 將使用如下所示的預設值。

參數	值	預設值
DetectorVersionStatus	ACTIVE：將新的/更新的偵測器版本設定為作用中狀態 草稿：將新/更新偵測器版本設定為草稿狀態	草稿
內嵌	TRUE：在create/update/delete堆疊時，允許 CloudFormation creating/updating/deleting資源。 FALSE：允許 CloudFormation 驗證物件是否存在，但不會對物件進行任何變更。	TRUE

Amazon Fraud Detector 資源的範例 AWS CloudFormation 範本

以下是用於管理偵測器和相關聯偵測器版本的 AWS CloudFormation YAML 範本範例。

```
# 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
- AWS CloudFormation API 參考
- AWS CloudFormation 命令列界面使用者指南

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。若要產生單一事件或一組事件的詐騙預測，您需要提供下列資訊給 Amazon Fraud Detector：

- 詐騙預測邏輯
- 事件中繼資料

詐騙偵測邏輯

詐騙預測邏輯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 - 定義預測詐騙的演算法和資料需求
- 變數 - 代表與事件相關聯的資料元素
- 規則 - 告知 Amazon Fraud Detector 如何在詐騙預測期間解譯變數值
- 結果 - 詐騙預測所產生的結果
- 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。開始產生詐騙預測之前，請確定您已建立並發佈包含詐騙預測邏輯的偵測器版本。您可以使用詐騙偵測器主控台或 API 來建立和發佈偵測器版本。如需使用 主控台的指示，請參閱入門（主控台）。如需使用 API 的指示，請參閱建立偵測器版本。

事件中繼資料

事件中繼資料提供正在評估之事件的詳細資訊。您要評估的每個事件都必須包含與偵測器版本相關聯的事件類型中每個變數的值。此外，您的事件中繼資料必須包含下列項目：

- EVENT_ID – 事件的識別符。例如，如果您的事件是線上交易，EVENT_ID 可能是提供給客戶的交易參考號碼。

  EVENT_ID 的重要備註

  - 該事件必須是唯一的
  - 應該代表對您的業務有意義的資訊

  - 必須滿足規則表達式模式： `^[0-9a-z_-]+$.`
  - 必須儲存。EVENT_ID 是事件的參考，用於對事件執行操作，例如刪除事件。
  - 不建議將時間戳記附加到 EVENT_ID，因為它可能會在稍後您想要更新事件時發生問題，因為您需要提供完全相同的 EVENT_ID。
- ENTITY_TYPE – 執行事件的實體，例如商家或客戶。
- ENTITY_ID - 執行事件之實體的識別符。ENTITY_ID 必須滿足下列規則表達式模式：`^[0-9a-z_-]+$`。如果評估時無法使用 ENTITY_ID，請傳遞未知的字串。
- EVENT_TIMESTAMP - 事件發生時的時間戳記。時間戳記必須在 UTC 中為 ISO 8601 標準。

即時預測

您可以透過呼叫 `GetEventPrediction` API 即時評估線上活動是否有詐騙。您可以提供每個請求中單一事件的相關資訊，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。

即時詐騙預測的運作方式

`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)。在回應中，Amazon Fraud Detector 會提供模型分數，以及與相符規則相關聯的任何結果。

取得即時詐騙預測

若要取得即時詐騙預測，請確定您已建立並發佈包含詐騙預測模型和規則的偵測器，或只是規則集。

您可以使用 AWS 命令列界面 (AWS CLI) 或其中一個 Amazon Fraud Detector SDKs 呼叫 GetEventPrediction API 操作，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，您必須指定 `detectorId` Amazon Fraud Detector 將使用 來評估事件。您可以選擇性地指定 `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，透過在 欄位中傳遞資料來叫用 SageMaker AI 模型`externalModelEndpointBlobs`。

使用 取得詐騙預測 適用於 Python (Boto3) 的 AWS SDK

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，以及任何相符的規則和對應的結果。您可以在 aws-fraud-detector-samples GitHub 儲存庫上找到GetEventPrediction請求的其他範例。

```
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

您可以使用 Amazon Fraud Detector 中的批次預測任務，以取得一組不需要即時評分的事件的預測。例如，您可以建立批次預測任務來執行離線proof-of-concept，或回溯性評估每小時、每日或每週的事件風險。

您可以使用 Amazon Fraud Detector 主控台建立批次預測任務，或使用 AWS Command Line Interface (AWS CLI) 或其中一個 Amazon Fraud Detector SDKs 呼叫 CreateBatchPredictionJob API 操作。

主題

- 批次預測的運作方式
- 輸入和輸出檔案
- 取得批次預測
- IAM 角色指引
- 使用 取得批次詐騙預測 適用於 Python (Boto3) 的 AWS SDK

批次預測的運作方式

CreateBatchPredictionJob API 操作使用指定的偵測器版本，根據位於 Amazon S3 儲存貯體的輸入 CSV 檔案中提供的資料進行預測。API 接著會將產生的 CSV 檔案傳回至 S3 儲存貯體。

批次預測任務會以與GetEventPrediction操作相同的方式計算模型分數和預測結果。與 類似GetEventPrediction，若要建立批次預測任務，您會先建立事件類型、選擇性地訓練模型，然後建立偵測器版本來評估批次任務中的事件。

批次預測任務評估的事件風險分數定價與 GetEventPrediction API 建立的分數定價相同。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任務。

輸入和輸出檔案

輸入 CSV 檔案應包含符合與所選偵測器版本相關聯的事件類型的標頭。輸入資料檔案的大小上限為 1GB。事件數量會因事件大小而異。

除非您為輸出資料指定不同的位置，否則 Amazon Fraud Detector 會在與輸入檔案相同的儲存貯體中建立輸出檔案。輸出檔案包含來自輸入檔案的原始資料和下列附加資料欄：

- MODEL_SCORES — 詳細說明與所選偵測器版本相關聯之每個模型的事件模型分數。
- OUTCOMES — 詳細說明所選偵測器版本及其規則評估的事件結果。
- STATUS — 指出事件是否已成功評估。如果事件未成功評估，此欄會顯示失敗的原因代碼。
- RULE_RESULTS — 根據規則執行模式比對的所有規則清單。

取得批次預測

下列步驟假設您已建立事件類型、使用該事件類型訓練模型 （選用），以及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 並開啟 Amazon Fraud Detector 主控台，網址為 https：//https://console.aws.amazon.com/frauddetector。
2. 在 Amazon Fraud Detector 主控台的左側導覽窗格中，選擇批次預測，然後選擇新批次預測。
3. 在任務名稱中，指定批次預測任務的名稱。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偵測器版本。如果您的偵測器具有處於 Active 狀態的偵測器版本，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，選擇或建立具有輸入和輸出 Amazon S3 儲存貯體讀取和寫入存取權的角色。如需更多資訊，請參閱IAM 角色指引。

   若要取得批次預測，呼叫 CreateBatchPredictionJob操作的 IAM 角色必須具有輸入 S3 儲存貯體的讀取許可，以及輸出 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。如果您想要將輸出檔案放在不同的 S3 儲存貯體中，請選取分開資料位置進行輸出，並提供輸出資料的 Amazon S3 位置。
8. （選用）為您的批次預測任務建立標籤。
9. 選擇 開始使用。

   Amazon Fraud Detector 會建立批次預測任務，且任務的狀態為 In progress。批次預測任務處理時間會根據事件數量和偵測器版本組態而有所不同。

若要停止正在進行的批次預測任務，請前往批次預測任務詳細資訊頁面，選擇動作，然後選擇停止批次預測。如果您停止批次預測任務，您將不會收到任務的任何結果。

當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。輸出檔案名稱的格式為 batch prediction job name_file creation timestamp_output.csv。例如，來自名為 之任務的輸出檔案mybatchjob為 mybatchjob_1611170650_output.csv。

若要搜尋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任務，請前往批次預測任務詳細資訊頁面，選擇動作，然後選擇刪除批次預測。

IAM 角色指引

若要取得批次預測，呼叫 CreateBatchPredictionJob 操作的 IAM 角色必須具有輸入 S3 儲存貯體的讀取許可，並將許可寫入輸出 S3 儲存貯體。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。在 Amazon Fraud Detector 主控台上，您有三個選項可選取批次預測的 IAM 角色：

1. 在建立新的批次預測任務時建立角色。
2. 選取您先前在 Amazon Fraud Detector 主控台中建立的現有 IAM 角色。執行此步驟之前，請務必將 `S3:PutObject` 許可新增至角色。
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，請確認下列事項：

1. 您的 Amazon S3 輸入和輸出儲存貯體與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`許可，以及輸出 S3 儲存貯體的`s3:PutObject`許可。
3. 您使用的 IAM 角色具有服務主體 的信任政策`frauddetector.amazonaws.com`。

使用 取得批次詐騙預測 適用於 Python (Boto3) 的 AWS SDK

下列範例顯示 CreateBatchPredictionJob API 的範例請求。批次預測任務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`、偵測器 `sample_detector`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

預測說明可讓您深入了解每個事件變數如何影響模型的詐騙預測分數，並自動產生做為詐騙預測的一部分。每個詐騙預測的風險分數介於 1 到 1000 之間。預測說明提供每個事件變數在大小 (0-5，5 為最

高）和方向（提高或降低分數）方面對風險分數影響的詳細資訊。您也可以針對下列任務使用預測說明：

- 在標記事件以供檢閱時，識別手動反轉期間的首要風險指標。
- 縮小導致誤報預測的根本原因（例如，合法事件的高風險分數）。
- 分析事件資料中的詐騙模式，並偵測資料集中的任何偏差。

> **Important**
>
> 預測說明會自動產生，且僅適用於 2021 年 6 月 30 日當天或之後訓練的模型。若要接收 2021 年 6 月 30 日之前所訓練模型的預測說明，請重新訓練這些模型。

預測說明為用於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之規模影響的視覺化參考。相對影響值由星星評分 (0-5，5 為最高）和詐騙風險的方向（增加/減少）影響組成。

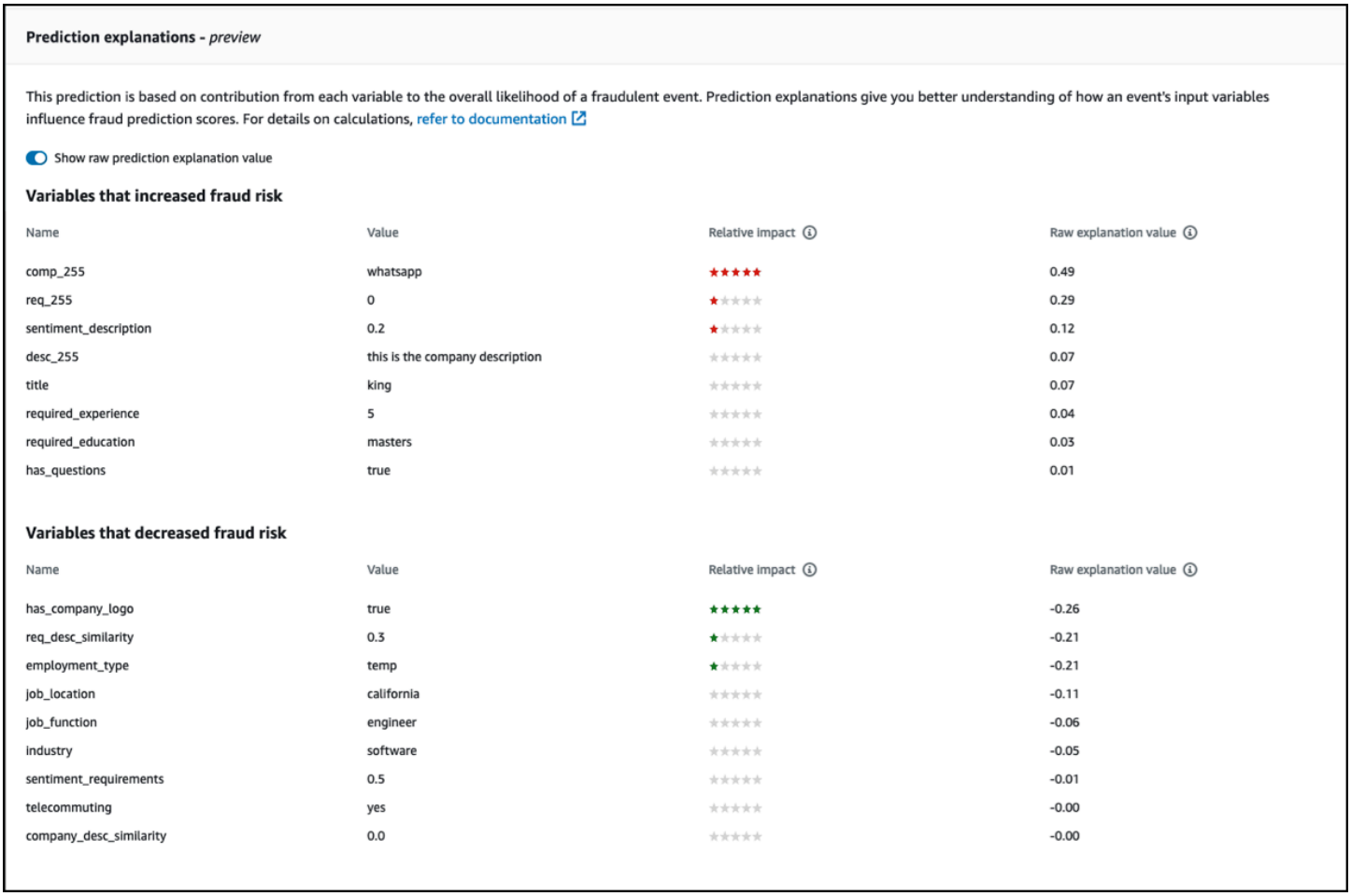
- 會增加詐騙風險的變數會以紅色星星表示。紅色星星的數量越高，變數就越能提高詐騙分數，並增加詐騙的可能性。
- 降低詐騙風險的變數會以綠色星星表示。綠色的啟動次數越高，變數越能降低詐騙風險分數，並降低詐騙的可能性。
- 所有變數的零星表示沒有任何變數本身會大幅改變詐騙風險。

原始說明值

提供原始、未解譯的值，以詐騙的日誌目錄表示。這些值通常介於 -10 到 +10 之間，但範圍從 - 無限到 + 無限。

- 正值表示變數提高風險分數。
- 負值表示變數將風險分數向下推。

在 Amazon Fraud Detector 主控台中，預測說明值會顯示如下。彩色星星評分和對應的原始數值，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 APIs 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 AWS 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，選擇搜尋過去的預測。
3. 使用 屬性、運算子和值篩選條件來選取您要檢閱的預測。
4. 在頂部篩選條件窗格中，請務必選取您要檢閱的預測產生時間期間。
5. 結果窗格會顯示指定期間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. 在 上設定顯示原始預測解釋值按鈕，以檢視所有變數的原始預測解釋值。

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 AWS SDK 的 `ListEventPredictions`和 `GetEventPredictionMetadata` API 檢視預測說明的範例請求。 APIs

範例 1：使用 `ListEventPredictions` API 取得最新預測的清單

```
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：取得使用 `GetEventPredictionMetadata` API 在指定期間內產生之指定事件 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。

首先呼叫 `ListEventPredictions` API 來取得此請求`predictionTimestamp`指定的 。

```
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 Additive exPlanations)，透過計算用於模型訓練之每個事件變數的原始解釋值來解釋個別事件預測。產生預測時，原始解釋值由模型計算為分類演算法的一部分。這些原始解釋值代表每個輸入對詐騙機率對日誌的貢獻。原始解釋值（從 -infinity 轉換為 +infinity) 會使用映射轉換為相對影響值 (-5 至 +5)。衍生自原始解釋值的相對影響值代表詐騙（正面）或合法（負面）機率增加的次數，讓您更容易了解預測解釋。

Amazon Fraud Detector 的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。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 Cloud 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。在AWS 合規計畫中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 Amazon Fraud Detector 的合規計劃，請參閱合規計劃的 AWS 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。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。

本文件可協助您了解如何在使用 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 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Amazon Fraud Detector 資源。

主題

Amazon Fraud Detector 中的資料保護

AWS 共同的責任模型適用於 Amazon Fraud Detector 中的資料保護。如此模型所述， AWS 負責保護執行所有 的 全球基礎設施 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，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 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。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，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) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Amazon Fraud Detector 或使用主控台、API AWS CLI或其他 AWS 服務 AWS SDKs 時。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，預設會使用此金鑰來加密資料。
- 客戶受管 KMS 金鑰。您可以使用金鑰政策控制對客戶受管 KMS 金鑰的存取。如需建立和管理客戶受管 KMS 金鑰的資訊，請參閱 金鑰管理。

加密傳輸中的資料

Amazon Fraud Detector 會從您的帳戶複製資料，並在內部 AWS 系統中處理資料。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 會使用兩種類型的金鑰之一來加密您的資料：

- AWS 擁有的 KMS 金鑰。此為預設值。

- 客戶受管 KMS 金鑰。

建立客戶受管 KMS 金鑰

您可以使用 KMS 主控台或 CreateKey API 來建立客戶受管 AWS KMS 金鑰。建立金鑰時，請務必：

- 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 Key Management Service 開發人員指南中的 中的非對稱 AWS KMS AWS 金鑰。
- 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 Key Management Service 開發人員指南中的 中的多區域 AWS KMS AWS 金鑰。
- 提供下列金鑰政策，以授予 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": "*"
}
```

如需金鑰政策的資訊，請參閱 Key Management Service 開發人員指南中的在 AWS KMS 中使用金鑰政策。 AWS

使用客戶受管 KMS 金鑰加密資料

使用 Amazon Fraud Detector 的 PutKMSEncryptionKey API，透過客戶受管 KMS 金鑰加密您的 Amazon Fraud Detector 靜態資料。您可以隨時使用 PutKMSEncryptionKey API 變更加密組態。

有關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。設定客戶受管 KMS 金鑰之前產生的資料將保持未加密。
- 如果變更客戶受管 KMS 金鑰，則不會重新加密使用先前加密組態加密的資料。

檢閱資料

當您使用客戶受管 KMS 金鑰來加密 Amazon Fraud Detector 資料時，無法使用 Amazon Fraud Detector 主控台的搜尋過去預測區域中的篩選條件來搜尋使用此方法加密的資料。為了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
- 評估時間戳記
- 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
- 規則比對狀態
- 規則版本
- 變數資料來源

如果客戶受管 KMS 金鑰已刪除或排定刪除，則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 和介面 VPC 端點 (AWS PrivateLink)

您可以建立介面 VPC 端點，在 VPC 和 Amazon Fraud Detector 之間建立私有連線。介面端點採用 AWS PrivateLink技術，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，私下存取 Amazon Fraud Detector APIs。VPC 中的執行個體不需要公有 IP 地址，即可與 Amazon Fraud Detector APIs通訊。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》中的界面 VPC 端點 (AWS PrivateLink)。

Amazon Fraud Detector VPC 端點的考量事項

為 Amazon Fraud Detector 設定介面 VPC 端點之前，請務必檢閱《Amazon VPC 使用者指南》中的介面端點屬性和限制。

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。根據預設，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 () 為 Amazon Fraud Detector 服務建立 VPC 端點AWS CLI。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，您可以使用區域的預設 DNS 名稱向 Amazon Fraud Detector 提出 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 建立介面 VPC 端點的政策，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 端點政策指定所有可存取 VPC 介面端點的使用者，都可以存取名為 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
- 叫用 Amazon Fraud Detector `GetEventPrediction` API

> **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

您提供給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、隱私權和內容的安全性是我們的最高優先順序，並確保我們的使用符合我們對您的承諾。如需詳細資訊，請參閱資料隱私權常見問答集

您可以選擇不讓事件資料用於開發或改善 Amazon Fraud Detector 的品質，方法是造訪 AWS Organizations 使用者指南中的 AI 服務選擇退出政策頁面，並遵循其中說明的程序。

> **Note**
>
> 您的 AWS 帳戶需要由 AWS Organizations 集中管理，您才能使用選擇退出政策。如果您尚未為 AWS 帳戶建立組織，請造訪建立和管理組織頁面，並遵循其中說明的程序。

Amazon Fraud Detector 的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ），以使用 Amazon Fraud Detector 資源。IAM 是您可以免費使用 AWS 服務 的 。

主題

目標對象

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

服務使用者 – 如果您使用 Amazon Fraud Detector 服務來執行任務，您的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 功能來執行工作時，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 對 Amazon Fraud Detector 身分和存取進行故障診斷。

服務管理員 – 如果您在公司負責 Amazon Fraud Detector 資源，您可能擁有 Amazon Fraud Detector 的完整存取權。您的任務是判斷服務使用者應存取哪些 Amazon Fraud Detector 功能和資源。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搭配 Amazon Fraud Detector 使用 IAM，請參閱 Amazon Fraud Detector 如何與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解撰寫政策以管理 Amazon Fraud Detector 存取權的詳細資訊。若要檢視您可以在 IAM 中使用的 Amazon Fraud Detector 身分型政策範例，請參閱 Amazon Fraud Detector 身分型政策範例。

使用身分驗證

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

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您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。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 《 使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

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 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。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 IAM 中的AWS 多重要素驗證。

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，該身分可以完整存取帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 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 中的身分 AWS 帳戶 ，具有單一人員或應用程式的特定許可。建議您盡可能依賴臨時憑證，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，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色（主控台）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以將政策直接連接到資源（而不是使用角色做為代理）。如需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 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，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。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在其中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。

- 服務連結角色 – 服務連結角色是一種連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。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 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。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臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件， AWS 當與身分或資源相關聯時， 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對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。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 API AWS 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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 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來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 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政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個 的服務。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 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括 AWS 服務 支援 RCPs 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 (RCPs)。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon Fraud Detector 如何與 IAM 搭配使用

使用 IAM 管理 Amazon Fraud Detector 的存取權之前，您應該了解哪些 IAM 功能可與 Amazon Fraud Detector 搭配使用。若要全面了解 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 AWS 搭配使用的 服務。

主題

- Amazon Fraud Detector 身分型政策
- Amazon Fraud Detector 資源型政策
- 根據 Amazon Fraud Detector 標籤的授權
- 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，建議您建立僅限存取 Amazon Fraud Detector 操作和必要許可的使用者。您可以視需要新增其他許可。下列政策提供使用 Amazon Fraud Detector 所需的許可：`AmazonFraudDetectorFullAccessPolicy`和 `AmazonS3FullAccess`。如需使用這些政策設定 Amazon Fraud Detector 的詳細資訊，請參閱 設定 Amazon Fraud Detector。

動作

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符的 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之前使用下列字首：frauddetector:。例如，若要使用 Amazon Fraud Detector CreateRule API 操作建立規則，請在政策中包含 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，描述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 ARNs。

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 ARNs 格式的詳細資訊，請參閱 Amazon Resource Name (ARNs) AWS 和服務命名空間。

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/*"
```

有些 Amazon Fraud Detector 動作無法在特定資源上執行，例如用於建立資源的動作。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 ARNs 的清單，請參閱《IAM 使用者指南》中的 Amazon Fraud Detector 定義的資源。若要了解您可以指定每個資源的 ARN 的動作，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內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值， 會使用邏輯OR操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，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的條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

Amazon Fraud Detector 會定義自己的一組條件金鑰，也支援使用一些全域條件金鑰。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。

根據 Amazon Fraud Detector 標籤的授權

您可以將標籤連接至 Amazon Fraud Detector 資源，或在請求中將標籤傳遞至 Amazon Fraud Detector。如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

Amazon Fraud Detector IAM 角色

IAM 角色是您 AWS 帳戶中具有特定許可的實體。

搭配 Amazon Fraud Detector 使用臨時登入資料

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 GetFederationToken 等 AWS STS API 操作來取得臨時安全登入資料。

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

根據預設，使用者和 IAM 角色沒有建立或修改 Amazon Fraud Detector 資源的許可。他們也無法使用 AWS Management Console AWS CLI或 AWS API 執行任務。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

身分型政策會判斷您帳戶中的某個人員是否可以建立、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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。

- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 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。

Amazon Fraud Detector 的 AWS 受管 （預先定義） 政策

AWS 透過提供由 建立和管理的獨立 IAM 政策，解決許多常見的使用案例 AWS。這些 AWS 受管政策會授予常見使用案例的必要許可，讓您不必調查需要哪些許可。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。

下列 AWS 受管政策是 Amazon Fraud Detector 特有的，您可以連接到您帳戶中的使用者：

`AmazonFraudDetectorFullAccess`：授予 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 SageMaker AI 中的所有模型端點
- 列出帳戶中的所有 IAM 角色
- 列出所有 Amazon S3 儲存貯體
- 允許 IAM Pass 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，則還需要 `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，以視需要允許 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。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

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

允許唯讀存取 Amazon Fraud Detector 資源

在此範例中，您將 Amazon Fraud Detector 資源 AWS 帳戶 的唯讀存取權授予 使用者。

```
{
    "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，您授予 使用者 AWS 帳戶 存取除一個特定偵測器資源以外的所有動作和資源。

```
{
    "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 提供雙模式取得可同時做為 List 和 Describe 操作APIs。呼叫 時，沒有任何參數的雙模式 API 會傳回與 相關聯的指定資源清單 AWS 帳戶。使用 參數呼叫 時，雙模式 API 會傳回指定資源的詳細資訊。資源可以是模型、變數、事件類型或實體類型。

雙模式 APIs 支援 IAM 政策中的資源層級許可。不過，只有在請求中提供一或多個參數時，才會套用資源層級許可。例如，如果使用者呼叫 GetVariables API 並提供變數名稱，而且有連接至變數資源或變數名稱的 IAM 拒絕政策，則使用者會收到`AccessDeniedException`錯誤。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，這可能會導致資訊洩漏。

若要允許使用者僅檢視特定資源的詳細資訊，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 拒絕政策後，使用者只能檢視 NotResource區塊中指定的資源詳細資訊。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：NotResource。

下列範例政策允許使用者存取 Amazon Fraud Detector 的所有資源。不過，NotResource政策元素用於將 GetVariables API 呼叫限制為只有字首為 user*、 job_*和 的變數名稱var*。

```
{
 "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

在此範例政策中，回應會顯示下列行為：

- 不包含變數名稱的 GetVariables 呼叫會導致AccessDeniedException錯誤，因為請求會映射到拒絕陳述式。
- 包含不允許的變數名稱的 GetVariables 呼叫會導致AccessDeniedException錯誤，因為變數名稱不會對應至NotResource區塊中的變數名稱。例如，具有變數名稱的 GetVariables 呼叫email_address會導致AccessDeniedException錯誤。
- 包含符合NotResource區塊中變數名稱之變數名稱的 GetVariables 呼叫會如預期傳回。例如，包含變數名稱的 GetVariables 呼叫會job_cpa傳回job_cpa變數的詳細資訊。

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：

- 在您的 中 AWS 帳戶 ，您已定義兩個不同的群組，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 的成員在其他 2 個偵測器上進行 API 呼叫

控制對 API 呼叫的存取權 (範例)

1. 將具有金鑰`Project`和值的標籤`A`新增至 Team1 使用的偵測器。
2. 將具有 金鑰`Project`和值的標籤`B`新增至 Team2 使用的偵測器。
3. 建立具有條件的 IAM 政策`ResourceTag`，拒絕存取具有索引鍵`Project`和值 標籤的偵測器`B`，並將該政策連接至 Team1。
4. 建立具有條件的 IAM 政策`ResourceTag`，拒絕存取具有索引鍵`Project`和值 標籤的偵測器`A`，並將該政策連接至 Team2。

以下是拒絕對任何 Amazon Fraud Detector 資源執行特定動作的政策範例，該資源具有索引鍵為`Project`且值為 的標籤`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

當沒有執行動作許可的實體強制更特權的實體執行動作時，就會發生混淆代理人問題。如果您提供第三方 （稱為跨帳戶) 或其他 AWS 服務 （稱為跨服務) 存取您帳戶中的資源， AWS 會提供可協助您保護帳戶的工具。

當一個服務 (呼叫服務) 呼叫另一個服務 (呼叫的服務) 時，可能會發生跨服務混淆代理人問題。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。若要防止這種情況，您可以建立政策，以透過已授予服務資源存取權的服務主體，協助保護所有 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`， AWS STS 會傳回一組臨時安全登入資料，供服務委託人用來存取角色許可政策所允許的資源。

為了防止跨服務混淆代理人問題，Amazon Fraud Detector 建議您在角色信任政策中使用 `aws:SourceArn`和 `aws:SourceAccount`全域條件內容索引鍵，將角色的存取限制為僅由預期資源產生的請求。

`aws:SourceAccount` 指定帳戶 ID，而 `aws:SourceArn`指定與跨服務存取相關聯的資源 ARN。`aws:SourceArn` 必須使用 ARN 格式指定 。確保 `aws:SourceAccount`和 `aws:SourceArn` 在相同的政策陳述式中使用相同的帳戶 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 或指定多個資源，請將`aws:SourceArn`全域內容條件金鑰與萬用字元 (*) 用於 ARN 的未知部分。例如 `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`。如需

有關您可以在許可政策中使用的 Amazon Fraud Detector 資源和動作的資訊，請參閱 Amazon Fraud Detector 的動作、資源和條件索引鍵。

下列角色信任政策範例在aws:SourceArn條件索引鍵中使用萬用字元 (*)，以允許 Amazon Fraud Detector 存取與帳戶 ID 相關聯的多個資源。

```
{
        "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。資源限定詞是使用用於進行 PutExternalModel API 呼叫的模型端點所建置。

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

對 Amazon Fraud Detector 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 Amazon Fraud Detector 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 Amazon Fraud Detector 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 AWS 帳戶外的人員存取我的 Amazon Fraud Detector 資源
- Amazon Fraud Detector 無法擔任指定的角色

我無權在 Amazon Fraud Detector 中執行動作

如果 AWS Management Console 告訴您未獲授權執行 動作，則您必須聯絡管理員尋求協助。您的管理員是為您提供簽署憑證的人員。

當mateojackson使用者嘗試使用主控台檢視###的詳細資訊，但沒有frauddetector:*GetDetectors*許可時，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。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 `iam:PassRole`動作，您的政策必須更新，以允許您將角色傳遞給 Amazon Fraud Detector。

有些 AWS 服務 可讓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 `marymajor` 使用者嘗試使用主控台在 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 管理員。您的管理員提供您的簽署憑證。

我想要允許 AWS 帳戶外的人員存取我的 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 搭配使用。
- 若要了解如何在您擁有 AWS 帳戶 的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 中提供存取權給 IAM 使用者。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有的 。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需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 中的跨帳戶資源存取。

Amazon Fraud Detector 無法擔任指定的角色

如果您收到 Amazon Fraud Detector 無法擔任指定角色的錯誤，則必須更新指定角色的信任關係。透過將 Amazon Fraud Detector 指定為信任的實體，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。您只需要為非由 Amazon Fraud Detector 建立的 IAM 角色建立此信任關係。

建立現有角色與 Amazon Fraud Detector 的信任關係

1. 在 https：//https://console.aws.amazon.com/iam/ 開啟 IAM 主控台
2. 在導覽窗格中，選擇角色。
3. 選擇您要修改的角色名稱，然後選擇信任關係索引標籤。
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"
    } ]
}
```

在 Amazon Fraud Detector 中記錄和監控

AWS 提供下列監控工具來監看 Amazon Fraud Detector、在發生錯誤時回報，以及適時採取自動動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。如需 CloudWatch 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》。

- AWS CloudTrail 會擷取由 AWS 您的帳戶發出或代表發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。如需 CloudTrail 的詳細資訊，請參閱 AWS CloudTrail 使用者指南。

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

第三方稽核人員會在多個合規計畫中評估 AWS 服務的安全性和 AWS 合規性，例如 SOC、PCI、FedRAMP 和 HIPAA。

若要了解 AWS 服務 是否在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱AWS 合規計劃。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載報告 in AWS Artifact

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源來協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南的集合可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同責任模型。本指南摘要說明跨多個架構 （包括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)) 保護 AWS 服務和映射指南至安全控制的最佳實務。
- 《AWS Config 開發人員指南》中的使用規則評估資源 – AWS Config 服務會評估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 可讓您全面檢視其中的安全狀態 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 控制參考」。
- Amazon GuardDuty – 這會監控您的環境是否有可疑和惡意活動，以 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和業界標準的方式。

Amazon Fraud Detector 中的彈性

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 中的基礎設施安全

Amazon Fraud Detector 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 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 解決方案可靠性、可用性和效能的重要部分。AWS 提供下列監控工具來監看 Amazon Fraud Detector、在發生錯誤時回報，以及適時採取自動動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。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 會擷取由 AWS 您的帳戶發出或代表發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 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

使用 Amazon CloudWatch 監控 Amazon Fraud Detector

您可以使用 CloudWatch 監控 Amazon Fraud Detector，這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 Amazon Fraud Detector 的 CloudWatch 指標。

要使用指標，您必須指定下列資訊：

- 指標命名空間。命名空間是 Amazon Fraud Detector 用來發佈其指標的 CloudWatch 容器。如果您使用 CloudWatch ListMetrics API 或 list-metrics 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。維度是名稱值對，可協助您唯一識別指標，例如，DetectorId可以是維度名稱。指定指標維度是選用的。
- 指標名稱，例如 GetEventPrediction。

您可以使用 AWS Management Console、 AWS CLI或 CloudWatch API 來取得 Amazon Fraud Detector 的監控資料。您也可以透過其中一個 Amazon AWS 軟體開發套件 (SDK) 或 Amazon CloudWatch API 工具使用 CloudWatch API。主控台會根據 CloudWatch API 的原始資料顯示一系列圖形。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 GetEventPrediction4xxError 指標。
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 CloudWatch 監控 Amazon Fraud Detector。如需詳細資訊，請參閱 Amazon CloudWatch 身分驗證與存取控制。

存取 Amazon Fraud Detector 指標

下列步驟說明如何使用 CloudWatch 主控台存取 Amazon Fraud Detector 指標。

檢視指標 (主控台)

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 選擇指標，選擇所有指標索引標籤，然後選擇詐騙偵測器。
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 警報，在警示變更狀態時傳送 Amazon Simple Notification Service (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。

警示僅會針對持續狀態變更呼叫動作。CloudWatch 警示不會僅因為它們處於特定狀態而叫用動作。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. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇警示，然後選擇建立警示。這會開啟建立警示精靈。
3. 選擇選取指標。
4. 在所有指標索引標籤中，選擇詐騙偵測器。
5. 選擇依偵測器 ID，然後選擇 GetEventPrediction 指標。
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. 針對條件，請針對閾值類型選擇靜態，針對任何時候...選擇較大，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 會儲存清單並將其顯示在 欄位中，以便您可以使用它來設定未來的警示。

    > **Note**
    >
    > 如果您使用新清單建立新的 Amazon SNS 主題，則必須在預期收件人收到通知之前驗證電子郵件地址。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，預期收件人不會收到通知。

11. 選擇下一步。新增警示的名稱和選用描述。選擇下一步。
12. 選擇建立警示 。

Amazon Fraud Detector 指標

Amazon Fraud Detector 會將下列指標傳送至 CloudWatch。所有指標都支援這些統計資料：Average、Minimum、Maximum、Sum。

指標	描述
GetEventPrediction	GetEventPrediction API 請求的數量。 有效維度：DetectorID
GetEventPredictionLatency	回應來自 GetEventPrediction 請求的用戶端請求所花費的時間間隔。 有效維度：DetectorID 單位：毫秒
GetEventPrediction4XXError	Amazon Fraud Detector 傳回 4xx HTTP 回應碼的 GetEventPrediction 請求數量。對於每個 4xx 回應，會傳送 1 個。 有效維度：DetectorID
GetEventPrediction5XXError	Amazon Fraud Detector 傳回 5xx HTTP 回應碼的 GetEventPrediction 請求數目。對於每個 5xx 回應，會傳送 1 個。 有效維度：DetectorID
Prediction	預測數目。如果成功，則會傳送 1。 有效維度：DetectorID 、 DetectorVersionID
PredictionLatency	預測操作所花費的時間間隔。 有效維度：DetectorID 、 DetectorVersionID 單位：毫秒

指標	描述
PredictionError	Amazon Fraud Detector 遇到錯誤的預測數量。如果遇到錯誤，則會傳送 1。 有效維度：DetectorID 、 DetectorVersionID
VariableUsed	在評估過程中使用該變數的 GetEventPrediction 請求數量。 有效維度：DetectorID 、DetectorVersionID 、 VariableName
VariableDefaultReturned	在事件屬性中不存在變數的 GetEventPrediction 請求數量，因此在評估期間使用變數的預設值。 有效維度：DetectorID 、DetectorVersionID 、 VariableName
RuleNotEvaluated	由於先前規則相符，因此未評估規則的 GetEventPrediction 請求數目。 有效維度：DetectorID 、DetectorVersionID 、 RuleID
RuleEvaluateTrue	規則觸發為 True 且傳回規則結果的 GetEventPrediction 請求數量。 有效維度：DetectorID 、DetectorVersionID 、 RuleID
RuleEvaluateFalse	規則評估為 False 的 GetEventPrediction 請求數目。 有效維度：DetectorID 、DetectorVersionID 、 RuleID
RuleEvaluateError	規則錯誤評估的 GetEventPrediction 請求數量 有效維度：DetectorID 、DetectorVersionID 、 RuleID

指標	描述
OutcomeReturned	傳回指定結果的 GetEventPrediction 呼叫數目。 有效維度：DetectorID 、DetectorVersionID 、 OutcomeName
ModelInvocation (Amazon SageMaker model endpoint)	在評估過程中調用 SageMaker 模型端點的 GetEventPrediction 請求數量。 有效維度：DetectorID 、DetectorVersionID 、 ModelEndpoint
ModelInvocationError (Amazon SageMaker model endpoint)	調用 SageMaker 模型端點在評估期間傳回錯誤的 GetEventPrediction 請求數目。 有效維度：DetectorID 、DetectorVersionID 、 ModelEndpoint
ModelInvocationLatency (Amazon SageMaker model endpoint)	從 Amazon Fraud Detector 檢視匯入模型回應所花費的時間間隔。此間隔僅包含模型調用。 有效維度：DetectorID 、DetectorVersionID 、 ModelEndpoint 單位：毫秒
ModelInvocation	在評估過程中調用模型的 GetEventPrediction 請求數量。 有效維度：DetectorID 、DetectorVersionID 、ModelType 、 ModelID
ModelInvocationError	Amazon Fraud Detector 模型在評估期間傳回錯誤的 GetEventPrediction 請求數目。 有效維度：DetectorID 、DetectorVersionID 、ModelType 、 ModelID

指標	描述
ModelInvocationLatency	從 Amazon Fraud Detector 檢視時，Amazon Fraud Detector Model 回應所花費的時間間隔。此間隔僅包含模型調用。 有效維度：DetectorID 、DetectorVersionID 、ModelType 、 ModelID 單位：毫秒

使用 記錄 Amazon Fraud Detector API 呼叫 AWS CloudTrail

Amazon Fraud Detector 已與 服務整合 AWS CloudTrail，此服務可提供由 Amazon Fraud Detector AWS 中的使用者、角色或服務所採取之動作的記錄。CloudTrail 會將 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，以及來自程式碼對 Amazon Fraud Detector APIs呼叫。

如果您建立追蹤，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Amazon Fraud Detector 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。您可以使用 CloudTrail 所收集的資訊，判斷向 Amazon Fraud Detector 提出的請求、提出請求的 IP 地址、提出請求的人員、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「AWS CloudTrail 使用者指南」。

CloudTrail 中的 Amazon Fraud Detector 資訊

當您建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。當 Amazon Fraud Detector 中發生活動時，該活動會與事件歷史記錄中的其他服務 AWS 事件一起記錄在 CloudTrail 事件中。您可以在 AWS 帳戶中檢視、搜尋和下載最近的事件。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html。

若要持續記錄您 AWS 帳戶中的事件，包括 Amazon Fraud Detector 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀

- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 從多個區域接收 CloudTrail 日誌檔案，以及從多個帳戶接收 CloudTrail 日誌檔案

Amazon Fraud Detector 支援將每個動作 (API 操作） 記錄為 CloudTrail 日誌檔案中的事件。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 userIdentity 元素。

了解 Amazon Fraud Detector 日誌檔項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件代表任何來源提出的單一請求，並包含所請求之操作的相關資訊、操作的日期和時間、請求參數等等。CloudTrail 日誌檔案並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的 CloudTrail 日誌項目會示範 `GetDetectors` 操作：

```
{
    "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

下列各節可協助您針對使用 Amazon Fraud Detector 時可能遇到的問題進行疑難排解

訓練資料問題疑難排解

使用本節中的資訊來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 - 導致模型訓練繼續，但有些變數可能會在訓練程序中遭到排除。檢查本節中的相關指引，以改善資料集的品質。
- 資訊（資訊）- 不會影響模型訓練，且所有變數都用於訓練。建議您查看本節中的相關指引，以進一步改善資料集和模型效能的品質。

主題

指定資料集中的不穩定詐騙率

問題類型：錯誤

Description

指定資料中的詐騙率隨著時間過於不穩定。請確定您的詐騙和合法事件會隨著時間統一抽樣。

原因

如果資料集中的詐騙和合法事件分佈不均勻，並從不同的時段取得，則會發生此錯誤。Amazon Fraud Detector 模型訓練程序範例，並根據 EVENT_TIMESTAMP 分割資料集。例如，如果您的資料集包含從過去 6 個月提取的詐騙事件，但只包含最後一個月的合法事件，則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中的偏差。

解決方案

請務必提供相同時段的詐騙和合法事件資料，而且詐騙率不會隨著時間而大幅改變。

資料不足

1. 問題類型：錯誤

   Description

   少於 50 個資料列會標記為詐騙事件。確保詐騙和合法事件都超過 50 個的最低計數，並重新訓練模型。

   原因

   如果您的資料集標記為詐騙的事件少於模型訓練所需的事件，則會發生此錯誤。Amazon Fraud Detector 需要至少 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。如有需要，您可以涵蓋較長的期間來確保這一點。
2. 問題類型：錯誤

   Description

   少於 50 個資料列會標記為合法事件。確保欺詐和合法事件都超過 $threshold 的最低計數，並重新訓練模型。

原因

如果您的資料集標記為合法的事件少於模型訓練所需的事件，則會發生此錯誤。Amazon Fraud Detector 需要至少 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。如有需要，您可以涵蓋較長的期間來確保這一點。

3. 問題類型：錯誤

   Description

   與詐騙相關聯的唯一實體數量少於 100。請考慮包含更多詐騙實體的範例，以改善效能。

   原因

   如果您的資料集具有的詐騙事件實體少於模型訓練所需的實體，則會發生此錯誤。Transaction Fraud Insights (TFI) 模型需要至少 100 個具有詐騙事件的實體，以確保詐騙空間的最大涵蓋範圍。如果所有詐騙事件都是由一小群實體執行，則模型可能不會有良好的概括性。

   解決方案

   請確定您的資料集包含至少 100 個具有詐騙事件的實體。如有需要，您可以確保涵蓋更長的時間。

4. 問題類型：錯誤

   Description

   與合法相關聯的唯一實體數量小於 100。考慮包含更多合法實體的範例，以改善效能。

   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，則會發生此錯誤。Transaction Fraud Insights (TFI) 模型需要至少 100 個具有合法事件的實體，以確保詐騙空間的最大涵蓋範圍。如果所有合法事件都由一小群實體執行，則模型可能不會妥善概括。

   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。如有需要，您可以確保涵蓋更長的時間。

5. 問題類型：錯誤

   Description

資料集中少於 100 個資料列。確保總資料集中有超過 100 個資料列，且至少 50 個資料列標記為詐騙。

原因

如果您的資料集包含的記錄少於 100 筆，就會發生此錯誤。Amazon Fraud Detector 需要至少 100 個資料集事件 （ 記錄 ） 的資料，才能進行模型訓練。

解決方案

請確定您的資料集中有來自超過 100 個事件的資料。

缺少或不同的 EVENT_LABEL 值

1. 問題類型：錯誤

   Description

   大於 1% 的 EVENT_LABEL 資料欄是 null 或值，而不是模型組態 中定義的值**$label_values**。請確定您的 EVENT_LABEL 資料欄中缺少的值少於 1%，且這些值是在模型組態 中定義的值**$label_values**。

   原因

   由於下列其中一個原因，發生此錯誤：

   - 包含訓練資料的 CSV 檔案中，有超過 1% 的記錄在 EVENT_LABEL 資料欄中缺少值。
   - 包含訓練資料的 CSV 檔案中超過 1% 的記錄，其 EVENT_LABEL 資料欄中的值與事件類型相關聯的值不同。

   線上詐騙洞見 (OFI) 模型要求每個記錄中的 EVENT_LABEL 資料欄填入與您的事件類型相關聯的其中一個標籤 （ 或在 中映射`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，或從資料集捨棄這些記錄。如果此錯誤是因為某些記錄的標籤不在 之間**label_values**，請務必將 EVENT_LABEL 欄中的所有值新增至事件類型的標籤，並在模型建立中映射到欺詐或合法 （ 欺詐、合法 ）。

2. 問題類型：資訊

Description

您的 EVENT_LABEL 資料欄包含 Null 值或標籤值，但模型組態 中定義的值除外**`$label_values`**。這些不一致的值在訓練之前已轉換為「非詐騙」。

原因

由於下列其中一個原因，您會收到此資訊：

- 包含訓練資料的 CSV 檔案中，少於 1% 的記錄在 EVENT_LABEL 欄中缺少值
- 包含訓練資料的 CSV 檔案中少於 1% 的記錄，其 EVENT_LABEL 資料欄中的值與事件類型相關聯的值不同。

這兩種情況下的模型訓練都會成功。不過，這些具有遺失或未映射標籤值的事件的標籤值會轉換為合法。如果您認為這是問題，請遵循以下提供的解決方案。

解決方案

如果您的資料集中缺少 EVENT_LABEL 值，請考慮從資料集捨棄這些記錄。如果為這些 EVENT_LABELS 提供的值未映射，請確保所有這些值都映射到每個事件的欺詐或合法（欺詐、合法）。

缺少或不正確的 EVENT_TIMESTAMP 值

1. 問題類型：錯誤

   Description

   您的訓練資料集包含 EVENT_TIMESTAMP，其時間戳記不符合可接受的格式。確保格式是其中一個可接受的日期/時間戳記格式。

   原因

   如果 EVENT_TIMESTAMP 資料欄包含的值不符合 Amazon Fraud Detector 支援的時間戳記格式，則會發生此錯誤。

   解決方案

確保為 EVENT_TIMESTAMP 資料欄提供的值符合支援的時間戳記格式。如果您在 EVENT_TIMESTAMP 欄中缺少值，您可以使用支援的時間戳記格式來回填這些值，或者考慮完全捨棄事件，而不是輸入字串，例如 none、 null或 missing。

2. 問題類型：錯誤

   您的訓練資料集包含缺少值的 EVENT_TIMESTAMP。請確定您沒有遺漏的值。

   原因

   如果資料集中的 EVENT_TIMESTAMP 資料欄缺少值，就會發生此錯誤。Amazon Fraud Detector 要求資料集中的 EVENT_TIMESTAMP 資料欄具有值。

   解決方案

   請確定資料集中的 EVENT_TIMESTAMP 資料欄具有值，且這些值符合支援的時間戳記格式。如果您在 EVENT_TIMESTAMP 欄中缺少值，您可以使用支援的時間戳記格式來回填這些值，或者考慮完全捨棄事件，而不是輸入字串，例如 none、 null或 missing。

資料未擷取

問題類型：錯誤

Description

找不到用於訓練的擷取事件，請檢查您的訓練組態。

原因

如果您使用 Amazon Fraud Detector 存放的事件資料建立模型，但在開始訓練模型之前未將資料集匯入 Amazon Fraud Detector，則會發生此錯誤。

解決方案

使用 Amazon Fraud Detector 主控台中的 SendEvent API 操作、CreateBatchImportJobAPI 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集。

> **Note**
>
> 建議您在完成匯入資料後等待 10 分鐘，再使用資料來訓練模型。

您可以使用 Amazon Fraud Detector 主控台來檢查已為每個事件類型存放的事件數量。如需詳細資訊，請參閱檢視預存事件的指標。

變數不足

問題類型：錯誤

Description

資料集必須至少包含 2 個適合訓練的變數。

原因

如果您的資料集包含少於 2 個適合模型訓練的變數，則會發生此錯誤。只有在 Amazon Fraud Detector 通過所有驗證時，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，您會在模型訓練診斷中看到訊息。

解決方案

確保您的資料集至少有兩個填入值並傳遞所有資料驗證的變數。請注意，您已提供資料欄標頭的事件中繼資料資料列 (EVENT_TIMESTAMP、EVENT_ID、ENTITY_ID、EVENT_LABEL 等） 不會視為變數。

變數類型遺失或不正確

問題類型：警告

Description

的預期資料類型**$variable_name**為 NUMERIC。在資料集**$variable_name**中檢閱和更新，並重新訓練模型。

原因

如果變數定義為 NUMERIC 變數，但資料集中有無法轉換為 NUMERIC 的值，則會收到此警告。因此，該變數會排除在模型訓練中。

解決方案

如果您想要將其保留為 NUMERIC 變數，請確定您提供的值可以轉換為浮點數。請注意，如果變數包含遺失的值，請不要將字串填入其中，例如 `none`、 `null`或 `missing`。如果變數包含非數值，請將其重新建立為 CATEGORICAL 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**$variable_name**缺少大於 **$threshold**的值。請考慮在資料集**$variable_name**中修改並重新訓練，以改善效能。

原因

如果指定的變數因遺失值太多而捨棄，您會收到此警告。Amazon Fraud Detector 允許遺失變數的值。不過，如果一個變數缺少太多值，則對模型的貢獻不大，而且該變數在模型訓練中會遭到捨棄。

解決方案

首先，確認這些遺失值不是由於資料收集和準備錯誤所致。如果它們是錯誤，您可以考慮將其從模型訓練中刪除。不過，如果您確信這些遺失值很有價值，但仍希望保留該變數，則可以在模型訓練和即時推論中以常數手動填入遺失值。

唯一的變數值不足

問題類型：警告

Description

的唯一值計數**$variable_name**低於 100。在資料集**$variable_name**中檢閱和更新，並重新訓練模型。

原因

如果指定變數的唯一值數目小於 100，您會收到此警告。閾值會根據變數類型而有所不同。使用極少的唯一值，可能會有資料集不夠一般的風險，無法涵蓋該變數的特徵空間。因此，模型在即時預測上可能不會有良好的概括性。

解決方案

首先，請確定變數分佈代表實際的商業流量。然後，您可以採用更多經過精細訓練且基數較高的變數，例如使用 `full_customer_name`而非 `first_name`和 `last_name` 分別使用 ，或將變數類型變更為 CATEGORICAL，以允許基數較低。

變數表達式不正確

1. 問題類型：資訊

   Description

   大於 50% **$email_variable_name**的值不符合預期的規則表達式 http://emailregex.com。請考慮在資料集**$email_variable_name**中修改並重新訓練，以改善效能。

   原因

   如果資料集中超過 50% 的記錄具有不符合一般電子郵件表達式的電子郵件值，因此驗證失敗，則會顯示此資訊。

   解決方案

   格式化電子郵件變數值以符合規則表達式。如果缺少電子郵件值，建議您將它們保留空白，而不是用 none、 null或 等字串填入missing。

2. 問題類型：資訊

   Description

   大於 50% **$IP_variable_name**的值不符合 IPv4 或 IPv6 地址 https：//https://digitalfortress.tech/tricks/top-15-commonly-used-regex/ 的規則表達式。請考慮在資料集**$IP_variable_name**中修改並重新訓練，以改善效能。

   原因

   如果資料集中超過 50% 的記錄的 IP 值不符合一般 IP 表達式，因此驗證失敗，則會顯示此資訊。

   解決方案

   格式化 IP 值以符合規則表達式。如果有遺失的 IP 值，建議您將它們保留空白，而不是以 none、null或 等字串填入missing。

3. 問題類型：資訊

   Description

   大於 50% **$phone_variable_name**的值不符合基本電話規則表達式 /$pattern/。請考慮在資料集**$phone_variable_name**中修改並重新訓練，以改善效能 。

原因

如果資料集中有 50% 以上的記錄的電話號碼不符合一般電話號碼表達式，因此驗證失敗，則會顯示此資訊。

解決方案

格式化電話號碼以符合規則表達式。如果缺少電話號碼，建議您將電話號碼保留空白，而不是用 none、 null或 等字串填入missing。

唯一實體不足

問題類型：資訊

Description

唯一實體的數量小於 1500。考慮包含更多資料來改善效能。

原因

如果您的資料集具有比建議數量更小的唯一實體數量，則會顯示此資訊。Transaction Fraud Insights (TFI) 模型同時使用時間序列彙總和一般交易功能，以提供最佳效能。如果您的資料集具有太少的唯一實體，則 IP_ADDRESS、EMAIL_ADDRESS 等大部分一般資料可能沒有唯一的值。然後，此資料集也有無法涵蓋該變數特徵空間的普遍風險。因此，模型可能無法很好地將來自新實體的交易進行一般化。

解決方案

包含更多實體。如有需要，請延長訓練資料時間範圍。

配額

您的 AWS 帳戶 具有每個 Amazon Web Service 的預設配額，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。您可以針對下表中提到的所有可調整配額請求增加配額。如需詳細資訊，請參閱請求提高配額

下表依元件概述 Amazon Fraud Detector 配額。

Amazon Fraud Detector 模型

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
每個模型的版本	200	否
每個帳戶的部署模型版本	5	否
每個帳戶的並行訓練任務	3	否
每個模型的並行訓練任務	1	否

Amazon Fraud Detectors/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
每個偵測器的清單	30	否
每個偵測器的草稿版本	100	否
每個偵測器版本的模型	10	否
每個帳戶的標籤	100	否
每個帳戶的事件類型	100	否
每個帳戶的實體類型	100	否

Amazon Fraud Detector API

配額名稱	預設配額	可調整
每秒 GetEventPrediction API 呼叫數	200 TPS	是
每次 GetEventPrediction API 呼叫的承載大小	256 KB	否
每次 GetEventPrediction API 呼叫的輸入數量	5000	否

文件歷史紀錄

下表說明 Amazon Fraud Detector 使用者指南中的重要變更。我們也經常更新 Amazon Fraud Detector 使用者指南，以處理您傳送給我們的意見回饋。

變更	描述	日期
新的變數和資料類型	Amazon Fraud Detector 推出新的變數類型和資料類型，可用來擷取有用的資訊。	2023 年 6 月 5 日
事件協調	事件協調可讓您使用 Amazon EventBridge 輕鬆將事件傳送至 AWS 服務 以進行下游處理。	2023 年 5 月 30 日
清單	清單資源可讓您參考一組值，例如 IP 地址或電子郵件地址，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
Data Models Explorer	Data Models Explorer 提供 Amazon Fraud Detector 建立詐騙偵測模型所需的資料元素的洞見。在準備事件資料集之前，請使用資料模型瀏覽器。	2022 年 12 月 15 日
帳戶接管洞見模型	使用帳戶接管洞察 (ATI) 模型，偵測透過惡意接管、網路釣魚或遭竊登入資料而洩露的帳戶。	2022 年 7 月 21 日
章節更新	使用有關 Amazon Fraud Detector 的其他資訊更新簡介章節	2022 年 4 月 11 日
變數擴充功能	啟用您提供的部分原始資料擴充功能，以提升使用這些資料	2022 年 2 月 8 日

	元素且已在 2022 年 2 月 8 日之前訓練之模型的效能。	
選擇退出政策	使用選擇退出政策來選擇不讓事件資料用於開發或改善 Amazon Fraud Detector 的品質。	2022 年 1 月 6 日
預防混淆代理人	建立政策，以防止第三方或跨服務實體操縱具有許可的實體，以代表其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引，準備和收集資料以訓練模型。	2021 年 11 月 22 日
預測說明	使用預測說明來深入了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
故障診斷	使用訓練資料問題疑難排解中的資訊，以協助診斷和解決您在訓練模型時在 Amazon Fraud Detector 主控台中可能看到的問題。	2021 年 10 月 11 日
交易詐騙洞見模型	使用交易詐騙洞見 (TFI) 模型來偵測線上或card-not-present交易詐騙。	2021 年 10 月 11 日

儲存的事件	將事件資料存放在 Amazon Fraud Detector 中，並使用儲存的資料來訓練模型。透過將事件資料儲存在 Amazon Fraud Detector 中，您可以訓練使用自動運算變數來改善效能、簡化模型重新訓練，以及更新詐騙標籤以關閉機器學習意見回饋迴圈的模型。	2021 年 10 月 11 日
模型變數重要性	使用模型變數重要性來深入了解驅動模型效能提升或降低的原因，以及哪些模型變數貢獻最大。然後調整您的模型以改善整體效能。	2021 年 7 月 9 日
與 AWS CloudFormation整合	使用 AWS CloudFormation 管理您的 Amazon Fraud Detector 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之事件的預測。	2021 年 3 月 31 日
章節重做	重做入門和其他章節	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。