aws

Guida per l'utente

Amazon Fraud Detector

Version latest

Amazon Fraud Detector: Guida per l'utente

Table of Contents

Cos'è Amazon Fraud Detector?

Amazon Fraud Detector è un servizio di rilevamento delle frodi completamente gestito che automatizza il rilevamento di attività potenzialmente fraudolente online. Queste attività includono transazioni non autorizzate e la creazione di account falsi. Amazon Fraud Detector funziona utilizzando l'apprendimento automatico per analizzare i dati. Lo fa in un modo che si basa sull'esperienza consolidata di oltre 20 anni di rilevamento delle frodi in Amazon.

Puoi utilizzare Amazon Fraud Detector per creare modelli di rilevamento delle frodi personalizzati, aggiungere logica decisionale per interpretare le valutazioni delle frodi del modello e assegnare risultati come passare o inviare per revisione a ogni possibile valutazione delle frodi. Con Amazon Fraud Detector, non hai bisogno di competenze di machine learning per rilevare attività fraudolente.

Per iniziare, raccogli e prepara i dati sulle frodi raccolti presso la tua organizzazione. Amazon Fraud Detector utilizza quindi questi dati per addestrare, testare e implementare un modello di rilevamento delle frodi personalizzato per tuo conto. Come parte di questo processo, Amazon Fraud Detector utilizza modelli di apprendimento automatico che hanno appreso i modelli di frode e l'esperienza di AWS Amazon in materia di frode per valutare i dati sulle frodi e generare punteggi e dati sulle prestazioni dei modelli. Puoi configurare la logica decisionale per interpretare il punteggio del modello e assegnare i risultati su come gestire ogni valutazione delle frodi.

Vantaggi

Amazon Fraud Detector offre i seguenti vantaggi. Questi vantaggi consentono di individuare rapidamente le frodi senza dover investire il tempo e le risorse tradizionalmente necessari per creare e mantenere un sistema di gestione delle frodi.

Creazione automatizzata di modelli antifrode

I modelli di rilevamento delle frodi di Amazon Fraud Detector sono modelli di machine learning completamente automatizzati e personalizzati per soddisfare le tue esigenze aziendali specifiche. Puoi utilizzare i modelli di Amazon Fraud Detector per identificare potenziali frodi in qualsiasi transazione online, come la creazione di nuovi account, i pagamenti online e il checkout con gli ospiti.

Poiché i modelli di frode vengono creati tramite un processo automatizzato, puoi rinunciare a molti dei passaggi associati alla creazione e alla formazione di un modello. Questi passaggi includono la convalida e l'arricchimento dei dati, l'ingegneria delle funzionalità, la selezione degli algoritmi, l'ottimizzazione degli iperparametri e l'implementazione del modello.

Per creare un modello di rilevamento delle frodi utilizzando Amazon Fraud Detector, devi solo caricare il set di dati storici sulle frodi della tua azienda e selezionare il tipo di modello. Quindi, Amazon Fraud Detector trova automaticamente l'algoritmo di rilevamento delle frodi più adatto al tuo caso d'uso e crea il modello. Non è necessario conoscere la programmazione o avere esperienza nell'apprendimento automatico per creare modelli di rilevamento delle frodi.

Modelli di frode che si evolvono e apprendono

I modelli di rilevamento delle frodi devono evolversi costantemente per stare al passo con il mutevole panorama delle frodi. Amazon Fraud Detector esegue questa operazione automaticamente calcolando informazioni tra cui l'età dell'account, il tempo trascorso dall'ultima attività e il conteggio delle attività. Il risultato è che il tuo modello impara la differenza tra i clienti fidati che effettuano spesso transazioni e i continui tentativi tipici dei truffatori. Questo aiuta a mantenere le prestazioni del modello più a lungo tra una sessione di riqualificazione e l'altra.

Visualizzazione delle prestazioni del modello antifrode

Dopo che il modello è stato addestrato utilizzando i dati forniti, Amazon Fraud Detector convalida le prestazioni del modello. Fornisce inoltre strumenti visivi per valutare le prestazioni. Per ogni modello addestrato, puoi visualizzare il punteggio delle prestazioni del modello, il grafico di distribuzione dei punteggi, la matrice di confusione, la tabella delle soglie e tutti gli input che hai fornito, classificati in base al loro impatto sulle prestazioni del modello. Utilizzando questi strumenti prestazionali, puoi scoprire le prestazioni del tuo modello e quali input influiscono sulle prestazioni del modello. Se necessario, puoi modificare il modello per migliorarne le prestazioni complessive.

Previsione delle frodi

Amazon Fraud Detector genera previsioni di frode per le attività aziendali della tua organizzazione. La previsione delle frodi è una valutazione del rischio di frode di un'attività aziendale. Amazon Fraud Detector genera previsioni utilizzando la logica di previsione con i dati associati all'attività. Hai fornito questi dati quando hai creato il tuo modello di rilevamento delle frodi. Puoi ottenere previsioni di frode per una singola attività in tempo reale o ottenere previsioni di frode offline per una serie di attività.

Visualizzazione della spiegazione della previsione delle frodi

Amazon Fraud Detector genera spiegazioni di previsione come parte del processo di previsione delle frodi. Le spiegazioni delle previsioni forniscono informazioni su come ogni elemento di dati utilizzato per addestrare il modello ha influito sul punteggio di previsione delle frodi del modello. Le spiegazioni delle previsioni vengono fornite utilizzando strumenti visivi come tabelle e grafici. Puoi utilizzare

questi strumenti per identificare visivamente l'influenza di ciascun elemento di dati sui punteggi di previsione. Quindi, puoi utilizzare queste informazioni per analizzare i modelli di frode nel tuo set di dati e rilevare eventuali pregiudizi. Infine, puoi utilizzare le spiegazioni delle previsioni anche per identificare i principali indicatori di rischio durante un processo manuale di indagine sulle frodi. Questo ti aiuta a restringere le cause profonde che portano a previsioni false positive.

Azioni basate su regole

Dopo aver addestrato il modello di rilevamento delle frodi, puoi aggiungere regole per intraprendere azioni sui dati valutati, ad esempio accettare i dati, inviarli per la revisione o raccogliere altri dati. Una regola è una condizione che indica ad Amazon Fraud Detector come interpretare i dati durante la previsione delle frodi. Ad esempio, puoi creare una regola che segnali gli account dei clienti sospetti da esaminare. Puoi impostare questa regola in modo che venga attivata se sia il punteggio del modello rilevato è superiore alla soglia predeterminata sia se il codice di autorizzazione al pagamento dell'account (AUTH_CODE) non è valido.

Termini e concetti fondamentali

Di seguito è riportato un elenco di concetti e termini fondamentali utilizzati in Amazon Fraud Detector:

Evento

Un evento è l'attività aziendale della tua organizzazione che viene valutata per il rischio di frode. Amazon Fraud Detector genera previsioni di frode per gli eventi.

Etichetta

Un'etichetta classifica un singolo evento come fraudolento o legittimo. Le etichette vengono utilizzate per addestrare modelli di apprendimento automatico in Amazon Fraud Detector.

Entità

Un'entità rappresenta chi esegue l'evento. Fornisci l'ID dell'entità come parte dei dati sulle frodi della tua azienda per indicare l'entità specifica che ha eseguito l'evento.

Tipo di evento

Un tipo di evento definisce la struttura di un evento inviato ad Amazon Fraud Detector. Ciò include i dati inviati come parte dell'evento, l'entità che esegue l'evento (ad esempio un cliente) e le etichette che classificano l'evento. I tipi di eventi di esempio includono le transazioni di pagamento online, le registrazioni di account e l'autenticazione.

Tipo di entità

Un tipo di entità classifica l'entità. Le classificazioni di esempio includono cliente, commerciante o account.

Set di dati di eventi

Il set di dati degli eventi è costituito dai dati storici della vostra azienda relativi a una specifica attività commerciale o a un evento. Ad esempio, l'evento della vostra azienda potrebbe essere la registrazione di un account online. I dati di un singolo evento (registrazione) potrebbero includere l'indirizzo IP, l'indirizzo e-mail, l'indirizzo di fatturazione e il timestamp dell'evento associati. Fornisci un set di dati sugli eventi ad Amazon Fraud Detector per creare e addestrare modelli di rilevamento delle frodi.

Modello

Un modello è un risultato di algoritmi di apprendimento automatico. Questi algoritmi sono implementati nel codice ed eseguiti sui dati degli eventi forniti dall'utente.

Tipo di modello

Il tipo di modello definisce gli algoritmi, gli arricchimenti e le trasformazioni delle funzionalità utilizzati durante l'addestramento del modello. Definisce inoltre i requisiti in materia di dati per addestrare il modello. Queste definizioni servono a ottimizzare il modello per un tipo specifico di frode. È necessario specificare il tipo di modello da utilizzare quando si crea il modello.

Training del modello

L'addestramento del modello è il processo di utilizzo di un set di dati di eventi fornito per creare un modello in grado di prevedere eventi fraudolenti. Tutte le fasi del processo di formazione dei modelli sono completamente automatizzate. Questi passaggi includono la convalida dei dati, la trasformazione dei dati, l'ingegneria delle funzionalità, la selezione degli algoritmi e l'ottimizzazione del modello.

Punteggio del modello

Il punteggio del modello è il risultato della valutazione dei dati storici sulle frodi della tua azienda. Durante il processo di formazione del modello, Amazon Fraud Detector valuta il set di dati per le attività fraudolente e genera un punteggio compreso tra 0 e 1000. Per questo punteggio, 0 rappresenta un basso rischio di frode mentre 1000 rappresenta il rischio di frode più elevato. Il punteggio stesso è direttamente correlato al tasso di falsi positivi (FPR).

Versione del modello

Una versione del modello è il risultato dell'addestramento di un modello.

Distribuzione di modelli

L'implementazione del modello è un processo per attivare una versione del modello e renderla disponibile per generare previsioni di frode.

Endpoint SageMaker modello Amazon

Oltre a creare modelli utilizzando Amazon Fraud Detector, puoi opzionalmente utilizzare endpoint del modello SageMaker ospitati nelle valutazioni di Amazon Fraud Detector.

Per ulteriori informazioni sulla creazione di un modello in SageMaker, consulta Train a Model with. Amazon SageMaker

Rilevatore

Un rilevatore contiene la logica di rilevamento, ad esempio il modello e le regole per un particolare evento che si desidera valutare per individuare eventuali frodi. Si crea un rilevatore utilizzando una versione del modello.

Versione del rilevatore

Un rilevatore può avere più versioni, ognuna delle quali ha lo stato di `DraftActive`, o. `Inactive` `Active`Lo stato può essere impostato su una sola versione del rilevatore alla volta.

Variabile

Una variabile rappresenta un elemento di dati associato a un evento che si desidera utilizzare per la previsione delle frodi. Le variabili possono essere inviate con un evento come parte di una previsione di frode o derivate, come l'output di un modello Amazon Fraud Detector o. Amazon SageMaker

Regola

Una regola è una condizione che indica ad Amazon Fraud Detector come interpretare i valori delle variabili durante una previsione di frode. Una regola è composta da una o più variabili, un'espressione logica e uno o più risultati. Le variabili utilizzate nella regola devono far parte del set di dati degli eventi valutato dal rilevatore. Inoltre, a ogni rilevatore deve essere associata almeno una regola.

Outcome

Questo è il risultato, o il risultato, di una previsione di frode. Ogni regola utilizzata in una previsione delle frodi deve specificare uno o più risultati.

Previsione delle frodi

La previsione delle frodi è una valutazione delle frodi per un singolo evento o per una serie di eventi. Amazon Fraud Detector genera previsioni di frode per un singolo evento online in tempo reale fornendo in modo sincrono un punteggio modello e un risultato basati sulle regole. Amazon Fraud Detector genera previsioni di frode per una serie di eventi offline. Puoi utilizzare le previsioni per eseguire operazioni offline proof-of-concept o per valutare retrospettivamente il rischio di frode su base oraria, giornaliera o settimanale.

Spiegazione della previsione delle frodi

Le spiegazioni sulla previsione delle frodi forniscono informazioni sull'impatto di ciascuna variabile sul punteggio di previsione delle frodi del modello. Fornisce informazioni su come ciascuna variabile influenzi i punteggi di rischio in termini di entità (da 0 a 5, dove 5 indica il valore più alto) e direzione (determinando un aumento o una diminuzione del punteggio).

Come funziona Amazon Fraud Detector

Amazon Fraud Detector crea un modello di apprendimento automatico personalizzato per rilevare potenziali attività fraudolente online nella tua azienda. Per iniziare, fornisci il tuo case d'uso aziendale. A seconda del tuo caso d'uso aziendale, Amazon Fraud Detector consiglia un tipo di modello che utilizzerà per creare un modello di rilevamento delle frodi per te. Inoltre, fornisce anche informazioni sugli elementi di dati che devi fornire come parte dei dati storici della tua azienda. Amazon Fraud Detector utilizza il set di dati storici per creare e addestrare automaticamente un modello personalizzato per te.

Il processo di formazione automatizzata dei modelli prevede la scelta di un algoritmo di apprendimento automatico in grado di rilevare le frodi per uno specifico caso d'uso aziendale, la convalida dei dati forniti e l'esecuzione di manipolazioni dei dati per migliorare le prestazioni del modello. Dopo aver addestrato il modello, Amazon Fraud Detector genera punteggi del modello e altre metriche prestazionali del modello. Puoi utilizzare il punteggio e le metriche delle prestazioni per valutare le prestazioni del modello. Se necessario, puoi aggiungere o rimuovere elementi di dati dal set di dati fornito per la formazione e riqualificare il modello per migliorare il punteggio del modello.

Dopo aver creato, addestrato e attivato il modello, è necessario configurare la logica decisionale, nota anche come regole, che indichi al modello come interpretare i dati generati dall'azienda e assegnare i risultati per gestire l'interpretazione di ciascuna attività. I risultati possono rappresentare azioni come l'approvazione o la revisione dell'attività oppure possono rappresentare livelli di rischio dell'attività come rischio alto, rischio medio e rischio basso.

Un rilevatore è un contenitore che contiene il modello e le regole associate. Dovrete creare, testare e installare il rilevatore nel vostro ambiente di produzione.

Il rilevatore installato nell'ambiente di produzione fornisce la funzionalità di rilevamento delle frodi alle applicazioni aziendali. Per eseguire la valutazione delle frodi, il modello confronta tutti i dati in entrata dall'attività aziendale con i dati storici dell'azienda e utilizza i sofisticati algoritmi di apprendimento automatico con le regole create per analizzare i risultati e assegnare i risultati. Con Amazon Fraud Detector, puoi valutare i dati di una singola attività aziendale in tempo reale o valutare i dati di più attività aziendali offline.

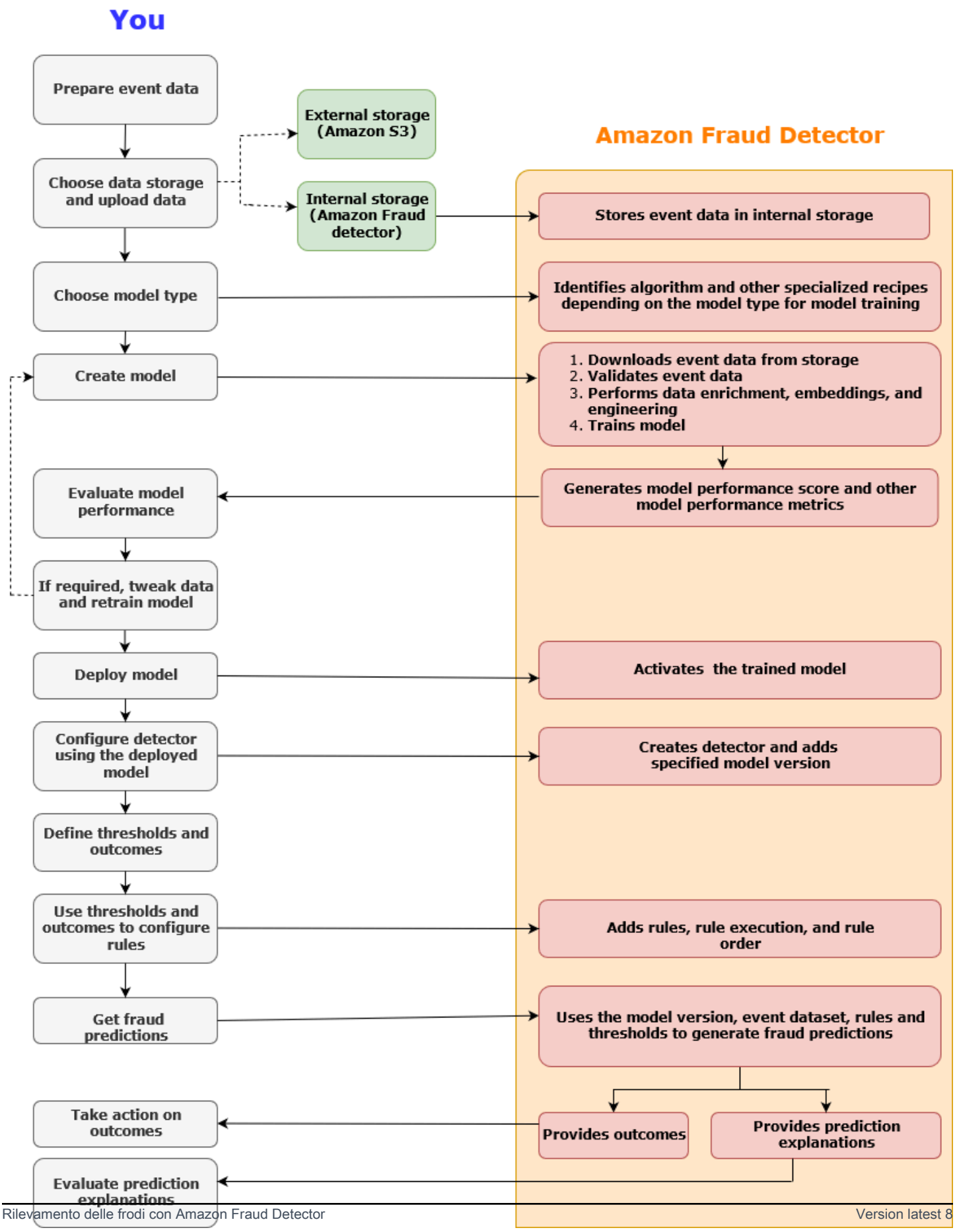
Supponiamo che tu abbia un'azienda che prevede il trasferimento di fondi online tra le sue attività. Vuoi utilizzare Amazon Fraud Detector per rilevare richieste fraudolente di trasferimento di fondi, in tempo reale. Per iniziare, devi prima fornire ad Amazon Fraud Detector i dati delle precedenti richieste di trasferimento di fondi. Amazon Fraud Detector utilizza questi dati per creare e addestrare un modello personalizzato per rilevare richieste fraudolente di trasferimenti di fondi. Quindi, crei un rilevatore aggiungendo il modello e configurando le regole per l'interpretazione dei dati da parte del modello. Un esempio di regola per l'attività di trasferimento di fondi online può essere se la richiesta di trasferimento di fondi proviene daxyz@example.comindirizzo email, invia la richiesta di revisione. Nell'ambiente di produzione aziendale, quando arriva una richiesta di trasferimento di fondi, il modello analizza i dati forniti con la richiesta e utilizza la regola per assegnare il risultato. È quindi possibile intraprendere un'azione sulla richiesta in base al risultato assegnato.

Amazon Fraud Detector utilizza componenti quali set di dati di formazione, modello, rilevatore, regole e risultati per fornire alla tua azienda una logica di valutazione delle frodi.

Per informazioni sul flusso di lavoro che utilizzerai per rilevare le frodi con Amazon Fraud Detector, consultaRilevamento delle frodi con Amazon Fraud Detector

Rilevamento delle frodi con Amazon Fraud Detector

Questa sezione descrive un flusso di lavoro tipico per rilevare le frodi con Amazon Fraud Detector. Inoltre, riassume come è possibile eseguire queste attività. Il diagramma seguente fornisce una visione di alto livello del flusso di lavoro per rilevare le frodi con Amazon Fraud Detector.


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

L'individuazione delle frodi è un processo continuo. Dopo aver implementato il modello, assicurati di valutarne i punteggi e le metriche delle prestazioni in base alle spiegazioni delle previsioni. In questo modo, puoi identificare i principali indicatori di rischio, restringere le cause alla base dei falsi positivi e analizzare i modelli di frode nell'intero set di dati e rilevare eventuali pregiudizi. Per aumentare la precisione delle previsioni, puoi modificare il set di dati per includere dati nuovi o rivisti. Quindi, puoi riqualificare il tuo modello con il set di dati aggiornato. Man mano che diventano disponibili più dati, continui a riqualificare il modello per aumentare la precisione.

Accesso ad Amazon Fraud Detector

Amazon Fraud Detector è disponibile in più versioni Regioni AWS ed è possibile accedervi tramite AWS interfacce.

Disponibilità

Amazon Fraud Detector è disponibile negli Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Europa (Irlanda), Asia Pacifico (Singapore) e Asia Pacifico (Sydney). Regioni AWS

Interfacce

Puoi creare, addestrare, implementare, testare, eseguire e gestire modelli e rilevatori di frodi utilizzando una delle seguenti interfacce:

AWS Management Console- Amazon Fraud Detector fornisce un'interfaccia utente basata sul Web, la console Amazon Fraud Detector. Se ti sei registrato aAccount AWS, puoi accedere alla console Amazon Fraud Detector. Per ulteriori informazioni, consulta Configurare Amazon Fraud Detector.

AWS Command Line Interface(AWS CLI) - Fornisce un'interfaccia che puoi usare per interagire con un'ampia gamma di dispositiviServizi AWS, tra cui Amazon Fraud Detector, utilizzando i comandi della tua shell a riga di comando. AWS CLIi comandi per Amazon Fraud Detector implementano funzionalità equivalenti a quelle fornite dalla console Amazon Fraud Detector.

AWSSDK: fornisce API specifiche per la lingua e gestisce molti dettagli di connessione, come il calcolo della firma, la gestione dei tentativi di richiesta e la gestione degli errori. Per ulteriori informazioni, vai alla AWS pagina Strumenti per la creazione, scorri verso il basso fino alla sezione SDK e scegli il segno più (+) per espandere la sezione.

AWS CloudFormation- Fornisce modelli che puoi utilizzare per definire le risorse e le proprietà di Amazon Fraud Detector. Per ulteriori informazioni, consulta il riferimento al tipo di risorsa Amazon Fraud Detector nella Guida per l'AWS CloudFormationutente.

Prezzi

Con Amazon Fraud Detector, paghi solo per ciò che usi. Non sono previsti importi minimi o impegni anticipati. I costi vengono addebitati in base alle ore di elaborazione utilizzate per addestrare e ospitare i tuoi modelli, alla quantità di spazio di archiviazione che utilizzi e alla quantità di previsioni di frode che fai. Per ulteriori informazioni, consulta i prezzi di Amazon Fraud Detector.

Configurazione per Amazon Fraud Detector

Per utilizzare Amazon Fraud Detector, devi prima avere un account Amazon Web Services (AWS), quindi devi configurare le autorizzazioni che ti consentano di Account AWS accedere a tutte le interfacce. Successivamente, quando inizi a creare le tue risorse Amazon Fraud Detector, devi concedere le autorizzazioni che consentano ad Amazon Fraud Detector di accedere al tuo account per eseguire attività per tuo conto e accedere alle risorse di tua proprietà.

Completa le seguenti attività in questa sezione per iniziare a usare Amazon Fraud Detector:

- Registrati per AWS.
- Configura le autorizzazioni che ti consentano di accedere Account AWS alle interfacce Amazon Fraud Detector.
- Configura le interfacce che desideri utilizzare per accedere ad Amazon Fraud Detector.

Dopo aver completato questi passaggi, vedi come continuare Inizia a usare Amazon Fraud Detector a usare Amazon Fraud Detector.

Registrati per AWS

Quando ti iscrivi ad Amazon Web Services (AWS), ti iscrivi automaticamente a tutti i servizi su Amazon Web Services () AWS, incluso Amazon Fraud Detector. Account AWS Ti vengono addebitati solo i servizi che utilizzi. Se ne hai già uno Account AWS, passa all'attività successiva.

Registrati per un Account AWS

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

Per iscriverti a un Account AWS

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

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura

consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center
2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Configura le autorizzazioni per accedere alle interfacce Amazon Fraud Detector

Per utilizzare Amazon Fraud Detector, configura le autorizzazioni per accedere alla console Amazon Fraud Detector e alle operazioni API.

Seguendo le best practice di sicurezza, crea un utente AWS Identity and Access Management (IAM) con accesso limitato alle operazioni di Amazon Fraud Detector e con le autorizzazioni richieste. È possibile aggiungere altre autorizzazioni in base alle esigenze.

Le seguenti politiche forniscono l'autorizzazione richiesta per utilizzare Amazon Fraud Detector:

- `AmazonFraudDetectorFullAccessPolicy`

  Consente di eseguire le seguenti operazioni:
  - Accedi a tutte le risorse di Amazon Fraud Detector
  - Elenca e descrivi tutti gli endpoint del modello in SageMaker
  - Elenca tutti i ruoli IAM nell'account
  - Elenca tutti i bucket Amazon S3

  - Consenti a IAM Pass Role di trasferire un ruolo ad Amazon Fraud Detector
- `AmazonS3FullAccess`

  Consente l'accesso completo a. Amazon Simple Storage Service Questo è necessario se devi caricare set di dati di addestramento su Amazon S3.

Di seguito viene descritto come creare un utente IAM e assegnare le autorizzazioni necessarie.

Per creare un utente e assegnare le autorizzazioni richieste

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione seleziona Utenti, quindi Aggiungi utente.
3. In Nome utente, inserisci **`AmazonFraudDetectorUser`**.
4. Seleziona la casella di controllo di accesso alla console di AWS gestione, quindi configura la password dell'utente.
5. (Facoltativo) Per impostazione predefinita, AWS richiede al nuovo utente di creare una nuova password al primo accesso. Puoi deselezionare la casella di controllo accanto a User must create a new password at next sign-in (L'utente deve creare una nuova password al prossimo accesso) per consentire al nuovo utente di reimpostare la propria password dopo aver effettuato l'accesso.
6. Scegli Successivo: Autorizzazioni.
7. Seleziona Crea gruppo.
8. Per il nome del gruppo, inserisci. **`AmazonFraudDetectorGroup`**
9. Nell'elenco delle politiche, seleziona la casella di controllo per AmazonFraudDetectorFullAccessPolicye FullAccessAmazonS3. Seleziona Crea gruppo.
10. Nell'elenco dei gruppi, selezionare la casella di controllo per il tuo nuovo gruppo. Scegli Aggiorna se non vedi il gruppo nell'elenco.
11. Scegli Successivo: Tag.
12. (Facoltativo) Aggiungi metadati all'utente collegando i tag come coppie chiave-valore. Per istruzioni su come utilizzare i tag in IAM, consulta Tagging IAM Users and Roles.
13. Scegli Avanti: revisione per visualizzare i dettagli dell'utente e il riepilogo delle autorizzazioni per il nuovo utente. Quando sei pronto per procedere, scegli Crea utente.

Configura le interfacce per accedere ad Amazon Fraud Detector con

Puoi accedere ad Amazon Fraud Detector utilizzando la console AWS CLI Amazon Fraud Detector o l'SDK. AWS Prima di poterli utilizzare, configura l' AWS CLI SDK and. AWS

Accedi alla console Amazon Fraud Detector

Puoi accedere alla console Amazon Fraud Detector e ad altri AWS servizi tramite. AWS Management Console Il tuo Account AWS, ti garantisce l'accesso a. AWS Management Console

Per accedere alla console Amazon Fraud Detector,

1. Vai a https://console.aws.amazon.com/ e accedi al tuo Account AWS.
2. Accedi ad Amazon Fraud Detector.

Con la console Amazon Fraud Detector, puoi creare e gestire i tuoi modelli e le tue risorse per il rilevamento delle frodi come rilevatori, variabili, eventi, entità, etichette e risultati. Puoi generare previsioni e valutare le prestazioni e le previsioni del tuo modello.

Configurare AWS CLI

Puoi usare AWS Command Line Interface (AWS CLI) per interagire con Amazon Fraud Detector eseguendo comandi nella shell della riga di comando. Con una configurazione minima, puoi utilizzare i comandi AWS CLI per eseguire funzionalità simili a quelle fornite dalla console Amazon Fraud Detector dal prompt dei comandi del tuo terminale.

Per configurare il AWS CLI

Scarica e configura la AWS CLI. Per istruzioni, consulta i seguenti argomenti nella Guida AWS Command Line Interface per l'utente:

- Configurazione con l'interfaccia a AWS riga di comando
- Configurazione dell'interfaccia a riga AWS di comando

Per informazioni sui comandi di Amazon Fraud Detector, consulta Available Commands

Configura SDK AWS

Puoi utilizzare gli AWS SDK per scrivere codice per creare e gestire le tue risorse per il rilevamento delle frodi e per ottenere previsioni sulle frodi. Gli AWS SDK supportano Amazon Fraud Detector in JavaScripte Python (Boto3).

Per configurare AWS SDK for Python (Boto3)

È possibile AWS SDK for Python (Boto3) utilizzarlo per creare, configurare e gestire AWS servizi. Per istruzioni su come installare Boto, consulta AWS SDK for Python (Boto3). Assicurati di utilizzare Boto3 SDK versione 1.14.29 o successiva.

Dopo l'installazione AWS SDK for Python (Boto3), esegui il seguente esempio di Python per confermare che l'ambiente sia configurato correttamente. Se è configurato correttamente, la risposta contiene un elenco di rilevatori. Se non è stato creato alcun rilevatore, l'elenco è vuoto.

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

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

Per configurare gli AWS SDK per Java

Per istruzioni su come installare e caricare il file AWS SDK for JavaScript, consulta Configurazione dell'SDK per. JavaScript

Inizia a usare Amazon Fraud Detector

Prima di iniziare, assicurati di aver lettoRilevamento delle frodi con Amazon Fraud Detector e completato i passaggi successiviConfigurazione per Amazon Fraud Detector.

Utilizza questi tutorial pratici in questa sezione per apprendere le nozioni di base, per approfondire la conoscenza e per implementare un modello di rilevamento delle frodi. In questo tutorial, assumi il ruolo di un analista antifrode che utilizza un modello di apprendimento automatico per prevedere se la registrazione di un nuovo account è fraudolenta. Il modello deve essere addestrato utilizzando i dati delle registrazioni degli account. Amazon Fraud Detector fornisce un set di dati di registrazione dell'account di esempio per questo tutorial. Il set di dati di esempio deve essere caricato prima di iniziare con il tutorial.

Puoi iniziare a usare Amazon Fraud Detector utilizzando una delle interfacce seguenti. Prima di iniziare il tutorial, assicurati di seguire le istruzioni perOttieni e carica un set di dati di esempio

- Tutorial: inizia a usare la console Amazon Fraud Detector
- Tutorial: Inizia subito a utilizzareAWS SDK for Python (Boto3)

Ottieni e carica un set di dati di esempio

Il set di dati di esempio utilizzato in questo tutorial fornisce i dettagli delle registrazioni degli account online. Il set di dati è in un file di testo che utilizza valori separati da virgole (CSV) nel formato UTF-8. La prima riga del file del set di dati CSV contiene le intestazioni. La riga di intestazione è seguita da più righe di dati. Ognuna di queste righe è composta da elementi di dati provenienti da una singola registrazione dell'account. I dati sono etichettati per comodità dell'utente. Una colonna nel set di dati indica se la registrazione dell'account è fraudolenta.

Per ottenere e caricare un set di dati di esempio

1. Vai a Esempi.

   Esistono due file di dati con dati di registrazione dell'account online: registration_data_20K_minimum.csv e registration_data_20K_full.csv. Il file`registration_data_20K_minimum` contiene solo due variabili: ip_address e email_address. Il file`registration_data_20K_full` contiene altre variabili. Queste variabili sono per ogni evento e includono billing_address, phone_number e user_agent. Entrambi i file di dati contengono anche due campi obbligatori:

- EVENT_TIMESTAMP — Definisce quando si è verificato l'evento
- EVENT_LABEL — Classificare l'evento come fraudolento o legittimo

Puoi usare uno dei due file per questo tutorial. Scarica il file di dati che desideri utilizzare.

2. Crea un bucketAmazon Simple Storage Service (Amazon S3).

   In questo passaggio, si crea una memoria esterna per archiviare il set di dati. Questo storage esterno è un bucket Amazon S3. Per maggiori informazioni su Amazon S3, consulta Cos'è Amazon S3?

   a. Accedi alla AWS Management Console e apri la console di Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
   b. In Bucks, scegli Crea bucket.
   c. Per Nome bucket, specifica un nome per bucket. Assicurati di seguire le regole di denominazione dei bucket nella console e di fornire un nome univoco globale. Ti consigliamo di utilizzare un nome che descriva lo scopo del bucket.
   d. Perché Regione AWS, scegli laRegione AWS in cui creare il tuo bucket. La regione scelta deve supportare Amazon Fraud Detector. Per ridurre la latenza, scegliRegione AWS quella più vicina alla tua posizione geografica. Per un elenco delle regioni che supportano Amazon Fraud Detector, consulta la tabella delle regioni nella Guida globale all'infrastruttura.
   e. Lascia le impostazioni predefinite per Object Ownership, Bucket Settings per Block Public Access, Bucket Versioning e Tag per questo tutorial.
   f. Per la crittografia predefinita, scegli Disabilita per questo tutorial.
   g. Controlla la configurazione del bucket, quindi scegli Crea bucket.

3. Caricare un file di esempio sul bucket Amazon S3

   Ora che hai un bucket, carica uno dei file di esempio che hai scaricato in precedenza nel bucket Amazon S3 che hai appena creato.

   a. Nei Bucket, viene elencato il nome del bucket. Scegli il bucket.
   b. Scegliere Upload (Carica).
   c. In File e cartelle, scegli Aggiungi file.
   d. Scegli uno dei file di dati di esempio che hai scaricato sul tuo computer, quindi scegli Apri.
   e. Lasciare le impostazioni predefinite per Destinazione, Autorizzazioni e Proprietà.

f. Rivedi le configurazioni, quindi scegli Carica.

g. Il file di esempio viene caricato sul bucket Amazon S3. Prendi nota della posizione del bucket. In Oggetti, scegli il file di dati di esempio che hai appena caricato.

h. Nella panoramica degli oggetti, copia la posizione nell'URI S3. Questa è la posizione Amazon S3 del file di dati di esempio. Lo usi in seguito. Puoi anche copiare l'Amazon Resource Name (ARN) del tuo bucket S3 e salvarlo.

Tutorial: inizia a usare la console Amazon Fraud Detector

Questo tutorial è composto da due parti. La prima parte descrive come creare, addestrare e implementare un modello di rilevamento delle frodi. La seconda parte spiega come utilizzare il modello per generare previsioni di frode in tempo reale. Il modello viene addestrato utilizzando il file di dati di esempio caricato in un bucket S3. Alla fine di questo tutorial, l'utente completa le seguenti azioni:

- Crea e addestra un modello Amazon Fraud Detector
- Genera previsioni di frode in tempo

> **Important**
>
> Prima di procedere, assicurati di aver seguito le istruzioni perOttieni e carica un set di dati di esempio

Parte A: Crea, addestra e distribuisci un modello Amazon Fraud Detector

Nella parte A, si definisce il caso d'uso aziendale, si definisce l'evento, si crea un modello, si addestra il modello, si valutano le prestazioni del modello e si implementa il modello.

Fase 1: Scelta del caso d'uso aziendale

- In questo passaggio, utilizzi il Data Models Explorer per abbinare il tuo caso d'uso aziendale ai tipi di modelli di rilevamento delle frodi supportati da Amazon Fraud Detector. Data models explorer è uno strumento integrato con la console Amazon Fraud Detector che consiglia un tipo di modello da utilizzare per creare e addestrare un modello di rilevamento delle frodi adatto al caso d'uso aziendale. Data models explorer fornisce anche informazioni sugli elementi di

dati obbligatori, consigliati e opzionali che dovrai includere nel tuo set di dati. Il set di dati verrà utilizzato per creare e addestrare il tuo modello di rilevamento delle frodi.

Ai fini di questo tutorial, il tuo caso d'uso aziendale è la registrazione di nuovi account. Dopo aver specificato il caso d'uso aziendale, Data Models Explorer consiglierà un tipo di modello per creare un modello di rilevamento delle frodi e fornirà anche un elenco di elementi di dati necessari per creare il set di dati. Poiché hai già caricato un set di dati di esempio contenente i dati delle registrazioni di nuovi account, non è necessario creare un nuovo set di dati.

a. Apri la console diAWS gestione e accedi al tuo account. Passa ad Amazon Fraud Detector.

b. Nel pannello di navigazione a sinistra, seleziona Data models explorer.

c. Nella pagina Esplora modelli di dati, in Caso d'uso aziendale, seleziona Nuovo account fraudolento.

d. Amazon Fraud Detector mostra il tipo di modello consigliato da utilizzare per creare un modello di rilevamento delle frodi per il caso d'uso aziendale selezionato. Il tipo di modello definisce gli algoritmi, gli arricchimenti e le trasformazioni che Amazon Fraud Detector utilizzerà per addestrare il tuo modello di rilevamento delle frodi.

   Prendi nota del tipo di modello consigliato. Ne avrai bisogno in seguito quando creerai il tuo modello.

e. Il riquadro Informazioni sul modello di dati fornisce informazioni sugli elementi di dati obbligatori e consigliati necessari per creare e addestrare un modello di rilevamento delle frodi.

   Dai un'occhiata al set di dati di esempio che hai scaricato e assicurati che contenga tutti gli elementi di dati obbligatori e alcuni consigliati elencati nella tabella.

   Successivamente, quando creerai un modello per il tuo caso d'uso aziendale specifico, utilizzerai le informazioni fornite per creare il tuo set di dati.

Fase 2: creazione di un tipo di evento

- In questa fase, definisci l'attività commerciale (evento) da valutare per eventuali frodi. La definizione dell'evento implica l'impostazione delle variabili che si trovano nel set di dati, l'entità che avvia l'evento e le etichette che classificano l'evento. Per questo tutorial, definisci l'evento di registrazione dell'account.

  a. Apri la console diAWS gestione e accedi al tuo account. Passa ad Amazon Fraud Detector.

b. Nel pannello di navigazione a sinistra, seleziona Eventi.

c. Nella pagina Tipo di eventi, scegli Crea.

d. In Dettagli del tipo di evento, inserisci`sample_registration` come nome del tipo di evento e, facoltativamente, inserisci una descrizione dell'evento.

e. Per Entità, scegli Crea entità.

f. Nella pagina Crea entità, inserisci`sample_customer` come nome del tipo di entità. Facoltativamente, inserisci una descrizione del tipo di entità.

g. Scegliere Create entity (Crea entità).

h. In Variabili di evento, in Scegli come definire le variabili di questo evento, scegli Seleziona variabili da un set di dati di addestramento.

i. Per il ruolo IAM, scegli Crea ruolo IAM.

j. Nella pagina Crea ruolo IAM, inserisci il nome del bucket S3 in cui hai caricato i dati di esempio e scegli Crea ruolo.

k. In Posizione dati, inserisci il percorso dei dati di esempio. Questo è il`S3 URI` percorso che hai salvato dopo aver caricato i dati di esempio. Il percorso è simile a questo:`S3://`*`your-bucket-name`*`/`*`example dataset filename`*`.csv`.

l. Scegliere Upload (Carica).

   Amazon Fraud Detector estrae le intestazioni dal file di dati di esempio e le mappa con un tipo di variabile. La mappatura viene visualizzata nella console.

m. In Etichette - opzionale, per Etichette, scegli Crea nuove etichette.

n. Nella pagina Crea etichetta, inserisci`fraud` come nome. Questa etichetta corrisponde al valore che rappresenta la registrazione fraudolenta dell'account nel set di dati di esempio.

o. Scegli Crea etichetta.

p. Crea una seconda etichetta, quindi inserisci`legit` come nome. Questa etichetta corrisponde al valore che rappresenta la registrazione legittima dell'account nel set di dati di esempio.

q. Scegli Crea tipo di evento.

Fase 3: Creazione del modello

1. Nella pagina Modelli, scegli Aggiungi modello, quindi scegli Crea modello.

2. Per la Fase 1 — Definizione dei dettagli del modello, immettetela`sample_fraud_detection_model` come nome del modello. Facoltativamente puoi aggiungere una descrizione del modello.
3. Per Tipo di modello, scegli il modello Online Fraud Insights.
4. Per Tipo di evento, scegli sample_registration. Questo è il tipo di evento creato nella fase 1.
5. In Dati storici degli eventi,
   a. In Origine dati evento, scegli Dati evento archiviati in S3.
   b. Per il ruolo IAM, seleziona il ruolo creato nella fase 1.
   c. In Posizione dei dati di allenamento, inserisci il percorso URI S3 del file di dati di esempio.
6. Seleziona Successivo.

Fase 4: modello di treno

1. Negli input del modello, lascia tutte le caselle di controllo selezionate. Per impostazione predefinita, Amazon Fraud Detector utilizza tutte le variabili del set di dati degli eventi storici come input del modello.
2. Nella classificazione delle etichette, per le etichette antifrode, scegli frode poiché questa etichetta corrisponde al valore che rappresenta gli eventi fraudolenti nel set di dati di esempio. Per le etichette legittime, scegli legit poiché questa etichetta corrisponde al valore che rappresenta gli eventi legittimi nel set di dati di esempio.
3. Per il trattamento degli eventi senza etichetta, mantieni la selezione predefinita Ignora gli eventi senza etichetta per questo set di dati di esempio.
4. Seleziona Successivo.
5. Dopo la revisione, scegli Crea e addestra il modello. Amazon Fraud Detector crea un modello e inizia a addestrare una nuova versione del modello.

   Nelle versioni del modello, la colonna Stato indica lo stato dell'addestramento del modello. L'addestramento del modello che utilizza il set di dati di esempio richiede circa 45 minuti per essere completato. Lo stato cambia in Pronto per l'implementazione al termine dell'addestramento del modello.

Fase 5: Esaminare le prestazioni del modello

Un passaggio importante nell'utilizzo di Amazon Fraud Detector consiste nel valutare l'accuratezza del modello utilizzando i punteggi del modello e le metriche delle prestazioni. Al termine della formazione sul modello, Amazon Fraud Detector convalida le prestazioni del modello utilizzando il 15% dei dati che non sono stati utilizzati per addestrare il modello e genera un punteggio delle prestazioni del modello e altre metriche delle prestazioni.

1. Per visualizzare le prestazioni del modello,

   a. Nel pannello di navigazione a sinistra della console Amazon Fraud Detector, seleziona Modelli.

   b. Nella pagina Modelli, scegli il modello che hai appena addestrato (sample_fraud_detection_model), quindi scegli 1.0. Questa è la versione creata da Amazon Fraud Detector del tuo modello.

2. Guarda il punteggio complessivo delle prestazioni del modello e tutte le altre metriche generate da Amazon Fraud Detector per questo modello.

   Per ulteriori informazioni sul punteggio delle prestazioni del modello e sulle metriche delle prestazioni in questa pagina, consultaPunteggi del modello eMetriche delle prestazioni del modello.

   Puoi aspettarti che tutti i tuoi modelli addestrati di Amazon Fraud Detector abbiano metriche delle prestazioni di rilevamento delle frodi nel mondo reale simili alle metriche delle prestazioni che vedi per il modello in questo tutorial.

Fase 6: Distribuzione del modello

Dopo aver esaminato le metriche delle prestazioni del modello addestrato e essere pronto a utilizzarlo per generare previsioni di frode, puoi implementare il modello.

1. Nel pannello di navigazione a sinistra della console Amazon Fraud Detector, seleziona Modelli.
2. Nella pagina Modelli, scegli sample_fraud_detection_model, quindi scegli la versione specifica del modello che desideri distribuire. Per questo tutorial, scegli 1.0.
3. Nella pagina Versione del modello, scegli Azioni, quindi scegli Distribuisci versione del modello.
4. Nelle versioni del modello, lo stato mostra lo stato della distribuzione. Lo stato cambia in Attivo al termine della distribuzione. Ciò indica che la versione del modello è attivata e disponibile per

generare previsioni di frode. ContinuaParte B: Generazione di previsioni sulle frodi a completare i passaggi per generare previsioni sulle frodi.

Parte B: Generazione di previsioni sulle frodi

La previsione delle frodi è una valutazione delle frodi per un'attività aziendale (evento). Amazon Fraud Detector utilizza i rilevatori per generare previsioni di frode. Un rilevatore contiene una logica di rilevamento, ad esempio modelli e regole, per un evento specifico che si desidera valutare per frode. La logica di rilevamento utilizza regole per indicare ad Amazon Fraud Detector come interpretare i dati associati al modello. In questo tutorial, valuti l'evento di registrazione dell'account utilizzando il set di dati di esempio di registrazione dell'account che hai caricato in precedenza.

Nella Parte A, hai creato, addestrato e distribuito il tuo modello. Nella parte B, si crea un rilevatore per il tipo di`sample_registration` evento, si aggiunge il modello distribuito, si creano regole e un ordine di esecuzione delle regole, quindi si crea e si attiva una versione del rilevatore da utilizzare per generare previsioni di frode.

Fase 1: costruzione del rivelatore

Per creare un rivelatore

1. Nel pannello di navigazione a sinistra della console Amazon Fraud Detector, seleziona Detettori.
2. Scegli Crea rilevatore.
3. Nella pagina Definisci i dettagli del rilevatore, inserisci`sample_detector` il nome del rilevatore. Facoltativamente, inserisci una descrizione del rivelatore, ad esempio`my sample fraud detector`.
4. Per Tipo di evento, seleziona sample_registration. Questo è l'evento che hai creato nella parte A di questo tutorial.
5. Seleziona Successivo.

Fase 2: aggiunta del modello

Se hai completato la parte A di questo tutorial, probabilmente hai già un modello Amazon Fraud Detector che puoi aggiungere al tuo rilevatore. Se non hai già creato un modello, vai alla Parte A e completa i passaggi per creare, addestrare e distribuire un modello, quindi continua con la Parte B.

1. In Aggiungi modello - opzionale, scegli Aggiungi modello.

2. Nella pagina Aggiungi modello, per Seleziona modello, scegli il nome del modello Amazon Fraud Detector che hai distribuito in precedenza. Per Seleziona la versione, scegli la versione del modello distribuito.
3. Scegliere Add model (Aggiungi modello).
4. Seleziona Successivo.

Fase 3: aggiunta di regole

Una regola è una condizione che indica ad Amazon Fraud Detector come interpretare il punteggio di performance del modello nella valutazione della previsione di frode. Per questo tutorial, crei tre regole:`high_fraud_risk`,`medium_fraud_risk`, `elow_fraud_risk`.

1. Nella pagina Aggiungi regole, in Definisci una regola, inserisci`high_fraud_risk` il nome della regola e in Descrizione - opzionale, inserisci**`This rule captures events with a high ML model score`** come descrizione della regola.
2. In Espressione, inserisci la seguente espressione di regola utilizzando il linguaggio semplificato delle espressioni delle regole di Amazon Fraud Detector:

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```
3. In Risultati, scegli Crea un nuovo risultato. Un risultato è il risultato di una previsione fraudolenta e viene restituito se la regola corrisponde durante una valutazione.
4. In Crea un nuovo risultato, inserisci`verify_customer` come nome del risultato. Facoltativamente, inserisci una descrizione.
5. Scegli Salva risultato.
6. Scegli Aggiungi regola per eseguire il controllo di convalida delle regole e salvare la regola. Dopo la creazione, Amazon Fraud Detector rende la regola disponibile per l'uso nel rilevatore.
7. Scegli Aggiungi un'altra regola, quindi scegli la scheda Crea regola.
8. Ripeti questa procedura altre due volte per creare le tue`low_fraud_risk` regole`medium_fraud_risk` e utilizzando i seguenti dettagli:

   - rischio di frode medio

     Nome della regola:`medium_fraud_risk`

     Esito:`review`

     Espressione:

```
$sample_fraud_detection_model_insightscore <= 900 and

$sample_fraud_detection_model_insightscore > 700
```

- basso rischio di frode

  Nome della regola:`low_fraud_risk`

  Esito:`approve`

  Espressione:

```
$sample_fraud_detection_model_insightscore <= 700
```

Questi valori sono esempi usati per questo tutorial. Quando crei regole per il tuo rilevatore, usa valori appropriati per il tuo modello e il tuo caso d'uso,

9. Dopo aver creato tutte e tre le regole, scegli Avanti.

   Per ulteriori informazioni sulla creazione e la scrittura di regole, consultaRegolamento eRiferimento linguistico delle regole.

Fase 4: configurazione dell'esecuzione e dell'ordine delle regole

La modalità di esecuzione delle regole incluse nel rilevatore determina se tutte le regole definite vengono valutate o se la valutazione delle regole si ferma alla prima regola corrispondente. E l'ordine delle regole determina l'ordine in cui desideri che la regola venga eseguita.

La modalità di esecuzione delle regole predefinita è`FIRST_MATCHED`.

Primo abbinamento

La modalità di esecuzione della prima regola corrispondente restituisce i risultati per la prima regola corrispondente in base all'ordine delle regole definito. Se si specifica `FIRST_MATCHED`, Amazon Fraud Detector valuta le regole in sequenza, dalla prima all'ultima, fermandosi alla prima regola corrispondente. Amazon Fraud Detector fornisce quindi i risultati per quella singola regola.

L'ordine in cui vengono eseguite le regole può influire sull'esito della previsione delle frodi risultante. Dopo aver creato le regole, riordina le regole per eseguirle nell'ordine desiderato seguendo questi passaggi:

Se la tuahigh_fraud_risk regola non è già in cima all'elenco delle regole, scegli Ordina, quindi scegli 1. Si passahigh_fraud_risk alla prima posizione.

Ripeti questa procedura in modo che la tuamedium_fraud_risk regola sia nella seconda posizione e la tualow_fraud_risk regola sia nella terza posizione.

Tutti abbinati

La modalità di esecuzione di tutte le regole corrispondenti restituisce i risultati per tutte le regole corrispondenti, indipendentemente dall'ordine delle regole. Se l'utente specificaALL_MATCHED, Amazon Fraud Detector valuta tutte le regole e restituisce i risultati per tutte le regole corrispondenti.

SelezionaFIRST_MATCHED questo tutorial, quindi scegli Avanti.

Fase 5: Revisione e creazione della versione del rivelatore

Una versione detector definisce i modelli e le regole specifici utilizzati per generare previsioni di frode.

1. Nella pagina Rivedi e crea, esamina i dettagli, i modelli e le regole del rilevatore che hai configurato. Se devi apportare modifiche, scegli Modifica accanto alla sezione corrispondente.
2. Scegli Crea rilevatore. Dopo la creazione, la prima versione del rilevatore viene visualizzata nella tabella Versioni del rilevatore conDraft lo stato.

   Utilizzi la versione Draft per testare il tuo Detector.

Fase 6: test e attivazione della versione del rivelatore

Nella console Amazon Fraud Detector, puoi testare la logica del tuo rilevatore utilizzando dati fittizi con la funzione Esegui test. Per questo tutorial, puoi utilizzare i dati di registrazione dell'account dal set di dati di esempio.

1. Scorri fino a Esegui test nella parte inferiore della pagina dei dettagli della versione del rilevatore.
2. Per i metadati dell'evento, inserisci un timestamp di quando si è verificato l'evento e inserisci un identificatore univoco per l'entità che esegue l'evento. Per questo tutorial, seleziona una data dal selettore di date per il timestamp e inserisci «1234» per l'ID dell'entità.
3. In Variabile evento, inserisci i valori della variabile che desideri testare. Per questo tutorial, sono necessari solo ie`email_address` campi`ip_address` e. Questo perché sono gli input utilizzati

per addestrare il tuo modello Amazon Fraud Detector. Puoi utilizzare i seguenti valori di esempio. Ciò presuppone che tu abbia usato i nomi delle variabili suggeriti:

- indirizzo_ip:`205.251.233.178`
- indirizzo_email:`johndoe@exampledomain.com`

4. Scegli Esegui test.
5. Amazon Fraud Detector restituisce l'esito della previsione delle frodi in base alla modalità di esecuzione delle regole. Se la modalità di esecuzione della regola è`FIRST_MATCHED`, il risultato restituito corrisponde alla prima regola corrispondente. La prima regola è quella con la massima priorità. È corrispondente se viene valutato come vero. Se la modalità di esecuzione delle regole è`ALL_MATCHED`, il risultato restituito corrisponde a tutte le regole corrispondenti. Ciò significa che sono tutte valutate come vere. Amazon Fraud Detector restituisce anche il punteggio del modello per tutti i modelli aggiunti al rilevatore.

   Puoi modificare gli input ed eseguire un paio di test per vedere risultati diversi. Puoi utilizzare i valori ip_address ed email_address del tuo set di dati di esempio per i test e verificare se i risultati sono quelli previsti.
6. Quando sei soddisfatto del funzionamento del rilevatore, promuovilo da`Draft` a`Active`. In questo modo il rilevatore è disponibile per l'uso nel rilevamento delle frodi in tempo reale.

   Nella pagina dei dettagli della versione del rilevatore, scegli Azioni, Pubblica, Versione pubblica. Questo modifica lo stato del rilevatore da Bozza a Attivo.

   A questo punto, il tuo modello e la logica di rilevamento associata sono pronti per valutare le attività online alla ricerca di frodi in tempo reale utilizzando l'`GetEventPrediction`API Amazon Fraud Detector. Puoi anche valutare gli eventi offline utilizzando un file di input CSV e l'`CreateBatchPredictionJob`API. Per ulteriori informazioni sulla previsione delle frodi, consultaPrevisioni di frode

Completando questo tutorial, l'utente ha eseguito le seguenti operazioni:

- Ha caricato un set di dati di esempio in Amazon S3.
- Ha creato e addestrato un modello di rilevamento delle frodi Amazon Fraud Detector utilizzando il set di dati di esempio.
- Ho visualizzato il punteggio delle prestazioni del modello e altre metriche di performance generate da Amazon Fraud Detector.

- Implementato il modello di rilevamento delle frodi.
- Ha creato un rilevatore e aggiunto il modello distribuito.
- Sono state aggiunte le regole, l'ordine di esecuzione delle regole e i risultati al rilevatore.
- Ho testato il rilevatore fornendo diversi input e controllando se le regole e l'ordine di esecuzione delle regole funzionavano come previsto.
- Hai attivato il rilevatore pubblicandolo.

Tutorial: Inizia subito a utilizzareAWS SDK for Python (Boto3)

Questo tutorial descrive come creare e addestrare un modello Amazon Fraud Detector e quindi utilizzare questo modello per generare previsioni di frode in tempo reale utilizzando ilAWS SDK for Python (Boto3). Il modello viene addestrato utilizzando il file di dati di esempio di registrazione dell'account che carichi nel bucket Amazon S3.

Alla fine di questo tutorial, si eseguono le seguenti azioni:

- Crea e addestra un modello Amazon Fraud Detector
- Genera previsioni di frode in tempo reale

Prerequisiti

Di seguito sono riportati i passaggi necessari per questo tutorial.

- CompletatoConfigurazione per Amazon Fraud Detector.

  Se lo hai già fattoConfigura SDK AWS, assicurati di utilizzare Boto3 SDK versione 1.14.29 o successiva.
- Ho seguito le istruzioni per l'Ottieni e carica un set di dati di esempioarchiviazione necessarie per questo tutorial.

Nozioni di base

Fase 1: Imposta e verifica il tuo ambiente Python

Boto è l'SDK di Amazon Web Services (AWS) per Python. Puoi usarlo per creare, configurare e gestireServizi AWS. Per istruzioni su come installare Boto3, consulta SDK AWS per Python (Boto3).

Dopo l'installazioneAWS SDK for Python (Boto3), esegui il seguente comando di esempio in Python per confermare che l'ambiente sia configurato correttamente. Se l'ambiente è configurato correttamente, la risposta contiene un elenco di rilevatori. Se non sono stati creati rilevatori, l'elenco è vuoto.

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

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

Fase 2: Creare variabili, tipo di entità ed etichette

In questo passaggio, si creano risorse che vengono utilizzate per definire modelli, eventi e regole.

Creazione di una variabile

Una variabile è un elemento di dati del set di dati che si desidera utilizzare per creare il tipo di evento, il modello e le regole.

Nell'esempio seguente, l'CreateVariableAPI viene utilizzata per creare due variabili. Le variabili sonoemail_address eip_address. Assegnali ai tipi di variabili corrispondenti:EMAIL_ADDRESS eIP_ADDRESS. Queste variabili fanno parte del set di dati di esempio che hai caricato. Quando specifichi il tipo di variabile, Amazon Fraud Detector interpreta la variabile durante l'addestramento del modello e quando ottiene le previsioni. Solo le variabili con un tipo di variabile associato possono essere utilizzate per l'addestramento del modello.

```
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>'
)
```

Crea tipo di entità

Un'entità rappresenta chi esegue l'evento e un tipo di entità classifica l'entità. Le classificazioni di esempio includono cliente, commerciante o account.

Nell'esempio seguente, l'PutEntityTypeAPI viene utilizzata per creare un tipo di`sample_customer` entità.

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

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

Crea etichetta

Un'etichetta classifica un evento come fraudolento o legittimo e viene utilizzata per addestrare il modello di rilevamento delle frodi. Il modello impara a classificare gli eventi utilizzando questi valori di etichetta.

Nell'esempio seguente, l'API Putlabel viene utilizzata per creare due etichette`fraud` `elegit`.

```
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'
)
```

Fase 3: Creazione di un tipo di evento

Con Amazon Fraud Detector, puoi creare modelli che valutano i rischi e generano previsioni di frode per singoli eventi. Un tipo di evento definisce la struttura di un singolo evento.

Nell'esempio seguente, l'PutEventTypeAPI viene utilizzata per creare un tipo di eventosample_registration. È possibile definire il tipo di evento specificando le variabili (email_address,ip_address), il tipo di entità (sample_customer) e le etichette (fraud,legit) create nel passaggio precedente.

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

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

Fase 4: creazione, addestramento e distribuzione del modello

Amazon Fraud Detector addestra i modelli per imparare a rilevare le frodi per un tipo di evento specifico. Nel passaggio precedente, hai creato il tipo di evento. In questo passaggio, si crea e si addestra un modello per il tipo di evento. Il modello funge da contenitore per le versioni del modello. Ogni volta che si addestra un modello, viene creata una nuova versione.

Utilizza i seguenti codici di esempio per creare e addestrare un modello Online Fraud Insights. Questo modello si chiamasample_fraud_detection_model. È per il tipo di evento chesample_registration utilizza il set di dati di esempio di registrazione dell'account che hai caricato su Amazon S3.

Per ulteriori informazioni sui diversi tipi di modelli supportati da Amazon Fraud Detector, consultaScegliete un tipo di modello.

Crea un modello

Nell'esempio seguente, l'CreateModelAPI viene utilizzata per creare un modello.

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

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

Addestra un modello

Nell'esempio seguente, l'CreateModelVersionAPI viene utilizzata per addestrare il modello. Specifica `'EXTERNAL_EVENTS'` la posizione`trainingDataSource` e la posizione Amazon S3 in cui hai archiviato il set di dati RoleArndi esempio e il bucket Amazon S3 per cui`externalEventsDetail`. Come`trainingDataSchema` parametro, specifica come Amazon Fraud Detector interpreta i dati di esempio. Più specificamente, specifica quali variabili includere e come classificare le etichette degli eventi.

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

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

```
}
)
```

Puoi addestrare il tuo modello più volte. Ogni volta che si addestra un modello, viene creata una nuova versione. Al termine dell'addestramento del modello, lo stato della versione del modello viene aggiornato a`TRAINING_COMPLETE`. Puoi esaminare il punteggio delle prestazioni del modello e altre metriche delle prestazioni del modello.

Esamina le prestazioni del modello

Un passaggio importante nell'utilizzo di Amazon Fraud Detector consiste nel valutare l'accuratezza del modello utilizzando i punteggi del modello e le metriche delle prestazioni. Una volta completata la formazione sul modello, Amazon Fraud Detector convalida le prestazioni del modello utilizzando il 15% dei dati che non sono stati utilizzati per addestrare il modello. Genera un punteggio delle prestazioni del modello e altre metriche delle prestazioni.

Utilizza l'DescribeModelVersionsAPI per esaminare le prestazioni del modello. Guarda il punteggio complessivo delle prestazioni del modello e tutte le altre metriche generate da Amazon Fraud Detector per questo modello.

Per ulteriori informazioni sul punteggio delle prestazioni del modello e sulle metriche delle prestazioni, consultaPunteggi del modello eMetriche delle prestazioni del modello.

Puoi aspettarti che tutti i tuoi modelli addestrati di Amazon Fraud Detector dispongano di metriche delle prestazioni di rilevamento delle frodi nel mondo reale, simili alle metriche di questo tutorial.

Implementa un modello

Dopo aver esaminato le metriche delle prestazioni del modello addestrato, implementa il modello e mettilo a disposizione di Amazon Fraud Detector per generare previsioni di frode. Per implementare il modello addestrato, utilizza l'UpdateModelVersionStatusAPI. Nell'esempio seguente, viene utilizzato per aggiornare lo stato della versione del modello su ATTIVO.

```
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'
)
```

Passaggio 5: creazione del rilevatore, dei risultati, delle regole e della versione del rilevatore

Un rilevatore contiene la logica di rilevamento, come i modelli e le regole. Questa logica si riferisce a un particolare evento che desideri valutare per frode. Una regola è una condizione che si specifica per indicare ad Amazon Fraud Detector come interpretare i valori delle variabili durante la previsione. E il risultato è il risultato di una previsione di frode. Un rilevatore può avere più versioni, ciascuna delle quali ha lo stato DRAFT, ACTIVE o INACTIVE. Una versione del rilevatore deve possedere almeno una regola associata ad essa.

Utilizza i seguenti codici di esempio per creare il rilevatore, le regole, il risultato e per pubblicare il rilevatore.

Creazione di un rilevatore

Nell'esempio seguente, l'PutDetectorAPI viene utilizzata per creare un`sample_detector` rilevatore per il tipo di`sample_registration` evento.

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

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

Crea risultati

I risultati vengono creati per ogni possibile risultato di previsione delle frodi. Nell'esempio seguente, l'PutOutcomeAPI viene utilizzata per creare tre risultati:`verify_customer`,`review`, e`approve`. Questi risultati vengono successivamente assegnati alle regole.

```
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'
)
```

Crea regole

La regola è composta da una o più variabili del set di dati, un'espressione logica e uno o più risultati.

Nell'esempio seguente, l'CreateRuleAPI viene utilizzata per creare tre regole diverse:`high_risk`medium_risk, `elow_risk`. Crea espressioni di regole per confrontare il`sample_fraud_detection_model_insightscore` valore del punteggio delle prestazioni del modello con varie soglie. Questo serve a determinare il livello di rischio di un evento e assegnare il risultato definito nella fase precedente.

```
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']
     )
```

Creazione di una versione del rilevatore

Una versione detector definisce il modello e le regole che vengono utilizzati per ottenere la previsione delle frodi.

Nell'esempio seguente, l'CreateDetectorVersionAPI viene utilizzata per creare una versione del rilevatore. A tale scopo fornisce dettagli sulla versione del modello, regole e una modalità di esecuzione delle regole FIRST_MATCHED. Una modalità di esecuzione delle regole specifica la sequenza per la valutazione delle regole. La modalità di esecuzione delle regole FIRST_MATCHED specifica che le regole vengono valutate in sequenza, dalla prima all'ultima, fermandosi alla prima regola corrispondente.

```
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'
)
```

Fase 6: Creazione di previsioni di frode

L'ultimo passaggio di questo tutorial utilizza il rilevatore`sample_detector` creato nel passaggio precedente per generare previsioni di frode per tipo di`sample_registration` evento in tempo reale. Il rilevatore valuta i dati di esempio caricati su Amazon S3. La risposta include i punteggi delle prestazioni del modello e tutti i risultati associati alle regole corrispondenti.

Nell'esempio seguente, l'GetEventPredictionAPI viene utilizzata per fornire dati provenienti dalla registrazione di un singolo account con ogni richiesta. Per questo tutorial, prendi i dati (email_address e ip_address) dal file di dati di esempio di registrazione dell'account. Ogni riga (riga) dopo la riga di intestazione superiore rappresenta i dati di un singolo evento di registrazione dell'account.

```
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'
}
)
```

Dopo aver completato questo tutorial, hai eseguito le seguenti operazioni:

- Ha caricato un set di dati di eventi di esempio su Amazon S3.
- Variabili, entità ed etichette create che vengono utilizzate per creare e addestrare un modello.
- Ha creato e addestrato un modello utilizzando il set di dati di esempio.
- Ho visualizzato il punteggio delle prestazioni del modello e altre metriche di performance generate da Amazon Fraud Detector.
- Implementato il modello di rilevamento delle frodi.
- Ha creato un rilevatore e aggiunto il modello distribuito.
- Sono state aggiunte le regole, l'ordine di esecuzione delle regole e i risultati al rilevatore.
- Versione del rilevatore creata.
- Ho testato il rilevatore fornendo diversi input e controllando se le regole e l'ordine di esecuzione delle regole funzionavano come previsto.

(Facoltativo) Esplora le API Amazon Fraud Detector con un notebook Jupyter (IPython)

Per altri esempi su come utilizzare le API Amazon Fraud Detector, consulta aws-fraud-detector-samples GitHub il repository. Gli argomenti trattati nei notebook includono sia la creazione di modelli e rilevatori utilizzando le API di Amazon Fraud Detector sia la creazione di richieste di previsione delle frodi in batch utilizzando l'`GetEventPrediction`API.

Fasi successive

Ora che hai creato un modello e un rilevatore, puoi approfondire e iniziare a creare modelli e rilevatori e generare previsioni di frode.

Le seguenti sezioni della Guida per l'utente di Amazon Fraud Detector descrivono in che modo la tua azienda o organizzazione può utilizzare Amazon Fraud Detector per rilevare le frodi.

- Prepara e crea il set di dati di eventi per addestrare il tuo modello.
- Crea un tipo di evento
- Creazione del modello
- Crea rivelatore
- Ottieni previsioni sulle frodi
- Gestisci le risorse di Amazon Fraud Detector (in particolare variabili, entità, risultati ed etichette)

- Configura Amazon Fraud Detector per soddisfare i tuoigli obiettivi di sicurezza e conformità
- Monitora Amazon Fraud Detector e registra le chiamate API di Amazon Fraud Detector
- Problemi relativi alla risoluzione dei problemi con Amazon Fraud Detector

Set di dati di evento

Un set di dati sugli eventi è costituito dai dati storici relativi alle frodi della tua azienda. Fornisci questi dati ad Amazon Fraud Detector per creare modelli di rilevamento delle frodi.

Amazon Fraud Detector utilizza modelli di apprendimento automatico per generare previsioni di frode. Ogni modello viene addestrato utilizzando un tipo di modello. Il tipo di modello specifica gli algoritmi e le trasformazioni utilizzati per addestrare il modello. La formazione dei modelli è il processo di utilizzo di un set di dati fornito per creare un modello in grado di prevedere eventi fraudolenti. Per ulteriori informazioni, consulta Come funziona Amazon Fraud Detector

Il set di dati utilizzato per creare un modello di rilevamento delle frodi fornisce i dettagli di un evento. Un evento è un'attività aziendale valutata per il rischio di frode. Ad esempio, la registrazione di un account può essere un evento. I dati associati all'evento di registrazione dell'account possono essere set di dati di eventi. Amazon Fraud Detector utilizza questo set di dati per valutare le frodi nella registrazione degli account.

Prima di fornire il set di dati ad Amazon Fraud Detector per la creazione di un modello, assicurati di definire l'obiettivo per la creazione del modello. È inoltre necessario determinare come si desidera utilizzare il modello e definire le metriche per valutare se il modello funziona in base ai requisiti specifici.

Ad esempio, i tuoi obiettivi per la creazione di un modello di rilevamento delle frodi che valuti le frodi nella registrazione degli account possono essere i seguenti:

- Per approvare automaticamente le registrazioni legittime.
- Per acquisire registrazioni fraudolente per indagini successive.

Dopo aver determinato l'obiettivo, il passaggio successivo consiste nel decidere come utilizzare il modello. Alcuni esempi di utilizzo del modello di rilevamento delle frodi per valutare le frodi di registrazione sono i seguenti:

- Per il rilevamento delle frodi in tempo reale per ogni registrazione dell'account.
- Per la valutazione offline di tutte le registrazioni degli account ogni ora.

Alcuni esempi di metriche che possono essere utilizzate per misurare le prestazioni del modello sono i seguenti:

- Ha prestazioni costantemente migliori rispetto all'attuale linea di base in termini di produzione.
- Registra registrazioni fraudolente del X% con una percentuale di falsi positivi dell'Y%.
- Accetta fino al 5% delle registrazioni approvate automaticamente che sono fraudolente.

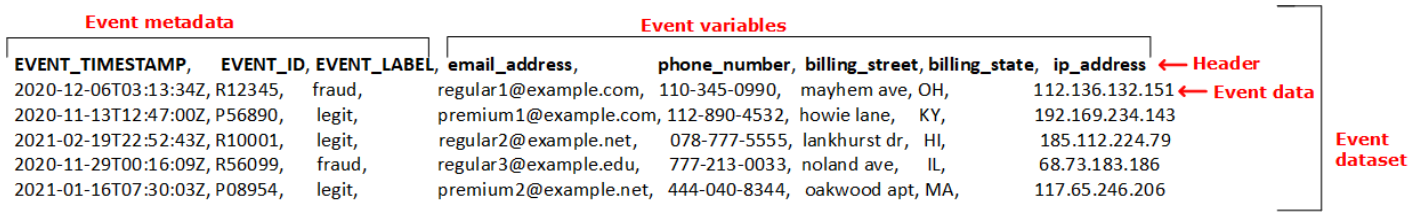
Struttura del set di dati di evento

Amazon Fraud Detector richiede che tu fornisca il set di dati degli eventi in un file di testo utilizzando valori separati da virgole (CSV) nel formato UTF-8. La prima riga del file del set di dati CSV deve contenere le intestazioni dei file. L'intestazione del file è composta da metadati e variabili di evento che descrivono ogni elemento di dati associato all'evento. L'intestazione è seguita dai dati dell'evento. Ogni riga è composta da elementi di dati provenienti da un singolo evento.

- Metadati dell'evento: forniscono informazioni sull'evento. Ad esempio, EVENT_TIMESTAMP è un metadato di evento che specifica l'ora in cui si è verificato l'evento. A seconda del caso d'uso aziendale e del tipo di modello utilizzato per creare e addestrare il modello di rilevamento delle frodi, Amazon Fraud Detector richiede di fornire metadati specifici degli eventi. Quando specifichi i metadati degli eventi nell'intestazione del file CSV, utilizza lo stesso nome dei metadati dell'evento specificato da Amazon Fraud Detector e usa solo lettere maiuscole.
- Variabile evento: rappresenta gli elementi di dati specifici del tuo evento che desideri utilizzare per creare e addestrare il tuo modello di rilevamento delle frodi. A seconda del caso d'uso aziendale e del tipo di modello utilizzato per creare e addestrare un modello di rilevamento delle frodi, Amazon Fraud Detector potrebbe richiedere o consigliare di fornire variabili di evento specifiche. Facoltativamente, puoi anche fornire altre variabili di evento del tuo evento che desideri includere nell'addestramento del modello. Alcuni esempi di variabili di evento per un evento di registrazione online possono essere l'indirizzo e-mail, l'indirizzo IP e il numero di telefono. Quando specifichi il nome della variabile di evento nell'intestazione del file CSV, usa qualsiasi nome di variabile di tua scelta e usa solo lettere minuscole.
- Dati dell'evento: rappresenta i dati raccolti dall'evento effettivo. Nel file CSV, ogni riga che segue l'intestazione del file è composta da elementi di dati provenienti da un singolo evento. Ad esempio, in un file di dati di un evento di registrazione online, ogni riga contiene i dati di una singola registrazione. Ogni elemento di dati nella riga deve corrispondere ai metadati dell'evento o alla variabile evento corrispondenti.

Di seguito viene riportato un esempio di un esempio di un file .V contenente i dati di un evento di registrazione di account. La riga di intestazione contiene sia i metadati degli eventi in maiuscolo

che le variabili degli eventi in lettere minuscole seguite dai dati dell'evento. Ogni riga del set di dati contiene elementi di dati associati alla registrazione di un singolo account e ogni elemento di dati corrisponde all'intestazione.



Ottieni i requisiti dei set di dati di eventi utilizzando Data models explorer

Il tipo di modello scelto per creare il modello definisce i requisiti per il set di dati. Amazon Fraud Detector utilizza il set di dati fornito per creare e addestrare il tuo modello di rilevamento delle frodi. Prima di iniziare a creare il modello, Amazon Fraud Detector verifica se il set di dati soddisfa le dimensioni, il formato e altri requisiti. Se il set di dati non soddisfa i requisiti, la creazione e l'addestramento del modello falliscono. È possibile utilizzare Data Models Explorer per identificare un tipo di modello da utilizzare per il caso d'uso aziendale e per ottenere informazioni sui requisiti del set di dati per il tipo di modello identificato.

Esplora modelli di dati

Data Models Explorer è uno strumento della console Amazon Fraud Detector che allinea il tuo caso d'uso aziendale al tipo di modello supportato da Amazon Fraud Detector. L'esploratore di modelli di dati fornisce anche informazioni sugli elementi di dati richiesti da Amazon Fraud Detector per creare il tuo modello di rilevamento delle frodi. Prima di iniziare a preparare il set di dati degli eventi, utilizza Data Models Explorer per individuare il tipo di modello consigliato da Amazon Fraud Detector per l'uso aziendale e anche per visualizzare un elenco di elementi di dati obbligatori, consigliati e opzionali necessari per creare il set di dati.

Per utilizzare Data Models Explorer,

1. Apri la console diAWS gestione e accedi al tuo account. Vai ad Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra seleziona Data models explorer.
3. Nella pagina Esplora modelli di dati, in Caso d'uso aziendale, seleziona il caso d'uso aziendale che desideri valutare per il rischio di frode.

4. Amazon Fraud Detector mostra il tipo di modello consigliato che corrisponde al caso d'uso aziendale. Il tipo di modello definisce gli algoritmi, gli arricchimenti e le trasformazioni che Amazon Fraud Detector utilizzerà per addestrare il tuo modello di rilevamento delle frodi.

   Prendi nota del tipo di modello consigliato. Ne avrai bisogno in seguito quando creerai il tuo modello.

   > **Note**
   >
   > Se non trovi il tuo caso d'uso aziendale, utilizza il link «raggiungici» nella descrizione per fornirci i dettagli del tuo caso d'uso aziendale. Ti consiglieremo il tipo di modello da utilizzare per creare un modello di rilevamento delle frodi per il tuo caso d'uso aziendale.

5. Il riquadro di analisi dei modelli di dati fornisce informazioni sugli elementi di dati obbligatori, consigliati e opzionali necessari per creare e addestrare un modello di rilevamento delle frodi adatto al tuo caso d'uso aziendale. Utilizza le informazioni nel riquadro degli approfondimenti per raccogliere i dati degli eventi e creare il set di dati.

Raccogli i dati di evento

La raccolta dei dati degli eventi è un passaggio importante nella creazione del modello. Questo perché le prestazioni del modello nella previsione delle frodi dipendono dalla qualità del set di dati. Quando inizi a raccogliere i dati degli eventi, tieni presente l'elenco degli elementi di dati che Data models explorer ti ha fornito per creare il tuo set di dati. Dovrai raccogliere tutti i dati obbligatori (metadati degli eventi) e decidere quali elementi di dati consigliati e facoltativi (variabili di evento) includere in base ai tuoi obiettivi per la creazione del modello. È anche importante decidere il formato di ogni variabile di evento che intendi includere e la dimensione totale del set di dati.

Qualità dei set di dati degli eventi

Per raccogliere set di dati di alta qualità per il modello, è consigliabile:

- Raccogli dati maturi: l'utilizzo dei dati più recenti aiuta a identificare il modello di frode più recente. Tuttavia, per individuare i casi di utilizzo fraudolento, attendi la maturazione dei dati. Il periodo di scadenza dipende dalla tua attività e può richiedere da due settimane a tre mesi. Ad esempio, se l'evento include una transazione con carta di credito, la scadenza dei dati potrebbe essere determinata dal periodo di addebito della carta di credito o dal tempo impiegato da un investigatore per prendere una decisione.

Assicurati che il set di dati utilizzato per addestrare il modello abbia avuto il tempo sufficiente per maturare in base alla tua azienda.

- Assicurati che la distribuzione dei dati non subisca variazioni significative: il processo di formazione del modello Amazon Fraud Detector, campiona e partiziona il tuo set di dati in base a EVENT_TIMESTAMP. Ad esempio, se il set di dati è composto da eventi fraudolenti estratti dagli ultimi 6 mesi, ma sono inclusi solo l'ultimo mese di eventi legittimi, la distribuzione dei dati è considerata errata e instabile. Un set di dati instabile potrebbe portare a distorsioni nella valutazione delle prestazioni del modello. Se ritieni che la distribuzione dei dati stia subendo variazioni significative, valuta la possibilità di bilanciare il set di dati raccogliendo dati simili all'attuale distribuzione dei dati.
- Assicurati che il set di dati sia rappresentativo del caso d'uso in cui il modello è implementato/testato. Altrimenti, le prestazioni stimate potrebbero essere distorte. Supponiamo che tu stia utilizzando un modello per rifiutare automaticamente tutti i candidati interni, ma che il tuo modello sia addestrato con un set di dati storici e etichette precedentemente approvati. Quindi, la valutazione del modello potrebbe essere imprecisa perché la valutazione si basa sul set di dati che non include la rappresentazione dei candidati rifiutati.

Formato dei dati dell'evento

Amazon Fraud Detector trasforma la maggior parte dei tuoi dati nel formato richiesto come parte del processo di formazione dei modelli. Tuttavia, esistono alcuni formati standard che puoi usare facilmente per fornire i tuoi dati che possono aiutarti a evitare problemi in seguito, quando Amazon Fraud Detector convalida il tuo set di dati. La tabella seguente fornisce indicazioni sui formati per fornire i metadati degli eventi consigliati.

> **Note**
>
> Quando crei il tuo file CSV, assicurati di inserire il nome dei metadati dell'evento come elencato di seguito, in lettere maiuscole.

Nome dei metadati	Formato	Obbligatorio
ID_EVENTO	Se fornito, deve soddisfare i seguenti requisiti:	Dipende dal tipo di modello

Nome dei metadati	Formato	Obbligatorio
	• È unico per quell'evento. • Rappresenta informazioni significative per la tua attività. • Segue lo schema delle espressioni regolari (ad esempio, `^[0-9a-z_-]+$`.) • Oltre ai requisiti di cui sopra, ti consigliamo di non aggiungere un timestamp a EVENT_ID. Questa operazione potrebbe causare problemi durante l'aggiornamento dell'evento. Questo perché devi fornire esattamente lo stesso EVENT_ID se lo fai.	

Nome dei metadati	Formato	Obbligatorio
TIMESTAMP DELL'EVENTO	• Deve essere specificato in uno dei seguenti formati: • %YYYy-%mm-%DDt%hH: %mm: %sSz (standard ISO 8601 solo in UTC senza millisecondi) Esempio: 2019-11-30T 13:01:01 Z • %aaaa/%mm/%dd %hh: %mm: %ss (AM/PM) Esempi: 30/11/2019 13:01:01 o 30/11/2019 13:01:01 • %mm/%gd/%aaaa %hh: %mm: %ss Esempi: 30/11/2019 13:01:01, 30/11/2019 13:01:01 • %mm/%dd/%yy %hh: %mm: %ss Esempi: 30/11/19 13:01:01 PM, 30/11/19 13:01:01 • Amazon Fraud Detector fa le seguenti ipotesi quando analizza i formati di data/ora per i timestamp degli eventi: • Se si utilizza lo standard ISO 8601, deve corrispon dere esattamente alla specifica precedente	Sì

Nome dei metadati	Formato	Obbligatorio

	• Se si utilizza uno degli altri formati, è disponibile una flessibilità aggiuntiva:
	  • Per mesi e giorni, puoi fornire cifre singole o doppie. Ad esempio, 1/12/2019 è una data valida.
	  • Non è necessario includere hh:mm:ss se non li avete (cioè, potete semplicem ente fornire una data). Puoi anche fornire un sottoinsieme delle sole ore e minuti (ad esempio, hh:mm). La semplice indicazione dell'ora non è supportat a. Anche i millisecondi non sono supportati.
	  • Se si forniscono etichette AM/PM, si presume un orologio di 12 ore. Se non sono disponibili informazioni AM/PM, si presume che l'orologio sia attivo 24 ore su 24.
	  • È possibile utilizzare «/» o «-» come delimitat ori per gli elementi della data. «:» è assunto	

Nome dei metadati	Formato	Obbligatorio
	per gli elementi del timestamp.	
ENTITY_ID	• Deve seguire lo schema delle espressioni regolari: `^[0-9A-Za-z_.@+-]+$` . • Se l'ID dell'entità non è disponibile al momento della valutazione, specifica l'ID dell'entità come sconosciuto.	Dipende dal tipo di modello
TIPO_ENTITÀ	È possibile utilizzare qualsiasi stringa	Dipende dal tipo di modello
ETICHETTA_EVENTO	Puoi utilizzare qualsiasi etichetta, come «frode», «legittimo», «1" o «0".	Obbligatorio se LABEL_TIMESTAMP è incluso
TIMESTAMP DELL'ETICHETTA	Deve seguire il formato del timestamp.	Obbligatorio se EVENT_LABEL è incluso

Per informazioni sulle variabili di evento, vedere Variabili.

> **Important**
>
> Se stai creando un modello Account Takeover Insights (ATI), consultaPreparazione dei dati i dettagli sulla preparazione e la selezione dei dati.

Valori nulli o mancanti

Le variabili EVENT_TIMESTAMP ed EVENT_LABEL non devono contenere valori nulli o mancanti. Puoi avere valori nulli o mancanti per altre variabili. Consigliamo, tuttavia, di utilizzare solo un numero

piccolo di nulli per tali variabili. Se Amazon Fraud Detector rileva che ci sono troppi valori nulli o mancanti per una variabile di evento, ometterà automaticamente una variabile dal tuo modello.

Variabili minime

Quando si crea il modello, il set di dati deve includere almeno due variabili di evento oltre ai metadati degli eventi richiesti. Le due variabili di evento devono superare il controllo di convalida.

Dimensione del set di dati dell'evento

Obbligatorio

Il set di dati deve soddisfare i seguenti requisiti di base per una corretta formazione del modello.

- Dati relativi ad almeno 100 eventi.
- Il set di dati deve includere almeno 50 eventi (righe) classificati come fraudolenti.

Consigliato

Consigliamo che il set di dati includa quanto segue per un addestramento efficace del modello e buone prestazioni del modello.

- Includi un minimo di tre settimane di dati storici, ma al massimo sei mesi di dati.
- Includi un minimo di 10.000 dati totali sugli eventi.
- Includi almeno 400 eventi (righe) classificati come fraudolenti e 400 eventi (righe) classificati come legittimi.
- Includi più di 100 entità uniche, se il tipo di modello richiede ENTITY_ID.

Convalida del set di dati

Prima che Amazon Fraud Detector inizi a creare il modello, verifica se le variabili incluse nel set di dati per addestrare il modello soddisfano le dimensioni, il formato e altri requisiti. Se il set di dati non supera la convalida, il modello non viene creato. È necessario innanzitutto correggere le variabili che non hanno superato la convalida prima di creare il modello. Amazon Fraud Detector ti offre un Data profiler che puoi utilizzare per aiutarti a identificare e risolvere i problemi con il tuo set di dati prima di iniziare ad addestrare il tuo modello

Profilatore di dati

Amazon Fraud Detector fornisce uno strumento open source per la profilazione e la preparazione dei dati per la formazione dei modelli. Questo profiler di dati automatizzato consente di evitare errori comuni di preparazione dei dati e di identificare potenziali problemi come tipi di variabili mappati in modo errato che potrebbero influire negativamente sulle prestazioni del modello. Il profiler genera un report intuitivo e completo del set di dati, che include statistiche variabili, distribuzione delle etichette, analisi categoriali e numeriche e correlazioni tra variabili ed etichette. Fornisce indicazioni sui tipi di variabili e un'opzione per trasformare il set di dati in un formato richiesto da Amazon Fraud Detector.

Utilizzo del data profiler

Il data profiler automatizzato è costruito con unoAWS CloudFormation stack, che puoi avviare facilmente con pochi clic. Tutti i codici sono disponibili su Github. Per informazioni su come utilizzare il data profiler, segui le indicazioni nel nostro blog Addestra i modelli più velocemente con un data profiler automatico per Amazon Fraud Detector

Errori comuni dei set di dati degli eventi

Di seguito sono riportati alcuni dei problemi più comuni riscontrati da Amazon Fraud Detector durante la convalida di un set di dati di eventi. Dopo aver eseguito il data profiler, utilizza questo elenco per verificare la presenza di errori nel set di dati prima di creare il modello.

- Il file .V. non è nel formato UTF-8.
- Il numero di eventi nel set di dati è inferiore a 100.
- Il numero di eventi identificati come fraudolenti o legittimi è inferiore a 50.
- Il numero di entità uniche associate a un evento di frode è inferiore a 100.
- Più dello 0,1% dei valori in EVENT_TIMESTAMP contiene valori nulli o diversi dai formati data/ora supportati.
- Più dell'1% dei valori in EVENT_LABEL contiene valori nulli o diversi da quelli definiti nel tipo di evento.
- Sono disponibili meno di due variabili per l'addestramento dei modelli.

Memorizzazione di set di dati

Dopo aver raccolto il set di dati, è possibile archiviarlo internamente utilizzando Amazon Fraud Detector o esternamente con Amazon Simple Storage Service (Amazon S3). Ti consigliamo di scegliere dove archiviare il set di dati in base al modello utilizzato per generare previsioni di frode.

Per ulteriori informazioni sui tipi di modello, consulta Scegliere un tipo di modello. Per ulteriori informazioni sulla memorizzazione del set di dati, consultaArchiviazione dati eventi.

Tipo di evento

Con Amazon Fraud Detector puoi generare previsioni di frode per eventi. Un tipo di evento definisce la struttura di un singolo evento inviato ad Amazon Fraud Detector. Una volta definiti, puoi creare modelli e rilevatori che valutano il rischio per tipi di eventi specifici.

La struttura di un evento include quanto segue:

- Tipo di entità: classifica chi esegue l'evento. Durante la previsione, specifica il tipo di entità e l'ID dell'entità per definire chi ha eseguito l'evento.
- Variabili: definisce quali variabili possono essere inviate come parte dell'evento. Le variabili vengono utilizzate da modelli e regole per valutare il rischio di frode. Una volta aggiunte, le variabili non possono essere rimosse da un tipo di evento.
- Etichette: classifica un evento come fraudolento o legittimo. Utilizzato durante l'addestramento dei modelli. Una volta aggiunte, le etichette non possono essere rimosse da un tipo di evento.

Crea un tipo di evento

Prima di creare il tuo modello di rilevamento delle frodi, devi prima creare un tipo di evento. La creazione di un tipo di evento implica la definizione dell'attività aziendale (evento) per la valutazione delle frodi. La definizione dell'evento implica l'identificazione delle variabili di evento nel set di dati da includere per la valutazione delle frodi, la specificazione dell'entità che avvia l'evento e le etichette che classificano l'evento.

Prerequisiti per creare un tipo di evento

Prima di iniziare a creare il tuo tipo di evento, assicurati di aver completato quanto segue:

- Hai utilizzato lo Esplora modelli di dati strumento per ottenere informazioni sugli elementi di dati richiesti da Amazon Fraud Detector per creare il tuo modello di rilevamento delle frodi.
- Hai utilizzato le informazioni ottenute da Data Models Explorer per creare il set di dati dell'evento e caricarlo nel bucket Amazon S3.
- Creato Variables e Etichette desideri che Amazon Fraud Detector venga utilizzato per creare un modello di rilevamento delle frodi per questo evento. Entità Assicurati che le variabili, il tipo di entità e le etichette che hai creato siano inclusi nel set di dati dell'evento.

Puoi creare il tuo tipo di evento nella console Amazon Fraud Detector, utilizzando l'API, utilizzando o utilizzando l'AWSSDK. AWS CLI

Crea un tipo di evento nella console Amazon Fraud Detector

Per creare un tipo di evento,

1. Apri la console di AWS gestione e accedi al tuo account. Accedi ad Amazon Fraud Detector.
2. Nel riquadro di navigazione a sinistra, scegli Eventi.
3. Nella pagina Tipo di eventi, scegli Crea.
4. In Dettagli sul tipo di evento,
   a. Nel Nome, inserisci il nome del tuo evento.
   b. Nella Descrizione, facoltativamente, inserisci una descrizione.
   c. Nell'Entità, seleziona il tipo di entità che hai creato per il tuo evento.
5. In Variabili di evento,
   - Nella sezione Scegli come definire le variabili di questo evento,
     - Se hai già creato le variabili di evento per questo evento, seleziona Seleziona variabili dall'elenco delle variabili e, in Variabili, seleziona le variabili che hai creato per questo evento.
     - Se non hai creato variabili per questo evento, seleziona Seleziona variabili da un set di dati di addestramento,
       - Nel ruolo IAM, seleziona il ruolo IAM che desideri che Amazon Fraud Detector utilizzi per accedere al bucket Amazon S3 che contiene il tuo set di dati
       - In Posizione dati, inserisci il percorso verso la posizione del tuo set di dati. Usa il `S3 URI` percorso simile a questo:`S3://`*`your-bucket-name`*`/`*`example dataset filename`*`.csv`.
       - Scegliere Upload (Carica).
       - In Variabili, vengono visualizzati tutti i nomi delle variabili di evento che Amazon Fraud Detector ha estratto dal file del set di dati.

         Se desideri includere la variabile per rilevare le frodi, nel Tipo di variabile seleziona il tipo di variabile. Scegli Rimuovi per rimuovere l'inclusione delle variabili per il rilevamento delle frodi. Ripetere questo passaggio per ogni variabile nell'elenco.

6. In Etichette (opzionale), in Etichette, seleziona le etichette che hai creato per questo evento. Assicurati di selezionare un'etichetta ciascuna per eventi fraudolenti e legittimi.
7. Se desideri configurare l'elaborazione automatica a valle per questo evento, nella sezione Orchestrazione degli eventi con Amazon EventBridge - opzionale, attiva Abilita l'orchestrazione degli eventi con Amazon. EventBridge Per ulteriori informazioni sull'orchestrazione degli eventi, vedere. Orchestrazione degli eventi

   > **Note**
   >
   > Puoi anche abilitare l'orchestrazione degli eventi in un secondo momento dopo aver creato il tipo di evento.

8. Scegli Crea tipo di evento.

Crea un tipo di evento utilizzando AWS SDK for Python (Boto3)

L'esempio seguente mostra una richiesta di esempio per l'`PutEventType`API. L'esempio presuppone che tu abbia creato le variabili `ip_address`email_address`, le etichette `legit` e `fraud` il tipo di `sample_customer` entità. Per informazioni su come creare queste risorse, vedereRisorse.

> **Note**
>
> È necessario creare variabili, tipi di entità ed etichette prima di aggiungerli al tipo di evento.

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

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

Eliminare un evento o un tipo di evento

Quando elimini un evento, Amazon Fraud Detector elimina definitivamente quell'evento e i dati associati all'evento non vengono più archiviati in Amazon Fraud Detector.

Per eliminare un evento che Amazon Fraud Detector ha valutato tramite API **`GetEventPrediction`**

1. Accedi AWS Management Console e apri la console Amazon Fraud Detector all'indirizzo https://console.aws.amazon.com/frauddetector.
2. Nel riquadro di navigazione a sinistra della console, scegli Cerca previsioni precedenti.
3. Scegli l'evento che desideri eliminare.
4. Scegli Azioni, quindi scegli Elimina evento.
5. Entra**`delete`**, quindi scegli Elimina evento.

> **Note**
>
> In questo modo vengono eliminati tutti i record associati a quell'ID evento, inclusi i dati sugli eventi inviati all'`SendEvent`operazione e i dati di previsione generati tramite l'`GetEventPrediction`operazione.

Per eliminare un evento archiviato in Amazon Fraud Detector ma non valutato (ovvero, è stato archiviato tramite l'`SendEvent`operazione), devi effettuare una `DeleteEvent` richiesta e specificare l'ID evento e l'ID del tipo di evento. Se desideri eliminare sia l'evento che la cronologia delle previsioni associata all'evento, imposta il valore del `deleteAuditHistory` parametro su «true». Con il `deleteAuditHistory` parametro impostato su «true», i dati dell'evento sono disponibili tramite la ricerca per un massimo di 30 secondi dopo il completamento dell'operazione di eliminazione.

Per eliminare tutti gli eventi associati a un tipo di evento

1. Nel riquadro di navigazione a sinistra della console, scegli Tipi di eventi
2. Scegli il tipo di evento per il quale desideri eliminare tutti gli eventi.
3. Vai alla scheda Eventi memorizzati e scegli Elimina eventi memorizzati

A seconda del numero di eventi memorizzati per il tipo di evento, l'eliminazione di tutti gli eventi memorizzati potrebbe richiedere del tempo. Ad esempio, l'eliminazione di un set di dati da 1 GB (circa

1-2 milioni di eventi per il cliente medio) richiede circa 2 ore. Durante questo periodo, i nuovi eventi che invii ad Amazon Fraud Detector di questo tipo non vengono archiviati, ma puoi continuare a generare previsioni di frode tramite l'`GetEventPrediction`operazione.

Per eliminare un tipo di evento

Non è possibile eliminare un tipo di evento utilizzato in un rilevatore o in un modello o con eventi memorizzati associati. Prima di eliminare un tipo di evento, è necessario eliminare tutti gli eventi associati a quel tipo di evento.

Quando elimini un tipo di evento, Amazon Fraud Detector elimina definitivamente quel tipo di evento e i dati non vengono più archiviati in Amazon Fraud Detector.

1. Nel riquadro di navigazione a sinistra della console Amazon Fraud Detector, scegli Risorse, quindi scegli Eventi.
2. Scegli il tipo di evento che desideri eliminare.
3. Scegli Azioni, quindi scegli Elimina tipo di evento.
4. Immettete il nome del tipo di evento, quindi scegliete Elimina tipo di evento.

Archiviazione dati eventi

Dopo aver raccolto il set di dati, è possibile archiviarlo internamente utilizzando Amazon Fraud Detector o esternamente con Simple Storage Service (Amazon S3). Ti consigliamo di scegliere dove archiviare il set di dati in base al modello utilizzato per generare previsioni di frode. Di seguito è riportata una suddivisione dettagliata di queste due opzioni di archiviazione.

- Archiviazione interna: il set di dati viene archiviato con Amazon Fraud Detector. Tutti i dati associati a un evento vengono archiviati insieme. Puoi caricare il set di dati degli eventi archiviato con Amazon Fraud Detector in qualsiasi momento. Puoi trasmettere gli eventi uno alla volta su un'API Amazon Fraud Detector oppure importare set di dati di grandi dimensioni (fino a 1 GB) utilizzando la funzione di importazione in batch. Quando addestri un modello utilizzando il set di dati archiviato con Amazon Fraud Detector, puoi specificare un intervallo di tempo per limitare le dimensioni del set di dati.
- Archiviazione esterna: il set di dati è archiviato in una fonte di dati esterna diversa da Amazon Fraud Detector. Attualmente, Amazon Fraud Detector supporta l'utilizzo di Amazon S3 per questo scopo. Se il tuo modello si trova su un file caricato su Amazon S3, quel file non può contenere più di 5 GB di dati non compressi. Se è più di questo, assicurati di abbreviare l'intervallo di tempo del tuo set di dati.

La tabella seguente fornisce dettagli sul tipo di modello e sulla fonte di dati che supporta.

Tipo di modello	Fonte dati di addestramento compatibile
Performance Fraud Online	Archiviazione esterna, memoria interna
Insights sulle frodi nelle transazioni	Archiviazione interna
Account Takeover Insights	Archiviazione interna

Per informazioni sull'archiviazione esterna del set di dati con Amazon Simple Storage Service, consultaArchivia i dati degli eventi esternamente con Amazon S3 . Per informazioni sull'archiviazione interna del set di dati con Amazon Fraud Detector, consultaArchivia i dati degli eventi internamente con Amazon Fraud Detector.

Archivia i dati degli eventi esternamente con Amazon S3

Se stai addestrando un modello Online Fraud Insights, puoi scegliere di archiviare i dati degli eventi esternamente con Amazon S3. Per archiviare i dati degli eventi in Amazon S3, devi prima creare un file di testo in formato CSV, aggiungere i dati dell'evento e quindi caricare il file CSV in un bucket Amazon S3.

> **Note**
>
> I tipi di modello Transaction Fraud Insights e Account Takeover Insights non supportano set di dati archiviati esternamente con Amazon S3

Crea file CSV

Amazon Fraud Detector richiede che la prima riga del file CSV contenga le intestazioni delle colonne. Le intestazioni delle colonne nel file CSV devono corrispondere alle variabili definite nel tipo di evento. Per un set di dati di esempio, vedereOttieni e carica un set di dati di esempio

Il modello Online Fraud Insights richiede un set di dati di formazione con almeno 2 variabili e fino a 100 variabili. Oltre alle variabili di evento, il set di dati di formazione deve contenere le seguenti intestazioni:

- EVENT_TIMESTAMP - Definisce quando si è verificato l'evento
- EVENT_LABEL - Classificare l'evento come fraudolento o legittimo. I valori nella colonna devono corrispondere ai valori definiti nel tipo di evento.

I seguenti dati CSV di esempio rappresentano gli eventi di registrazione storici di un commerciante online:

```
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**
>
> Il file di dati CSV può contenere virgolette e virgole come parte dei dati.

Di seguito è rappresentata una versione semplificata del tipo di evento corrispondente. Le variabili di evento corrispondono alle intestazioni del file CSV e i valori in`EVENT_LABEL` corrispondono ai valori nell'elenco delle etichette.

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

Formati Timestamp degli eventi

Assicurati che il timestamp dell'evento sia nel formato richiesto. Come parte del processo di creazione del modello, il tipo di modello Online Fraud Insights ordina i dati in base al timestamp dell'evento e li divide per scopi di formazione e test. Per ottenere una stima equa delle prestazioni, il modello si addestra prima sul set di dati di addestramento e quindi testa questo modello sul set di dati di test.

Amazon Fraud Detector supporta i seguenti formati di data/ora per i valori inseriti`EVENT_TIMESTAMP` durante l'addestramento del modello:

- %YYYy-%mm-%DDt%hH: %mm: %sSz (standard ISO 8601 solo in UTC senza millisecondi)

  Esempio: 2019-11-30T 13:01:01 Z
- %aaaa/%mm/%dd %hh: %mm: %ss (AM/PM)

  Esempi: 30/11/2019 13:01:01 o 30/11/2019 13:01:01
- %mm/%gd/%aaaa %hh: %mm: %ss

  Esempi: 30/11/2019 13:01:01, 30/11/2019 13:01:01
- %mm/%dd/%yy %hh: %mm: %ss

  Esempi: 30/11/19 13:01:01 PM, 30/11/19 13:01:01

Amazon Fraud Detector fa le seguenti ipotesi quando analizza i formati di data/ora per i timestamp degli eventi:

- Se si utilizza lo standard ISO 8601, deve corrispondere esattamente alla specifica precedente
- Se si utilizza uno degli altri formati, è disponibile una flessibilità aggiuntiva:
  - Per mesi e giorni, puoi fornire cifre singole o doppie. Ad esempio, 1/12/2019 è una data valida.
  - Non è necessario includere hh:mm:ss se non li avete (cioè, potete semplicemente fornire una data). Puoi anche fornire un sottoinsieme delle sole ore e minuti (ad esempio, hh:mm). La semplice indicazione dell'ora non è supportata. Anche i millisecondi non sono supportati.
  - Se si forniscono etichette AM/PM, si presume un orologio di 12 ore. Se non sono disponibili informazioni AM/PM, si presume che l'orologio sia attivo 24 ore su 24.
  - È possibile utilizzare «/» o «-» come delimitatori per gli elementi della data. «:» è assunto per gli elementi del timestamp.

Campionamento del set di dati nel tempo

Ti consigliamo di fornire esempi di frode e campioni legittimi nello stesso intervallo temporale. Ad esempio, se fornisci eventi fraudolenti degli ultimi 6 mesi, dovresti fornire anche eventi legittimi che coprano lo stesso periodo di tempo. Se il set di dati contiene una distribuzione estremamente irregolare di frodi ed eventi legittimi, potresti ricevere il seguente errore: «La distribuzione delle frodi nel tempo è inaccettabilmente fluttuante. Impossibile suddividere correttamente il set di dati.» In genere, la soluzione più semplice per questo errore è garantire che gli eventi fraudolenti e gli eventi legittimi vengano campionati in modo uniforme nello stesso lasso di tempo. Potrebbe inoltre essere necessario rimuovere i dati se si verifica un forte aumento delle frodi in un breve periodo di tempo.

Se non riesci a generare dati sufficienti per creare un set di dati distribuito uniformemente, un approccio consiste nel randomizzare EVENT_TIMESTAMP dei tuoi eventi in modo che siano distribuiti uniformemente. Tuttavia, ciò spesso fa sì che le metriche delle prestazioni non siano realistiche perché Amazon Fraud Detector utilizza EVENT_TIMESTAMP per valutare i modelli sul sottoinsieme appropriato di eventi nel set di dati.

Valori nulli e mancanti

Amazon Fraud Detector gestisce i valori nulli e mancanti. Tuttavia, la percentuale di valori nulli per le variabili dovrebbe essere limitata. Le colonne EVENT_TIMESTAMP e EVENT_LABEL non devono contenere valori mancanti.

Convalida dei file

Amazon Fraud Detector non riuscirà ad addestrare un modello se viene attivata una delle seguenti condizioni:

- Se il CSV non può essere analizzato
- Se il tipo di dati di una colonna non è corretto

Caricare i dati degli eventi in un bucket Amazon S3

Dopo aver creato un file CSV con i dati dell'evento, caricare il file nel bucket Amazon S3.

Come caricare in un bucket Amazon S3

1. Accedi alla AWS Management Console e apri la console di Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. Scegliere Create bucket (Crea bucket).

   Si apre la procedura guidata Create bucket (Crea bucket).
3. In Bucket name (Nome bucket), immettere un nome conforme a DNS per il bucket.

   Il nome del bucket deve:

   - Essere univoco in tutto Amazon S3.
   - Deve contenere da 3 a 63 caratteri
   - Non contiene caratteri maiuscoli.
   - Iniziare con una lettera minuscola o un numero.

   Una volta creato il bucket, non è possibile modificarne il nome. Per informazioni sulla denominazione dei bucket, consulta Regole di denominazione dei bucket nella Guida per l'utente di Amazon SStorage Service.

   > **Important**
   >
   > Evitare di includere informazioni riservate, ad esempio numeri di account, nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.

4. In Regione scegliere la Regione AWS in cui si desidera che il bucket risieda. È necessario selezionare la stessa regione in cui si utilizza Amazon Fraud Detector, ovvero Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Europa (Irlanda), Asia Pacifico (Singapore) o Asia Pacifico (Sydney).
5. In Bucket settings for Block Public Access (Impostazioni bucket per blocco dell'accesso pubblico), scegliere le impostazioni del blocco dell'accesso pubblico che si desidera applicare al bucket.

   Si consiglia di lasciare abilitate tutte le impostazioni. Per ulteriori informazioni sul blocco dell'accesso pubblico, consulta blocco dell'accesso pubblico allo storage Amazon S3 nella Guida per l'utente di Amazon S3 nella Guida per l'utente di Amazon S3.
6. Seleziona Create bucket (Crea bucket).
7. Caricare i file di dati di addestramento nel bucket Amazon S3. Prendi nota del percorso di localizzazione di Amazon S3 per il tuo file di training (ad esempio, s3://bucketname/object.csv).

Archivia i dati degli eventi internamente con Amazon Fraud Detector

Puoi scegliere di archiviare i dati degli eventi in Amazon Fraud Detector e utilizzare i dati archiviati in un secondo momento per addestrare i tuoi modelli. Archiviando i dati degli eventi in Amazon Fraud Detector, puoi addestrare modelli che utilizzano variabili calcolate automaticamente per migliorare le prestazioni, semplificare la riqualificazione dei modelli e aggiornare le etichette antifrode per chiudere il ciclo di feedback del machine learning. Gli eventi vengono archiviati a livello di risorsa del tipo di evento, quindi tutti gli eventi dello stesso tipo di evento vengono archiviati insieme in un unico set di dati del tipo di evento. Come parte della definizione di un tipo di evento, puoi facoltativamente specificare se archiviare gli eventi per quel tipo di evento attivando l'impostazione Event Ingestion nella console di Amazon Fraud Detector.

Puoi archiviare singoli eventi o importare un gran numero di set di dati di eventi in Amazon Fraud Detector. I singoli eventi possono essere trasmessi in streaming utilizzando l'GetEventPredictionAPI o l'SendEventAPI. I set di dati di grandi dimensioni possono essere importati rapidamente e facilmente in Amazon Fraud Detector utilizzando la funzione di importazione in batch nella console Amazon Fraud Detector o utilizzando l'CreateBatchImportJobAPI.

Puoi utilizzare la console Amazon Fraud Detector in qualsiasi momento per verificare il numero di eventi già archiviati per ogni tipo di evento.

Prepara i dati degli eventi per l'archiviazione

I dati degli eventi archiviati internamente con Amazon Fraud Detector vengono archiviati a livello di`Event Type` risorsa. Pertanto, tutti i dati degli eventi che provengono dallo stesso evento vengono archiviati in un unico`Event Type`. Gli eventi memorizzati possono essere successivamente utilizzati per addestrare un nuovo modello o riaddestrare un modello esistente. Quando si addestra un modello utilizzando i dati degli eventi memorizzati, è possibile specificare facoltativamente un intervallo temporale di eventi per limitare le dimensioni del set di dati di allenamento.

Ogni volta che archivi i tuoi dati in Amazon Fraud Detector, utilizzando la console Amazon Fraud Detector, l'`SendEvent`API o l'`CreateBatchImportJob`API, Amazon Fraud Detector convalida i tuoi dati prima di archiviarli. Se i dati non superano la convalida, i dati dell'evento non vengono archiviati.

Prerequisiti per l'archiviazione interna dei dati con Amazon Fraud Detector

- Per assicurarti che i dati dell'evento superino la convalida e che il set di dati venga archiviato correttamente, assicurati di aver utilizzato le informazioni fornite da Data models explorer per preparare il set di dati.
- Hai creato un tipo di evento per i dati degli eventi che desideri archiviare con Amazon Fraud Detector. In caso contrario, segui le istruzioni per creare un tipo di evento.

Convalida intelligente dei dati

Quando carichi il set di dati nella console Amazon Fraud Detector per l'importazione in batch, Amazon Fraud Detector utilizza Smart Data Validation (SDV) per convalidare il set di dati prima di importare i dati. SDV esegue la scansione del file di dati caricato e identifica problemi come dati mancanti e formati o tipi di dati errati. Oltre a convalidare il set di dati, SDV fornisce anche un rapporto di convalida che elenca tutti i problemi identificati e suggerisce azioni per risolvere i problemi più gravi. Alcuni dei problemi identificati da SDV potrebbero essere critici e devono essere risolti prima che Amazon Fraud Detector possa importare correttamente il set di dati. Per ulteriori informazioni, consulta Rapporto di convalida intelligente dei dati.

L'SDV convalida il set di dati a livello di file e a livello di dati (riga). A livello di file, SDV analizza il file di dati e identifica problemi quali autorizzazioni inadeguate per accedere al file, dimensioni del file, formato e intestazioni (metadati degli eventi e variabili di evento) errati. A livello di dati, SDV analizza i dati di ogni evento (riga) e identifica problemi come il formato dei dati errati, la lunghezza dei dati, il formato del timestamp e i valori nulli.

La convalida intelligente dei dati è attualmente disponibile solo nella console Amazon Fraud Detector e la convalida è attivata per impostazione predefinita. Se non desideri che Amazon Fraud Detector utilizzi la convalida intelligente dei dati prima di importare il set di dati, disattiva la convalida nella console Amazon Fraud Detector quando carichi il set di dati.

Convalida dei dati archiviati quando si utilizzano API oAWS SDK

Quando si caricano eventi tramite l'operazione`SendEvent`, `GetEventPrediction`, o l'`CreateBatchImportJob` API, Amazon Fraud Detector convalida quanto segue:

- L' EventIngestion impostazione per quel tipo di evento è ABILITATA.
- I timestamp degli eventi non possono essere aggiornati. Un evento con un ID evento ripetuto e un EVENT_TIMESTAMP diverso verrà considerato un errore.
- I nomi e i valori delle variabili corrispondono al formato previsto. Per ulteriori informazioni, consulta Creare una variabile.
- Le variabili obbligatorie sono compilate con un valore.
- Tutti i timestamp degli eventi non sono più vecchi di 18 mesi e non sono future.

Archivia i dati degli eventi utilizzando l'importazione in batch

Con la funzione di importazione in batch, puoi caricare rapidamente e facilmente set di dati di eventi storici di grandi dimensioni in Amazon Fraud Detector utilizzando la console, l'API o l'SDK AWS. Per utilizzare l'importazione in batch, crea un file di input in formato CSV che contenga tutti i dati dell'evento, carica il file CSV su un bucket Amazon S3 e avvia un processo di importazione. Amazon Fraud Detector convalida innanzitutto i dati in base al tipo di evento e quindi importa automaticamente l'intero set di dati. Una volta importati, i dati sono pronti per essere utilizzati per addestrare nuovi modelli o per riaddestrare modelli esistenti.

File di input e output

Il file CSV di input deve contenere intestazioni che corrispondono alle variabili definite nel tipo di evento associato più quattro variabili obbligatorie. Per ulteriori informazioni, consulta Prepara i dati degli eventi per l'archiviazione. La dimensione massima del file di dati di input è di 20 Gigabyte (GB), ovvero circa 50 milioni di eventi. Il numero di eventi varierà in base alle dimensioni dell'evento. Se il processo di importazione ha avuto successo, il file di output è vuoto. Se l'importazione non ha avuto successo, il file di output contiene i log degli errori.

Crea un file CSV

Amazon Fraud Detector importa dati solo da file in formato CSV (valori separati da virgola). La prima riga del file CSV deve contenere intestazioni di colonna che corrispondono esattamente alle variabili definite nel tipo di evento associato più quattro variabili obbligatorie: EVENT_ID, EVENT_TIMESTAMP, ENTITY_ID e ENTITY_TYPE. Puoi anche includere facoltativamente EVENT_LABEL e LABEL_TIMESTAMP (LABEL_TIMESTAMP è obbligatorio se è incluso EVENT_LABEL).

Definire le variabili obbligatorie

Le variabili obbligatorie sono considerate metadati degli eventi e devono essere specificate in lettere maiuscole. I metadati degli eventi vengono inclusi automaticamente per l'addestramento dei modelli. La tabella seguente elenca le variabili obbligatorie, la descrizione di ciascuna variabile e il formato richiesto per la variabile.

Nome	Descrizione	Requisiti
ID_EVENTO	Un identificatore per l'evento. Ad esempio, se l'evento è una transazione online, EVENT_ID potrebbe essere il numero di riferimento della transazione fornito al cliente.	• L'EVENT_ID è obbligatorio per i processi di importazi one in batch. • Deve essere univoco per quell'evento. • Dovrebbe rappresentare informazioni significative per la tua attività. • Deve soddisfare il modello di espressione regolare (ad esempio,`^[0-9a-z_-]+$.`) • Non è consigliabile aggiungere un timestamp a EVENT_ID. Questa operazione potrebbe causare problemi durante l'aggiornamento dell'evento. Questo perché devi fornire

Nome	Descrizione	Requisiti
		esattamente lo stesso EVENT_ID se lo fai.

Nome	Descrizione	Requisiti

TIMESTAMP DELL'EVENTO	Timestamp del momento in cui si è verificato l'evento. Il timestamp deve essere nello standard ISO 8601 in UTC.	• L'EVENT_TIMESTAMP è obbligatorio per i processi di importazione in batch.
		• Deve essere specificato in uno dei seguenti formati:
		  • %YYYy-%mm-%DDt%hH: %mm: %sSz (standard ISO 8601 solo in UTC senza millisecondi)
		
		  Esempio: 2019-11-30T 13:01:01 Z
		  • %aaaa/%mm/%dd %hh: %mm: %ss (AM/PM)
		
		  Esempi: 30/11/2019 13:01:01 o 30/11/2019 13:01:01
		  • %mm/%gd/%aaaa %hh: %mm: %ss
		
		  Esempi: 30/11/2019 13:01:01, 30/11/2019 13:01:01
		  • %mm/%dd/%yy %hh: %mm: %ss
		
		  Esempi: 30/11/19 13:01:01 PM, 30/11/19 13:01:01
		• Amazon Fraud Detector fa le seguenti ipotesi quando analizza i formati di data/ora per i timestamp degli eventi:

Nome	Descrizione	Requisiti

		• Se si utilizza lo standard ISO 8601, deve corrispondere esattamente alla specifica precedente
		• Se si utilizza uno degli altri formati, è disponibile una flessibilità aggiuntiva:
		  • Per mesi e giorni, puoi fornire cifre singole o doppie. Ad esempio, 1/12/2019 è una data valida.
		  • Non è necessario includere hh:mm:ss se non li avete (cioè, potete semplicemente fornire una data). Puoi anche fornire un sottoinsieme delle sole ore e minuti (ad esempio, hh:mm). La semplice indicazione dell'ora non è supportata. Anche i millisecondi non sono supportati.
		  • Se si forniscono etichette AM/PM, si presume un orologio di 12 ore. Se non sono disponibili informazioni AM/PM, si presume che l'orologio sia attivo 24 ore su 24.

Nome	Descrizione	Requisiti
		• È possibile utilizzare «/» o «-» come delimitatori per gli elementi della data. «:» è assunto per gli elementi del timestamp.
ENTITY_ID	Un identificatore per l'entità che esegue l'evento.	• ENTITY_ID è obbligatorio per i processi di importazione in batch • Deve seguire lo schema delle espressioni regolari: `^[0-9A-Za-z_.@+-]+$` . • Se l'ID dell'entità non è disponibile al momento della valutazione, specifica l'ID dell'entità come sconosciuto.
TIPO_ENTITÀ	L'entità che organizza l'evento, ad esempio un commerciante o un cliente	ENTITY_TYPE è obbligatorio per i processi di importazione in batch
ETICHETTA_EVENTO	Classifica l'evento come`fraudulent` o`legitimate`	EVENT_LABEL è obbligatorio se è incluso LABEL_TIMESTAMP
TIMESTAMP DELL'ETICHETTA	Il timestamp dell'ultima volta che l'etichetta dell'evento è stata compilata o aggiornata	• LABEL_TIMESTAMP è obbligatorio se è incluso EVENT_LABEL. • Deve seguire il formato del timestamp.

Caricare file CSV in Amazon S3 per l'importazione in batch

Dopo aver creato un file CSV con i tuoi dati, caricare il file nel bucket Amazon SStorage Service (Amazon S3).

Come caricare i dati degli eventi in un bucket Amazon S3

1. Accedi alla AWS Management Console e apri la console di Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/.
2. Scegliere Create bucket (Crea bucket).

   Si apre la procedura guidata Create bucket (Crea bucket).
3. In Bucket name (Nome bucket), immettere un nome conforme a DNS per il bucket.

   Il nome del bucket deve:

   - Essere univoco in tutto Amazon S3.
   - Deve contenere da 3 a 63 caratteri
   - Non contiene caratteri maiuscoli.
   - Iniziare con una lettera minuscola o un numero.

   Una volta creato il bucket, non è possibile modificarne il nome. Per informazioni sulla denominazione dei bucket, consulta Regole di denominazione dei bucket nella Guida per l'utente di Amazon SStorage Service.

   > **Important**
   >
   > Evitare di includere informazioni riservate, ad esempio numeri di account, nel nome del bucket. Il nome bucket è visibile nell'URL che punta agli oggetti nel bucket.
4. In Regione scegliere la Regione AWS in cui si desidera che il bucket risieda. È necessario selezionare la stessa regione in cui si utilizza Amazon Fraud Detector, ovvero Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Europa (Irlanda), Asia Pacifico (Singapore) o Asia Pacifico (Sydney).
5. In Bucket settings for Block Public Access (Impostazioni bucket per blocco dell'accesso pubblico), scegliere le impostazioni del blocco dell'accesso pubblico che si desidera applicare al bucket.

Si consiglia di lasciare abilitate tutte le impostazioni. Per informazioni sul blocco dell'accesso pubblico, blocco accesso pubblico, consulUso dell'accesso pubblico, consulUso dell'accesso pubblico, consulUso dell'accesso pubblico, consulUso dell'accesso pubblico, consulUso dell'accesso pubblico, consulUso dell'accesso pubblico, consulUso dell'accesso pubblico

6. Seleziona Create bucket (Crea bucket).
7. Caricare i file di dati di addestramento nel bucket Amazon S3. Prendi nota del percorso di localizzazione di Amazon S3 per il tuo file di training (ad esempio, s3://bucketname/object.csv).

Importazione in batch dei dati degli eventi nella console Amazon Fraud Detector

Puoi importare facilmente un gran numero di set di dati di eventi nella console Amazon Fraud Detector, utilizzando l'`CreateBatchImportJob`API o utilizzando l'SDK AWS. Prima di procedere, assicurati di aver seguito le istruzioni per preparare il set di dati come file CSV. Assicurati di aver caricato anche il file CSV in un bucket Amazon S3.

Utilizzo della console Amazon Fraud Detector

Per importare in batch i dati degli eventi nella console

1. Apri la console AWS, accedi al tuo account e accedi ad Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra, seleziona Eventi.
3. Scegliere il tipo di evento.
4. Seleziona la scheda Eventi memorizzati.
5. Nel riquadro dei dettagli degli eventi archiviati, assicurati che l'inserimento degli eventi sia attivo.
6. Nel riquadro Importa dati eventi, scegli Nuova importazione.
7. Nella pagina di importazione di nuovi eventi, fornisci le seguenti informazioni:
   - [Consigliato] Lascia Attiva la convalida intelligente dei dati per questo set di dati - nuovo set all'impostazione predefinita.
   - Per il ruolo IAM per i dati, seleziona il ruolo IAM che hai creato per il bucket Amazon S3 che contiene il file CSV che intendi importare.
   - Per la posizione dei dati di input, inserisci la posizione S3 in cui hai il file CSV.

- Se desideri specificare una posizione separata per archiviare i risultati dell'importazione, fai clic sul pulsante Separa posizione dati per input e risultati e fornisci una posizione valida per il bucket Amazon S3.

> **Important**
>
> Assicurati che il ruolo IAM selezionato disponga delle autorizzazioni di lettura per il bucket Amazon S3 di input e di scrittura per il bucket Amazon S3 di output.

8. Scegli Start (Avvia).
9. La colonna Stato nel riquadro Importa dati eventi mostra lo stato del processo di convalida e importazione. Il banner in alto fornisce una descrizione di alto livello dello stato quando il set di dati viene prima sottoposto alla convalida e poi all'importazione.
10. Segui le indicazioni fornite aMonitorare l'avanzamento della convalida del set di dati e del processo di importazione.

Monitorare l'avanzamento della convalida del set di dati e del processo di importazione

Se utilizzi la console Amazon Fraud Detector per eseguire un processo di importazione in batch, per impostazione predefinita, Amazon Fraud Detector convalida il set di dati prima dell'importazione. Puoi monitorare l'avanzamento e lo stato dei processi di convalida e importazione nella pagina di importazione di nuovi eventi della console Amazon Fraud Detector. Un banner nella parte superiore della pagina fornisce una breve descrizione dei risultati della convalida e dello stato del processo di importazione. A seconda dei risultati della convalida e dello stato del processo di importazione, potrebbe essere necessario intraprendere azioni per garantire la corretta convalida e importazione del set di dati.

La tabella seguente fornisce i dettagli delle azioni da intraprendere in base all'esito delle operazioni di convalida e importazione.

Messaggio banner	Stato	Significato	Cosa devo fare
La convalida dei dati è iniziata	Convalida in corso	SDV ha iniziato a convalidare il set di dati	Attendi che lo stato cambi

Messaggio banner	Stato	Significato	Cosa devo fare
La convalida dei dati non può procedere a causa di errori nel set di dati. Correggi gli errori nel tuo file di dati e avvia un nuovo processo di importazione. Consulta il rapporto di convalida per ulteriori informazioni	Convalida fallita	SDV ha identificato problemi nel file di dati. Questi problemi devono essere risolti per una corretta importazione del set di dati.	Nel riquadro Importa dati eventi, seleziona l'ID del Job e visualizza il rapporto di convalida. Segui i consigli contenuti nel rapporto per risolvere tutti gli errori elencati. Per ulteriori informazioni, consulta Utilizzo del rapporto di convalida.
L'importazione dei dati è iniziata. Convalida completata correttamente	Importazione in corso	Il set di dati ha superato la convalida. AFD ha iniziato a importare il tuo set di dati	Attendi che lo stato cambi

Messaggio banner	Stato	Significato	Cosa devo fare
Convalida completata con avvisi. L'importazione dei dati è iniziata	Importazione in corso	La convalida di alcuni dati del set di dati non è riuscita. Tuttavia, i dati che hanno superato la convalida soddisfano i requisiti minimi di dimensione dei dati per l'importazione.	Monitora il messaggio nel banner e attendi che lo stato cambi

Messaggio banner	Stato	Significato	Cosa devo fare
I tuoi dati sono stati importati parzialmente. Alcuni dati non sono stati convalidati e non sono stati importati. Consultare il rapporto di convalida per ulteriori informazioni.	Importato. Lo stato mostra un'icona di avviso.	Alcuni dei dati del file di dati che non sono stati convalidati non sono stati importati. Il resto dei dati che hanno superato la convalida è stato importato.	Nel riquadro Importa dati eventi, seleziona l'ID del Job e visualizza il rapporto di convalida. Segui i consigli nella tabella degli avvisi a livello di dati per rispondere agli avvisi elencati. Non è necessario rispondere a tutte le avvertenze. Tuttavia, assicurati che il tuo set di dati contenga più del 50% dei dati che superano la convalida per una corretta importazione. Dopo aver risposto agli avvisi, avvia un nuovo processo di importazione. Per ulteriori informazioni, consulta Utilizzo del rapporto di convalida.
L'importazione dei dati non è riuscita a causa di un errore di elaborazione. Avvio di un nuovo processo di importazione di dati	Importazione non riuscita	L'importazione non è riuscita a causa di un errore transitorio in fase di esecuzione	Avvio di un nuovo processo di importazione

Messaggio banner	Stato	Significato	Cosa devo fare
I dati sono stati importati con successo	importato	Sia la convalida che l'importazione sono state completate con successo	Seleziona l'ID del Job di importazione per visualizzare i dettagli e quindi procedi con l'addestramento del modello

> **Note**
>
> Ti consigliamo di attendere 10 minuti dopo che il set di dati è stato importato correttamente in Amazon Fraud Detector per assicurarti che vengano completamente assorbiti dal sistema.

Rapporto di convalida intelligente dei dati

La convalida intelligente dei dati crea un rapporto di convalida al termine della convalida. Il rapporto di convalida fornisce dettagli su tutti i problemi che SDV ha identificato nel set di dati, con azioni suggerite per risolvere i problemi più gravi. È possibile utilizzare il rapporto di convalida per determinare quali sono i problemi, dove si trovano nel set di dati, la gravità dei problemi e come risolverli. Il rapporto di convalida viene creato anche quando la convalida viene completata correttamente. In questo caso, puoi visualizzare il rapporto per vedere se ci sono problemi elencati e, in caso affermativo, decidere se vuoi correggerli.

> **Note**
>
> La versione attuale di SDV analizza il set di dati alla ricerca di problemi che potrebbero causare il fallimento dell'importazione in batch. Se la convalida e l'importazione in batch hanno esito positivo, il set di dati può ancora presentare problemi che potrebbero causare il fallimento dell'addestramento del modello. Ti consigliamo di visualizzare il rapporto di convalida anche se la convalida e l'importazione hanno avuto esito positivo e di risolvere eventuali problemi elencati nel rapporto per una corretta formazione del modello. Dopo aver risolto i problemi, crea un nuovo processo di importazione in batch.

Accesso al rapporto di convalida

È possibile accedere al rapporto di convalida in qualsiasi momento dopo il completamento della convalida utilizzando una delle seguenti opzioni:

1. Al termine della convalida e mentre il processo di importazione è in corso, nel banner in alto, scegli Visualizza rapporto di convalida.
2. Al termine del processo di importazione, nel riquadro Importa dati eventi, scegli l'ID del Job di importazione appena completato.

Utilizzo del rapporto di convalida

La pagina del rapporto di convalida del processo di importazione fornisce i dettagli di questo processo di importazione, un elenco degli eventuali errori critici, un elenco di avvisi su eventi specifici (righe) nel set di dati, se trovati, e un breve riepilogo del set di dati che include informazioni quali valori non validi e valori mancanti per ogni variabile.

- Importa i dettagli del lavoro

  Fornisce i dettagli del processo di importazione. Se il processo di importazione non è riuscito o il set di dati è stato importato parzialmente, scegli Vai al file dei risultati per visualizzare i log degli errori degli eventi che non sono stati importati.
- Errori critici

  Fornisce dettagli sui problemi più importanti del set di dati identificato da SDV. Tutti i problemi elencati in questo riquadro sono critici ed è necessario risolverli prima di procedere con l'importazione. Se si tenta di importare il set di dati senza risolvere i problemi critici, il processo di importazione potrebbe non riuscire.

  Per risolvere i problemi critici, segui i consigli forniti per ogni avviso. Dopo aver risolto tutti i problemi elencati nel riquadro Errori critici, crea un nuovo processo di importazione in batch.
- Avvisi a livello di dati

  Fornisce un riepilogo degli avvisi per eventi specifici (righe) nel set di dati. Se il riquadro degli avvisi a livello di dati è popolato, alcuni eventi nel set di dati non sono stati convalidati e non sono stati importati.

  Per ogni avviso, la colonna Descrizione mostra il numero di eventi che presentano il problema. Inoltre, gli ID degli eventi di esempio forniscono un elenco parziale di ID di eventi di esempio che

è possibile utilizzare come punto di partenza per individuare il resto degli eventi che presentano il problema. Utilizza la Raccomandazione fornita per l'avviso per risolvere il problema. Utilizza anche i log degli errori del file di output per ulteriori informazioni sul problema. I log degli errori vengono generati per tutti gli eventi che non sono riusciti a importare in batch. Per accedere ai registri degli errori, nel riquadro Importa dettagli del lavoro, scegli Vai al file dei risultati.

> **Note**
>
> Se più del 50% degli eventi (righe) nel set di dati non è stata convalidata, anche il processo di importazione ha esito negativo. In questo caso, è necessario correggere i dati prima di iniziare un nuovo processo di importazione.

- Riepilogo del set di dati

  Fornisce un riepilogo del rapporto di convalida del set di dati. Se la colonna Numero di avvisi mostra più di 0 avvisi, decidi se è necessario correggere tali avvisi. Se la colonna Numero di avvisi mostra 0, continua ad addestrare il tuo modello.

Importazione in batch di dati di eventi tramite SDK AWS per Python (Boto3)

Nell'esempio seguente viene illustrata una richiesta di esempio per CreateBatchImportJobAPI. Un processo di importazione in batch deve includere JobID, InputPath, OutputPath eventTypeNamee iamRoleArn. Il JoBid non può contenere lo stesso ID di un lavoro passato, a meno che il lavoro non esista nello stato CREATE_FAILED. InputPath e OutputPath devono essere percorsi S3 validi. Puoi scegliere di non specificare il nome del file in OutputPath, tuttavia dovrai comunque fornire una posizione valida del bucket S3. La eventTypeName terra iamRoleArn deve esistere. Il ruolo IAM deve concedere le autorizzazioni di lettura per l'ingresso del bucket Amazon S3 e le autorizzazioni di scrittura per l'output del bucket Amazon S3.

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

```
)
```

Annullare il processo di importazione in batch

Puoi annullare un processo di importazione in batch in corso in qualsiasi momento nella console di Amazon Fraud Detector, utilizzando l'`CancelBatchImportJob`API o l'SDK AWS.

Per annullare un processo di importazione in batch nella console,

1. Apri la console AWS, accedi al tuo account e accedi ad Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra, seleziona Eventi.
3. Scegliere il tipo di evento.
4. Seleziona la scheda Eventi memorizzati.
5. Nel riquadro Importa dati eventi, scegli l'ID del processo di importazione in corso che desideri annullare.
6. Nella pagina del processo dell'evento, fai clic su Azioni e seleziona Annulla l'importazione degli eventi.
7. Scegli Interrompi l'importazione degli eventi per annullare il processo di importazione in batch.

Annullamento del processo di importazione in batch tramite SDK AWS per Python (Boto3)

Nell'esempio seguente viene illustrata una richiesta di esempio per l'`CancelBatchImportJob`API. L'operazione di annullamento dell'importazione deve includere l'ID del processo di importazione in batch in corso.

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

Memorizza i dati degli eventi utilizzando l'operazione GetEventPredictions API

Per impostazione predefinita, tutti gli eventi inviati all'`GetEventPrediction`API per la valutazione vengono archiviati in Amazon Fraud Detector. Ciò significa che Amazon Fraud Detector archivia automaticamente i dati degli eventi quando si genera una previsione e li utilizza per aggiornare le variabili calcolate quasi in tempo reale. Puoi disabilitare l'archiviazione dei dati accedendo al tipo di evento nella console di Amazon Fraud Detector e impostando l'inserimento degli eventi su OFF o aggiornando il EventIngestion valore su DISABLED utilizzando l'operazione`PutEventType` API. Per ulteriori informazioni sul funzionamento dell'`GetEventPrediction`API, consultaPrevisioni di frode.

> **Important**
>
> Consigliamo vivamente di mantenerlo abilitato, una volta abilitato l'inserimento di eventi per un tipo di evento. La disabilitazione dell'inserimento degli eventi per lo stesso tipo di evento e quindi la generazione di previsioni potrebbero comportare un comportamento incoerente.

Memorizza i dati degli eventi utilizzando l'operazione SendEvent API

Puoi utilizzare l'operazione`SendEvent` API per archiviare gli eventi in Amazon Fraud Detector senza generare previsioni di frode per tali eventi. Ad esempio, puoi utilizzare l'`SendEvent`operazione per caricare un set di dati storico, che potrai utilizzare in seguito per addestrare un modello.

Formati di timestamp degli eventi per SendEvent API

Quando si archiviano i dati degli eventi tramite l'`SendEvent`API, è necessario assicurarsi che il timestamp dell'evento sia nel formato richiesto. Amazon Fraud Detector supporta i seguenti formati di data/ora:

- %YYYy-%mm-%DDt%hH: %mm: %sSz (standard ISO 8601 solo in UTC senza millisecondi)

  Esempio: 2019-11-30T 13:01:01 Z
- %aaaa/%mm/%dd %hh: %mm: %ss (AM/PM)

  Esempi: 30/11/2019 13:01:01 o 30/11/2019 13:01:01
- %mm/%gd/%aaaa %hh: %mm: %ss

  Esempi: 30/11/2019 13:01:01, 30/11/2019 13:01:01

- %mm/%dd/%yy %hh: %mm: %ss

  Esempi: 30/11/19 13:01:01 PM, 30/11/19 13:01:01

Amazon Fraud Detector fa le seguenti ipotesi quando analizza i formati di data/ora per i timestamp degli eventi:

- Se si utilizza lo standard ISO 8601, deve corrispondere esattamente alla specifica precedente
- Se si utilizza uno degli altri formati, è disponibile una flessibilità aggiuntiva:
  - Per mesi e giorni, puoi fornire cifre singole o doppie. Ad esempio, 1/12/2019 è una data valida.
  - Non è necessario includere hh:mm:ss se non li avete (cioè, potete semplicemente fornire una data). Puoi anche fornire un sottoinsieme delle sole ore e minuti (ad esempio, hh:mm). La semplice indicazione dell'ora non è supportata. Anche i millisecondi non sono supportati.
  - Se si forniscono etichette AM/PM, si presume un orologio di 12 ore. Se non sono disponibili informazioni AM/PM, si presume che l'orologio sia attivo 24 ore su 24.
  - È possibile utilizzare «/» o «-» come delimitatori per gli elementi della data. «:» è assunto per gli elementi del timestamp.

Di seguito è riportato un esempio di chiamata`SendEvent` API.

```
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'}],

)
```

Ottieni i dettagli dei dati di un evento archiviati

Dopo aver archiviato i dati degli eventi in Amazon Fraud Detector, puoi controllare i dati più recenti archiviati per un evento utilizzando l'GetEventAPI. Il seguente codice di esempio controlla i dati più recenti memorizzati per l'`sample_registration`evento.

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

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

Visualizza le metriche del set di dati di eventi memorizzato

Per ogni tipo di evento, puoi visualizzare metriche come il numero di eventi archiviati, la dimensione totale degli eventi archiviati e i timestamp dei primi e degli ultimi eventi archiviati, nella console di Amazon Fraud Detector.

Per visualizzare le metriche degli eventi memorizzate di un tipo di evento,

1. Apri laAWS console e accedi al tuo account. Accedere ad Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra, seleziona Eventi.
3. Scegliere il tipo di evento.
4. Seleziona la scheda Eventi memorizzati.
5. Nel riquadro dei dettagli degli eventi archiviati vengono visualizzate le metriche. Queste metriche vengono aggiornate automaticamente una volta al giorno.
6. Facoltativamente, fai clic su Aggiorna le metriche degli eventi per aggiornare manualmente le metriche.

> **Note**
>
> Se hai appena importato i dati, ti consigliamo di attendere 5-10 minuti dopo aver terminato l'importazione dei dati per aggiornare e visualizzare le metriche.

Orchestrazione degli eventi

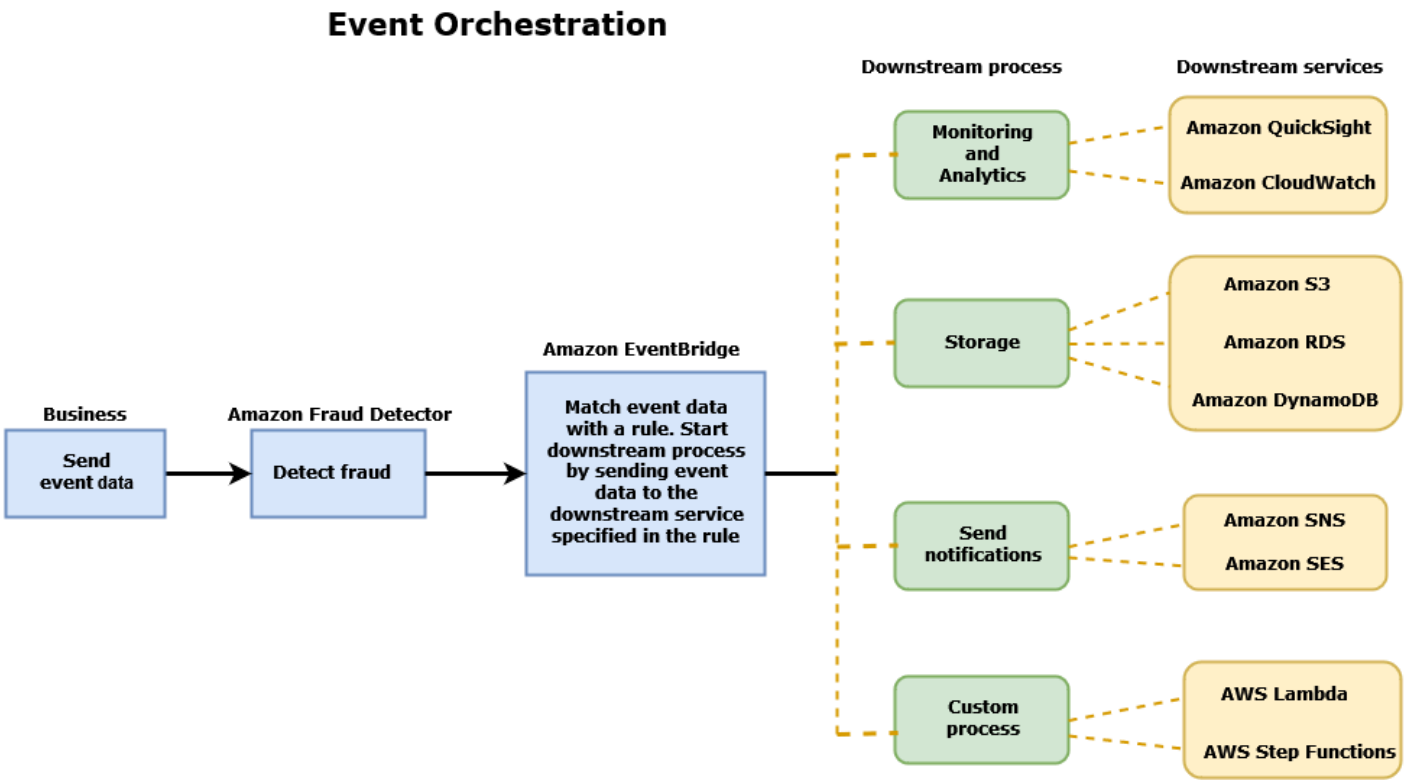
L'orchestrazione degli eventi semplifica l'invio di eventi Servizi AWS per l'elaborazione a valle, utilizzando Amazon. EventBridge Amazon Fraud Detector ti fornisce regole semplici che puoi utilizzare per automatizzare l'elaborazione degli eventi dopo il rilevamento delle frodi. Con l'orchestrazione degli eventi, puoi automatizzare i processi relativi agli eventi a valle, come l'invio di eventi alle dashboard per ottenere informazioni dai dati sugli eventi, la generazione di notifiche basate sui risultati del rilevamento delle frodi e l'aggiornamento degli eventi con un'etichetta basata su quanto appreso dal rilevamento delle frodi.

L'orchestrazione degli eventi fornisce un facile accesso ai servizi nell'AWSambiente, tramite Amazon. EventBridge Puoi configurare Amazon EventBridge per inviare eventi direttamente Servizi AWS o indirettamente utilizzando destinazioni API. I dati Servizi AWS che usi per orchestrare i processi a valle sono anche chiamati obiettivi. Alcuni degli obiettivi che è possibile utilizzare per orchestrare l'elaborazione a valle sono i seguenti:

- Per il monitoraggio e l'analisi — Amazon QuickSight, Amazon CloudWatch
- Per lo storage: Amazon S3, Amazon RDS, Amazon DynamoDB
- Per l'invio di notifiche: Amazon SNS, Amazon SES
- Per l'elaborazione personalizzata: AWS Lambda, AWS Step Functions

Per ulteriori informazioni sugli obiettivi di orchestrazione supportati da Amazon EventBridge, consulta Amazon EventBridge targets.

Il diagramma seguente fornisce una visione di alto livello di come funziona l'orchestrazione degli eventi.



Configurazione dell'orchestrazione degli eventi

La configurazione dell'orchestrazione degli eventi richiede l'impostazione dei processi nel servizio di destinazione, la configurazione di Amazon EventBridge per la ricezione e l'invio di dati sugli eventi e la creazione di regole in Amazon EventBridge che specifichino le condizioni per l'avvio dei processi downstream. Completa i seguenti passaggi per configurare l'orchestrazione degli eventi:

Per configurare l'orchestrazione degli eventi

1. Vai alla Amazon EventBridge User Guide e scopri come usare Amazon EventBridge. Assicurati di imparare a creare regole in Amazon EventBridge per il tuo caso d'uso.
2. Segui le istruzioni perAbilita l'orchestrazione degli eventi in Amazon Fraud Detector.

   > **Note**
   >
   > L'orchestrazione degli eventi per il tuo evento è disabilitata per impostazione predefinita.

3. Configura il servizio di destinazione per ricevere ed elaborare i dati dell'evento. Ad esempio, se il processo downstream prevede l'invio di notifiche e desideri utilizzare Amazon SNS, vai alla console Amazon SNS, crea un argomento SNS e quindi sottoscrivi un endpoint all'argomento.

4. Segui le istruzioni per creare EventBridge regole Amazon.

> **Important**
>
> Quando crei il modello di eventi in Amazon EventBridge, assicurati di fornire il campo `aws.frauddetector` di origine e `Event Prediction Result Returned` il campo del tipo di dettaglio.

Abilita l'orchestrazione degli eventi in Amazon Fraud Detector

Puoi abilitare l'orchestrazione degli eventi per un evento durante la creazione del tipo di evento o dopo aver creato il tipo di evento. L'orchestrazione degli eventi può essere abilitata nella console Amazon Fraud Detector, utilizzando `put-event-type` il comando, utilizzando `PutEventType` l'API o utilizzando il. AWS SDK for Python (Boto3)

Abilita l'orchestrazione degli eventi nella console Amazon Fraud Detector

Questo esempio abilita l'orchestrazione degli eventi per un tipo di evento che è già stato creato. Se state creando un nuovo tipo di evento e desiderate abilitare l'orchestrazione, seguite le istruzioni per. Crea un tipo di evento

Per abilitare l'orchestrazione degli eventi

1. Apri la console AWS di gestione e accedi al tuo account. Accedi ad Amazon Fraud Detector.
2. Nel riquadro di navigazione a sinistra, scegli Eventi.
3. Nella pagina Tipo di evento, scegli il tipo di evento.
4. Attiva Abilita l'orchestrazione degli eventi con Amazon. EventBridge
5. Continua con le istruzioni del passaggio 3 per. Configurazione dell'orchestrazione degli eventi

Abilita l'orchestrazione degli eventi utilizzando il AWS SDK for Python (Boto3)

L'esempio seguente mostra un esempio di richiesta per l'aggiornamento di un tipo di evento per `sample_registration` abilitare l'orchestrazione degli eventi. L'esempio utilizza l'`PutEventType`API e presuppone che siano state create le variabili `ip_addressemail_address`,

le etichette `legit` e `fraud` il tipo di entità. `sample_customer` Per informazioni su come creare queste risorse, consulta Risorse.

```
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'])
```

Disattiva l'orchestrazione degli eventi in Amazon Fraud Detector

Puoi disabilitare l'orchestrazione degli eventi per un evento in qualsiasi momento nella console Amazon Fraud Detector, utilizzando il `put-event-type` comando, utilizzando l'`PutEventType`API o utilizzando il. AWS SDK for Python (Boto3)

Disattiva l'orchestrazione degli eventi nella console Amazon Fraud Detector

Per disabilitare l'orchestrazione degli eventi

1. Apri la console AWS di gestione e accedi al tuo account. Accedi ad Amazon Fraud Detector.
2. Nel riquadro di navigazione a sinistra, scegli Eventi.
3. Nella pagina Tipo di evento, scegli il tipo di evento.
4. Disattiva Abilita l'orchestrazione degli eventi con Amazon. EventBridge

Disabilita l'orchestrazione degli eventi utilizzando il AWS SDK for Python (Boto3)

L'esempio seguente mostra un esempio di richiesta per l'aggiornamento di un tipo di evento per `sample_registration` disabilitare l'orchestrazione degli eventi utilizzando l'API. `PutEventType`

```
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'])
```

Modello

Amazon Fraud Detector utilizza modelli di apprendimento automatico per generare previsioni di frode. Ogni modello viene addestrato utilizzando un tipo di modello. Il tipo di modello specifica gli algoritmi e le trasformazioni utilizzati per addestrare il modello. L'addestramento del modello è il processo di utilizzo di un set di dati fornito dall'utente per creare un modello in grado di prevedere eventi fraudolenti.

Per creare un modello, è necessario innanzitutto scegliere un tipo di modello, quindi preparare e fornire i dati che verranno utilizzati per addestrare il modello.

Scegliete un tipo di modello

I seguenti tipi di modelli sono disponibili in Amazon Fraud Detector. Scegli un tipo di modello adatto al tuo caso d'uso.

- Informazioni sulle frodi online

  Il tipo di modello Online Fraud Insights è ottimizzato per rilevare le frodi quando sono disponibili pochi dati storici sull'entità oggetto della valutazione, ad esempio quando un nuovo cliente si registra online per creare un nuovo account.
- Informazioni sulle frodi transazionali

  Il tipo di modello Transaction Fraud Insights è più adatto per rilevare casi d'uso fraudolenti in cui l'entità oggetto della valutazione potrebbe avere una cronologia di interazioni che il modello può analizzare per migliorare l'accuratezza delle previsioni (ad esempio, un cliente esistente con una cronologia degli acquisti passati).
- Account Takeover Insights

  Il tipo di modello Account Takeover Insights rileva se un account è stato compromesso dal phishing o da un altro tipo di attacco. I dati di accesso di un account compromesso, come il browser e il dispositivo utilizzati al momento dell'accesso, sono diversi dai dati di accesso storici associati all'account.

Informazioni sulle frodi online

Online Fraud Insights è un modello di machine learning supervisionato, il che significa che utilizza esempi storici di transazioni fraudolente e legittime per addestrare il modello. Il modello Online Fraud Insights è in grado di rilevare le frodi sulla base di pochi dati storici. Gli input del modello sono flessibili, quindi puoi adattarlo per rilevare una serie di rischi di frode, tra cui recensioni false, abusi nelle promozioni e frodi al check-out degli ospiti.

Il modello Online Fraud Insights utilizza un insieme di algoritmi di apprendimento automatico per l'arricchimento, la trasformazione e la classificazione delle frodi dei dati. Come parte del processo di formazione del modello, Online Fraud Insights arricchisce elementi di dati grezzi come l'indirizzo IP e il numero BIN con dati di terze parti come la geolocalizzazione dell'indirizzo IP o la banca emittente di una carta di credito. Oltre ai dati di terze parti, Online Fraud Insights utilizza algoritmi di deep learning che tengono conto dei modelli di frode rilevati su Amazon eAWS. Questi modelli di frode diventano funzionalità di input per il modello utilizzando un algoritmo di potenziamento dell'albero dei gradienti.

Per aumentare le prestazioni, Online Fraud Insights ottimizza gli iperparametri dell'algoritmo di potenziamento dell'albero del gradiente tramite un processo di ottimizzazione bayesiano. Addestra in sequenza dozzine di modelli diversi con diversi parametri del modello (come il numero di alberi, la profondità degli alberi e il numero di campioni per foglia). Utilizza inoltre diverse strategie di ottimizzazione, come l'aumento di peso della popolazione minoritaria responsabile delle frodi per far fronte a tassi di frode molto bassi.

Selezione della fonte di dati

Durante l'addestramento di un modello Online Fraud Insights, puoi scegliere di addestrare il modello sui dati degli eventi archiviati esternamente (al di fuori di Amazon Fraud Detector) o archiviati all'interno di Amazon Fraud Detector. Lo storage esterno attualmente supportato da Amazon Fraud Detector è Amazon Simple Storage Service (Amazon S3). Se utilizzi uno storage esterno, il set di dati degli eventi deve essere caricato come formato di valori separati da virgole (CSV) in un bucket Amazon S3. Queste opzioni di archiviazione dei dati sono indicate nella configurazione di addestramento del modello come EXTERNAL_EVENTS (per lo storage esterno) e INGESTED_EVENTS (per lo storage interno). Per ulteriori informazioni sulle fonti di dati disponibili e su come archiviare i dati al loro interno, vedere. Archiviazione dati eventi

Preparazione dei dati

Indipendentemente da dove scegli di archiviare i dati degli eventi (Amazon S3 o Amazon Fraud Detector), i requisiti per il tipo di modello Online Fraud Insights sono gli stessi.

Il set di dati deve contenere l'intestazione della colonna EVENT_LABEL. Questa variabile classifica un evento come fraudolento o legittimo. Quando si utilizza un file CSV (archiviazione esterna), è necessario includere EVENT_LABEL per ogni evento nel file. Per l'archiviazione interna, il campo EVENT_LABEL è facoltativo, ma tutti gli eventi devono essere etichettati per essere inclusi in un set di dati di formazione. Quando configuri il modello di addestramento, puoi scegliere se ignorare gli eventi senza etichetta, assumere un'etichetta legittima per gli eventi senza etichetta o ipotizzare un'etichetta fraudolenta per tutti gli eventi senza etichetta.

Selezione dei dati

Consulta Raccogliere i dati degli eventi per informazioni sulla selezione dei dati per la formazione del modello Online Fraud Insights.

Il processo di formazione di Online Fraud Insights campiona e partiziona i dati storici in base a EVENT_TIMESTAMP. Non è necessario campionare manualmente i dati e ciò potrebbe influire negativamente sui risultati del modello.

Variabili di evento

Il modello Online Fraud Insights richiede almeno due variabili, oltre ai metadati degli eventi richiesti, che abbiano superato la convalida dei dati per l'addestramento del modello e consenta fino a 100 variabili per modello. In genere, maggiore è il numero di variabili fornite, migliore è la capacità del modello di distinguere tra frodi ed eventi legittimi. Sebbene il modello Online Fraud Insights sia in grado di supportare dozzine di variabili, incluse variabili personalizzate, consigliamo di includere l'indirizzo IP e l'indirizzo e-mail, poiché queste variabili sono in genere le più efficaci per identificare l'entità oggetto di valutazione.

Convalida dei dati

Come parte del processo di formazione, Online Fraud Insights convaliderà il set di dati per rilevare eventuali problemi di qualità dei dati che potrebbero influire sulla formazione dei modelli. Dopo aver convalidato i dati, Amazon Fraud Detector intraprenderà le azioni appropriate per creare il miglior modello possibile. Ciò include l'emissione di avvisi per potenziali problemi di qualità dei dati, la rimozione automatica delle variabili che presentano problemi di qualità dei dati o l'emissione di un errore e l'interruzione del processo di addestramento del modello. Per ulteriori informazioni, consulta Convalida del set di dati.

Informazioni sulle frodi nelle transazioni

Il tipo di modello Transaction Fraud Insights è progettato per rilevare frodi online o card-not-present relative a transazioni. Transaction Fraud Insights è un modello di apprendimento automatico supervisionato, il che significa che utilizza esempi storici di transazioni fraudolente e legittime per addestrare il modello.

Il modello Transaction Fraud Insights utilizza un insieme di algoritmi di apprendimento automatico per l'arricchimento, la trasformazione e la classificazione delle frodi dei dati. Sfrutta un motore di progettazione delle funzionalità per creare aggregati a livello di entità e a livello di evento. Come parte del processo di formazione del modello, Transaction Fraud Insights arricchisce gli elementi di dati grezzi come l'indirizzo IP e il numero BIN con dati di terze parti come la geolocalizzazione dell'indirizzo IP o la banca emittente di una carta di credito. Oltre ai dati di terze parti, Transaction Fraud Insights utilizza algoritmi di deep learning che tengono conto dei modelli di frode rilevati su Amazon e AWS questi modelli di frode diventano funzionalità di input per il tuo modello utilizzando un algoritmo di potenziamento dell'albero dei gradienti.

Per aumentare le prestazioni, Transaction Fraud Insights ottimizza gli iperparametri dell'algoritmo di potenziamento dell'albero a gradiente tramite un processo di ottimizzazione bayesiano, addestrando in sequenza dozzine di modelli diversi con diversi parametri del modello (come numero di alberi, profondità degli alberi, numero di campioni per foglia) e diverse strategie di ottimizzazione, come l'aumento di peso della popolazione minoritaria di frodi per far fronte a tassi di frode molto bassi.

Come parte del processo di formazione del modello, il motore di progettazione delle funzionalità del modello Transaction Fraud calcola i valori per ogni entità unica all'interno del set di dati di formazione per contribuire a migliorare le previsioni sulle frodi. Ad esempio, durante il processo di formazione, Amazon Fraud Detector calcola e memorizza l'ultima volta che un'entità ha effettuato un acquisto e aggiorna dinamicamente questo valore ogni volta che chiami l'API or. `GetEventPrediction` `SendEvent` Durante una previsione di frode, le variabili degli eventi vengono combinate con altri metadati di entità ed eventi per prevedere se la transazione è fraudolenta.

Selezione della fonte dei dati

I modelli Transaction Fraud Insights vengono addestrati solo su set di dati archiviati internamente con Amazon Fraud Detector (INGESTED_EVENTS). Ciò consente ad Amazon Fraud Detector di aggiornare continuamente i valori calcolati sulle entità che stai valutando. Per ulteriori informazioni sulle fonti di dati disponibili, consulta Archiviazione dati eventi

Preparazione dei dati

Prima di addestrare un modello Transaction Fraud Insights, assicurati che il file di dati contenga tutte le intestazioni, come indicato in Prepare il set di dati degli eventi. Il modello Transaction Fraud Insights confronta le nuove entità ricevute con gli esempi di entità fraudolente e legittime presenti nel set di dati, quindi è utile fornire molti esempi per ciascuna entità.

Amazon Fraud Detector trasforma automaticamente il set di dati degli eventi archiviato nel formato corretto per la formazione. Dopo che il modello ha completato l'addestramento, puoi rivedere le metriche delle prestazioni e determinare se aggiungere entità al set di dati di addestramento.

Selezione dei dati

Per impostazione predefinita, Transaction Fraud Insights si basa sull'intero set di dati archiviato per il tipo di evento selezionato. Facoltativamente, puoi impostare un intervallo di tempo per ridurre gli eventi utilizzati per addestrare il tuo modello. Quando impostate un intervallo di tempo, assicuratevi che i record utilizzati per addestrare il modello abbiano avuto un tempo sufficiente per maturare. Cioè, è trascorso abbastanza tempo per garantire che i record legittimi e fraudolenti siano stati identificati correttamente. Ad esempio, per le frodi relative ai chargeback, spesso occorrono 60 giorni o più per identificare correttamente gli eventi fraudolenti. Per ottenere le migliori prestazioni del modello, assicuratevi che tutti i record del set di dati di allenamento siano maturi.

Non è necessario selezionare un intervallo di tempo che rappresenti un tasso di frode ideale. Amazon Fraud Detector campiona automaticamente i dati per raggiungere un equilibrio tra tassi di frode, intervallo di tempo e numero di entità.

Amazon Fraud Detector restituisce un errore di convalida durante l'addestramento del modello se selezioni un intervallo di tempo per il quale non ci sono abbastanza eventi per addestrare correttamente un modello. Per i set di dati memorizzati, il campo EVENT_LABEL è facoltativo, ma gli eventi devono essere etichettati per essere inclusi nel set di dati di addestramento. Quando configuri il modello di addestramento, puoi scegliere se ignorare gli eventi senza etichetta, assumere un'etichetta legittima per gli eventi senza etichetta o assumere un'etichetta fraudolenta per gli eventi senza etichetta.

Variabili di evento

Il tipo di evento utilizzato per addestrare il modello deve contenere almeno 2 variabili, oltre ai metadati degli eventi richiesti, che hanno superato la convalida dei dati e possono contenere fino a 100 variabili. In genere, maggiore è il numero di variabili fornite, migliore è la capacità del modello di distinguere tra frodi ed eventi legittimi. Sebbene il modello Transaction Fraud Insight possa

supportare dozzine di variabili, incluse variabili personalizzate, ti consigliamo di includere l'indirizzo IP, l'indirizzo email, il tipo di strumento di pagamento, il prezzo dell'ordine e il BIN della carta.

Convalida dei dati

Come parte del processo di formazione, Transaction Fraud Insights convalida il set di dati di formazione per problemi di qualità dei dati che potrebbero influire sulla formazione dei modelli. Dopo aver convalidato i dati, Amazon Fraud Detector intraprende le azioni appropriate per creare il miglior modello possibile. Ciò include l'emissione di avvisi per potenziali problemi di qualità dei dati, la rimozione automatica delle variabili che presentano problemi di qualità dei dati o l'emissione di un errore e l'interruzione del processo di addestramento del modello. Per ulteriori informazioni, vedere Convalida del set di dati.

Amazon Fraud Detector emetterà un avviso ma continuerà ad addestrare un modello se il numero di entità uniche è inferiore a 1.500, poiché ciò può influire sulla qualità dei dati di addestramento. Se ricevi un avviso, esamina la metrica delle prestazioni.

Informazioni sull'acquisizione dell'account

Il tipo di modello Account Takeover Insights (ATI) identifica le attività online fraudolente rilevando se gli account sono stati compromessi a seguito di acquisizioni dolose, phishing o furto di credenziali. Account Takeover Insights è un modello di apprendimento automatico che utilizza gli eventi di accesso della tua attività online per addestrare il modello.

Puoi incorporare un modello Account Takeover Insights addestrato nel flusso di accesso in tempo reale per rilevare se un account è compromesso. Il modello valuta una varietà di tipi di autenticazione e accesso. Includono accessi alle applicazioni Web, autenticazioni basate su API e (SSO). single-sign-on Per utilizzare il modello Account Takeover Insights, chiama l'GetEventPredictionAPI dopo aver fornito credenziali di accesso valide. L'API genera un punteggio che quantifica il rischio di compromissione dell'account. Amazon Fraud Detector utilizza il punteggio e le regole che hai definito per restituire uno o più risultati per gli eventi di accesso. I risultati sono quelli che hai configurato. In base ai risultati ricevuti, puoi intraprendere le azioni appropriate per ogni accesso. Cioè, puoi approvare o contestare le credenziali presentate per l'accesso. Ad esempio, puoi contestare le credenziali chiedendo il PIN dell'account come verifica aggiuntiva.

Puoi anche utilizzare il modello Account Takeover Insights per valutare gli accessi agli account in modo asincrono e intraprendere azioni sugli account ad alto rischio. Ad esempio, è possibile aggiungere un account ad alto rischio alla coda di indagine per consentire a un revisore umano di determinare se sono necessarie ulteriori azioni, come sospendere l'account.

Il modello Account Takeover Insights viene addestrato utilizzando un set di dati che contiene gli eventi di accesso storici della tua azienda. Questi dati sono forniti dall'utente. Facoltativamente, puoi etichettare gli account come legittimi o fraudolenti. Tuttavia, ciò non è necessario per addestrare il modello. Il modello Account Takeover Insights rileva le anomalie in base alla cronologia degli accessi riusciti di un account. Impara inoltre a rilevare anomalie nel comportamento di un utente che suggeriscono un aumento del rischio di un evento di acquisizione dolosa dell'account. Ad esempio, un utente che in genere accede dallo stesso set di dispositivi e indirizzi IP. Un truffatore in genere accede da un dispositivo e da una geolocalizzazione diversi. Questa tecnica genera un punteggio di rischio relativo all'anomalia di un'attività, che in genere è una caratteristica principale delle acquisizioni dolose di account.

Prima di addestrare un modello Account Takeover Insights, Amazon Fraud Detector utilizza una combinazione di tecniche di apprendimento automatico per eseguire l'arricchimento, l'aggregazione e la trasformazione dei dati. Quindi, durante il processo di formazione, Amazon Fraud Detector arricchisce gli elementi di dati grezzi che fornisci. Esempi di elementi di dati grezzi includono l'indirizzo IP e lo user agent. Amazon Fraud Detector utilizza questi elementi per creare input aggiuntivi che descrivono i dati di accesso. Questi input includono gli input del dispositivo, del browser e della geolocalizzazione. Amazon Fraud Detector utilizza anche i dati di accesso che fornisci per calcolare continuamente variabili aggregate che descrivono il comportamento passato degli utenti. Esempi di comportamento dell'utente includono il numero di volte in cui l'utente ha effettuato l'accesso da un indirizzo IP specifico. Utilizzando questi arricchimenti e aggregati aggiuntivi, Amazon Fraud Detector può generare ottime prestazioni del modello da un piccolo set di input dai tuoi eventi di accesso.

Il modello Account Takeover Insights rileva i casi in cui un malintenzionato accede a un account legittimo, indipendentemente dal fatto che il malintenzionato sia umano o robot. Il modello produce un singolo punteggio che indica il rischio relativo di compromissione dell'account. Gli account che potrebbero essere stati compromessi vengono contrassegnati come account ad alto rischio. È possibile elaborare gli account ad alto rischio in due modi. In entrambi i casi, puoi imporre un'ulteriore verifica dell'identità. In alternativa, puoi mettere l'account in coda per un'indagine manuale.

Selezione della fonte di dati

I modelli Account Takeover Insights vengono addestrati su un set di dati archiviato internamente, in Amazon Fraud Detector. Per archiviare i dati degli eventi di accesso con Amazon Fraud Detector, crea un file CSV con gli eventi di accesso degli utenti. Per ogni evento, includi dati di accesso come data e ora dell'evento, ID utente, indirizzo IP, agente utente e verifica se i dati di accesso sono validi. Dopo aver creato il file CSV, carica prima il file su Amazon Fraud Detector, quindi utilizza la

funzionalità di importazione per archiviare i dati. Puoi quindi addestrare il tuo modello utilizzando i dati memorizzati. Per ulteriori informazioni sull'archiviazione del set di dati degli eventi con Amazon Fraud Detector, consulta Archivia i dati degli eventi internamente con Amazon Fraud Detector

Preparazione dei dati

Amazon Fraud Detector richiede che tu fornisca i dati di accesso al tuo account utente in un file con valori separati da virgole (CSV) codificato nel formato UTF-8. La prima riga del file CSV deve contenere un'intestazione del file. L'intestazione del file è composta da metadati di eventi e variabili di evento che descrivono ogni elemento di dati. I dati dell'evento seguono l'intestazione. Ogni riga dei dati dell'evento è costituita dai dati di un singolo evento di accesso.

Per il modello Accounts Takeover Insights, è necessario fornire i seguenti metadati e variabili di evento nella riga di intestazione del file CSV.

Metadati degli eventi

Ti consigliamo di fornire i seguenti metadati nell'intestazione del file CSV. I metadati dell'evento devono essere in lettere maiuscole.

- EVENT_ID - Un identificatore univoco per l'evento di accesso.
- ENTITY_TYPE - L'entità che esegue l'evento di accesso, ad esempio un commerciante o un cliente.
- ENTITY_ID - Un identificatore per l'entità che esegue l'evento di accesso.
- EVENT_TIMESTAMP - Il timestamp in cui si è verificato l'evento di accesso. Il timestamp deve essere conforme allo standard ISO 8601 in UTC.
- EVENT_LABEL (consigliato): un'etichetta che classifica l'evento come fraudolento o legittimo. Puoi utilizzare qualsiasi etichetta, come «fraudolenta», «legittima», «1" o «0".

> **Note**
>
> - I metadati degli eventi devono essere in lettere maiuscole. Fa differenza tra maiuscole e minuscole
> - Le etichette non sono richieste per gli eventi di accesso. Tuttavia, ti consigliamo di includere i metadati EVENT_LABEL e di fornire etichette per i tuoi eventi di accesso. Va bene se le etichette sono incomplete o sporadiche. Se fornisci etichette, Amazon Fraud

Detector le utilizzerà per calcolare automaticamente un Account Takeover Discovery Rate e visualizzarlo nel grafico e nella tabella delle prestazioni del modello.

Variabili di evento

Per il modello Accounts Takeover Insights, ci sono sia variabili obbligatorie (obbligatorie) che è necessario fornire sia variabili facoltative. Quando create le variabili, assicuratevi di assegnare la variabile al tipo di variabile corretto. Come parte del processo di formazione del modello, Amazon Fraud Detector utilizza il tipo di variabile associato alla variabile per eseguire l'arricchimento delle variabili e l'ingegnerizzazione delle funzionalità.

> **Note**
>
> I nomi delle variabili di evento devono essere in lettere minuscole. Sono sensibili alle maiuscole.

Variabili obbligatorie

Le seguenti variabili sono necessarie per la formazione di un modello Accounts Takeover Insights.

Categoria	Tipo di variabile	Descrizione
Indirizzo IP	IP_ADDRESS	L'indirizzo IP utilizzato nell'evento di accesso
Browser e dispositivo	AGENTE UTENTE	Il browser, il dispositivo e il sistema operativo utilizzati nell'evento di accesso
Credenziali valide	CARTA DI CREDITO VALIDA	Indica se le credenziali utilizzate per l'accesso sono valide

Variabili opzionali

Le seguenti variabili sono opzionali per la formazione di un modello Accounts Takeover Insights.

Categoria	Type	Descrizione
Browser e dispositivo	IMPRONTA DIGITALE	L'identificatore univoco dell'impronta digitale del browser o del dispositivo
ID della sessione	SESSION_ID	L'identificatore per una sessione di autenticazione
Etichetta	EVENT_LABEL	Un'etichetta che classific a l'evento come fraudolen to o legittimo. Puoi utilizzar e qualsiasi etichetta, come «frode», «legittimo», «1" o «0".
Timestamp	LABEL_TIMESTAMP	Il timestamp dell'ultimo aggiornamento dell'etichetta. Questo è necessario se viene fornito EVENT_LABEL.

Note

- È possibile fornire qualsiasi nome di variabile per entrambe le variabili obbligatorie (variabili opzionali). È importante che ogni variabile obbligatoria e facoltativa sia assegnata al tipo di variabile corretto.
- Puoi fornire variabili aggiuntive. Tuttavia, Amazon Fraud Detector non includerà queste variabili per la formazione di un modello Accounts Takeover Insights.

Selezione dei dati

La raccolta di dati è un passaggio importante per creare il modello Account Takeover Insights. Quando inizi a raccogliere i tuoi dati di accesso, prendi in considerazione i seguenti requisiti e consigli:

Campo obbligatorio

- Fornisci almeno 1.500 esempi di account utente, ciascuno con almeno due eventi di accesso associati.
- Il set di dati deve coprire almeno 30 giorni di eventi di accesso. Successivamente è possibile specificare l'intervallo di tempo specifico degli eventi da utilizzare per addestrare il modello.

Consigliato

- Il set di dati include esempi di eventi di accesso non riusciti. Facoltativamente, puoi etichettare questi accessi non riusciti come «fraudolenti» o «legittimi».
- Prepara i dati storici con eventi di accesso che durano più di sei mesi e includi 100.000 entità.

Se non disponi di un set di dati che soddisfi già i requisiti minimi, valuta la possibilità di trasmettere i dati degli eventi ad Amazon Fraud Detector chiamando SendEventl'operatore dell'API.

Convalida dei dati

Prima di creare il modello Account Takeover Insights, Amazon Fraud Detector verifica se i metadati e le variabili che hai incluso nel set di dati per l'addestramento del modello soddisfano i requisiti di dimensione e formato. Per ulteriori informazioni, consulta Convalida del set di dati. Verifica anche la presenza di altri requisiti. Se il set di dati non supera la convalida, il modello non viene creato. Affinché il modello venga creato correttamente, assicurati di correggere i dati che non hanno superato la convalida prima di eseguire nuovamente l'addestramento.

Errori comuni dei set di dati

Durante la convalida di un set di dati per l'addestramento di un modello Account Takeover Insights, Amazon Fraud Detector analizza questi e altri problemi e genera un errore se riscontra uno o più problemi.

- Il file CSV non è in formato UTF-8.
- L'intestazione del file CSV non contiene almeno uno dei seguenti metadati:, o. `EVENT_ID` `ENTITY_ID` `EVENT_TIMESTAMP`
- L'intestazione del file CSV non contiene almeno una variabile dei seguenti tipi di variabili:, o. `IP_ADDRESS` `USERAGENT` `VALIDCRED`
- Esiste più di una variabile associata allo stesso tipo di variabile.
- Oltre lo 0,1% dei valori `EVENT_TIMESTAMP` contiene valori null o valori diversi dai formati di data e ora supportati.

- Il numero di giorni tra il primo e l'ultimo evento è inferiore a 30 giorni.
- Più del 10% delle variabili del tipo di `IP_ADDRESS` variabile non sono valide o sono nulle.
- Oltre il 50% delle variabili del tipo di `USERAGENT` variabile contiene valori null.
- Tutte le variabili del tipo di `VALIDCRED` variabile sono impostate su. `false`

Crea un modello

I modelli Amazon Fraud Detector imparano a rilevare le frodi per un tipo di evento specifico. In Amazon Fraud Detector, devi prima creare un modello che funge da contenitore per le versioni del tuo modello. Ogni volta che si addestra un modello, viene creata una nuova versione. Per i dettagli su come creare e addestrare un modello utilizzando la AWS Console, consultaFase 3: Creazione del modello.

Ogni modello ha una variabile di punteggio del modello corrispondente. Amazon Fraud Detector crea questa variabile per tuo conto quando crei un modello. Puoi utilizzare questa variabile nelle espressioni delle regole per interpretare i punteggi del modello durante una valutazione delle frodi.

Addestra e distribuisci un modello utilizzando il AWS SDK for Python (Boto3)

Una versione del modello viene creata chiamando le `CreateModelVersion` operazioni `CreateModel` and. `CreateModel`avvia il modello, che funge da contenitore per le versioni del modello. `CreateModelVersion`avvia il processo di addestramento, che si traduce in una versione specifica del modello. Una nuova versione della soluzione viene creata ogni volta che si richiama `CreateModelVersion`.

L'esempio seguente mostra un esempio di richiesta per l'`CreateModel`API. Questo esempio crea un tipo di modello Online Fraud Insights e presuppone che tu abbia creato un tipo di `sample_registration` evento. Per ulteriori dettagli sulla creazione di un tipo di evento, vedereCrea un tipo di evento.

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

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

```
modelType = 'ONLINE_FRAUD_INSIGHTS')
```

Addestra la tua prima versione utilizzando l'CreateModelVersionAPI. Per il `TrainingDataSource` e `ExternalEventsDetail` specifica l'origine e la posizione in Amazon S3 del set di dati di addestramento. Per `TrainingDataSchema` specificare come Amazon Fraud Detector deve interpretare i dati di addestramento, in particolare quali variabili di evento includere e come classificare le etichette degli eventi. Per impostazione predefinita, Amazon Fraud Detector ignora gli eventi senza etichetta. Questo codice di esempio utilizza `AUTO` for `unlabeledEventsTreatment` per specificare che Amazon Fraud Detector decide come utilizzare gli eventi senza etichetta.

```
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'
}
)
```

Una richiesta andata a buon fine produrrà una nuova versione del modello con stato. `TRAINING_IN_PROGRESS` In qualsiasi momento durante il corso di formazione, puoi annullarlo chiamando `UpdateModelVersionStatus` e aggiornando lo stato a`TRAINING_CANCELLED`. Una volta completato l'addestramento, lo stato della versione del modello verrà aggiornato a`TRAINING_COMPLETE`. Puoi esaminare le prestazioni del modello utilizzando la console Amazon Fraud Detector o chiamando. `DescribeModelVersions` Per ulteriori informazioni su come

interpretare i punteggi e le prestazioni dei modelli, consulta Punteggi del modello eMetriche delle prestazioni del modello.

Dopo aver esaminato le prestazioni del modello, attivalo per renderlo disponibile ai rilevatori per le previsioni di frode in tempo reale. Amazon Fraud Detector distribuirà il modello in più zone di disponibilità per la ridondanza con l'auto-scaling attivato per garantire che il modello si adatti al numero di previsioni di frode che stai facendo. Per attivare il modello, chiama l'API e aggiorna lo stato a. `UpdateModelVersionStatus` `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'
)
```

Punteggi del modello

Amazon Fraud Detector genera punteggi di modello in modo diverso a seconda dei diversi tipi di modello.

Per i modelli Account Takeover Insights (ATI), Amazon Fraud Detector utilizza solo il valore aggregato (un valore calcolato combinando un insieme di variabili non elaborate) per generare il punteggio del modello. Viene generato un punteggio di -1 per il primo evento di una nuova entità, che indica un rischio sconosciuto. Questo perché per una nuova entità, i valori utilizzati per il calcolo dell'aggregato saranno zero o nulli. Il modello Account Takeeeover Insights (ATI) genera punteggi del modello compresi tra 0 e 1000 per tutti gli eventi successivi per la stessa entità e per le entità esistenti, dove 0 indica un basso rischio di frode e 1000 indica un rischio di frode elevato. Per i modelli ATI, i punteggi dei modelli sono direttamente correlati al tasso di sfida (CR). Ad esempio, un punteggio di 500 corrisponde a un tasso di sfida stimato del 5%, mentre un punteggio di 900 corrisponde a un tasso di sfida stimato dello 0,1%.

Per i modelli Online Fraud Insights (OFI) e Transaction Fraud Insights (TFI), Amazon Fraud Detector utilizza sia il valore aggregato (un valore calcolato combinando un insieme di variabili non elaborate) che il valore non elaborato (il valore fornito per la variabile) per generare i punteggi del modello. I punteggi del modello possono essere compresi tra 0 e 1000, dove 0 indica un basso rischio di

frode e 1000 indica un rischio di frode elevato. Per i modelli OFI e TFI, i punteggi dei modelli sono direttamente correlati al tasso di falsi positivi (FPR). Ad esempio, un punteggio di 600 corrisponde a un tasso di falsi positivi stimato del 10%, mentre un punteggio di 900 corrisponde a un tasso di falsi positivi stimato del 2%. La tabella seguente fornisce dettagli sulla correlazione di determinati punteggi del modello con i tassi di falsi positivi stimati.

Punteggio del modello	FPR stimato
975	0,50%
950	1%
900	2%
860	3%
775	5%
700	7%
600	10%

Metriche delle prestazioni del modello

Una volta completata la formazione del modello, Amazon Fraud Detector convalida le prestazioni del modello utilizzando il 15% dei dati che non sono stati utilizzati per addestrare il modello. Puoi aspettarti che il tuo modello Amazon Fraud Detector addestrato abbia prestazioni di rilevamento delle frodi reali simili alle metriche delle prestazioni di convalida.

Come azienda, devi trovare un equilibrio tra l'individuazione di un maggior numero di frodi e l'aumento delle difficoltà nei confronti dei clienti legittimi. Per aiutarti a scegliere il giusto equilibrio, Amazon Fraud Detector fornisce i seguenti strumenti per valutare le prestazioni del modello:

- Grafico di distribuzione dei punteggi: un istogramma delle distribuzioni dei punteggi del modello presuppone una popolazione di esempio di 100.000 eventi. L'asse Y sinistro rappresenta gli eventi legittimi e l'asse Y destro rappresenta gli eventi di frode. È possibile selezionare una soglia specifica del modello facendo clic sull'area del grafico. Ciò aggiornerà le viste corrispondenti nella matrice di confusione e nel grafico ROC.

- Matrice di confusione: riassume l'accuratezza del modello per una determinata soglia di punteggio confrontando le previsioni del modello con i risultati effettivi. Amazon Fraud Detector presuppone una popolazione di esempio di 100.000 eventi. La distribuzione di frodi ed eventi legittimi simula il tasso di frode nelle tue aziende.
  - Veri aspetti positivi: il modello prevede le frodi e l'evento è in realtà una frode.
  - Falsi positivi: il modello prevede la frode, ma l'evento è in realtà legittimo.
  - Veri aspetti negativi: il modello prevede che l'evento sia legittimo e l'evento è effettivamente legittimo.
  - Falsi negativi: il modello prevede che l'evento sia legittimo, ma in realtà si tratta di una frode.
  - Tasso di vera positività (TPR): percentuale della frode totale rilevata dal modello. Conosciuto anche come tasso di acquisizione.
  - Percentuale di falsi positivi (FPR): percentuale del totale di eventi legittimi erroneamente previsti come frodi.
- Receiver Operator Curve (ROC): traccia il tasso di veri positivi in funzione del tasso di falsi positivi su tutte le possibili soglie di punteggio del modello. Visualizza questo grafico scegliendo Advanced Metrics.
- Area sotto la curva (AUC): riassume TPR e FPR in tutte le possibili soglie di punteggio del modello. Un modello senza potere predittivo ha un AUC di 0,5, mentre un modello perfetto ha un punteggio di 1,0.
- Intervallo di incertezza: mostra l'intervallo di AUC previsto dal modello. Un intervallo più ampio (differenza tra il limite superiore e inferiore dell'AUC > 0,1) significa una maggiore incertezza del modello. Se l'intervallo di incertezza è ampio (>0,1), valuta la possibilità di fornire più eventi etichettati e riqualifica il modello.

Per utilizzare le metriche delle prestazioni del modello

1. Inizia con la tabella di distribuzione dei punteggi per esaminare la distribuzione dei punteggi dei modelli relativi a frodi ed eventi legittimi. Idealmente, avrai una netta separazione tra frode ed eventi legittimi. Ciò indica che il modello è in grado di identificare con precisione quali eventi sono fraudolenti e quali sono legittimi. Seleziona una soglia del modello facendo clic sull'area del grafico. Puoi vedere come la modifica della soglia di punteggio del modello influisce sui tassi di veri positivi e falsi positivi.

> **Note**
>
> Il grafico di distribuzione dei punteggi riporta le frodi e gli eventi legittimi su due diversi assi Y. L'asse Y sinistro rappresenta gli eventi legittimi e l'asse Y destro rappresenta gli eventi di frode.

2. Esamina la matrice di confusione. A seconda della soglia di punteggio del modello selezionata, puoi vedere l'impatto simulato sulla base di un campione di 100.000 eventi. La distribuzione di frodi ed eventi legittimi simula il tasso di frode nelle vostre aziende. Utilizzate queste informazioni per trovare il giusto equilibrio tra il tasso di veri positivi e il tasso di falsi positivi.
3. Per ulteriori dettagli, scegli Advanced Metrics. Utilizza il grafico ROC per comprendere la relazione tra il tasso di veri positivi e il tasso di falsi positivi per qualsiasi soglia di punteggio del modello. La curva ROC può aiutarti a perfezionare il compromesso tra tasso di vero positivo e tasso di falsi positivi.

> **Note**
>
> Puoi anche rivedere le metriche sotto forma di tabella scegliendo Tabella.
> La visualizzazione della tabella mostra anche la precisione della metrica. La precisione è la percentuale di eventi di frode correttamente previsti come fraudolenti rispetto a tutti gli eventi previsti come fraudolenti.

4. Utilizza le metriche delle prestazioni per determinare le soglie del modello ottimali per le tue attività in base ai tuoi obiettivi e al caso d'uso del rilevamento delle frodi. Ad esempio, se prevedi di utilizzare il modello per classificare le nuove registrazioni di account come ad alto, medio o basso rischio, devi identificare due punteggi di soglia in modo da poter redigere le tre condizioni delle regole seguenti:

   - I punteggi > X sono ad alto rischio
   - I punteggi < X but > Y sono a rischio medio
   - I punteggi < Y sono a basso rischio

Importanza della variabile del modello

L'importanza delle variabili del modello è una funzionalità di Amazon Fraud Detector che classifica le variabili del modello all'interno di una versione del modello. A ogni variabile del modello viene

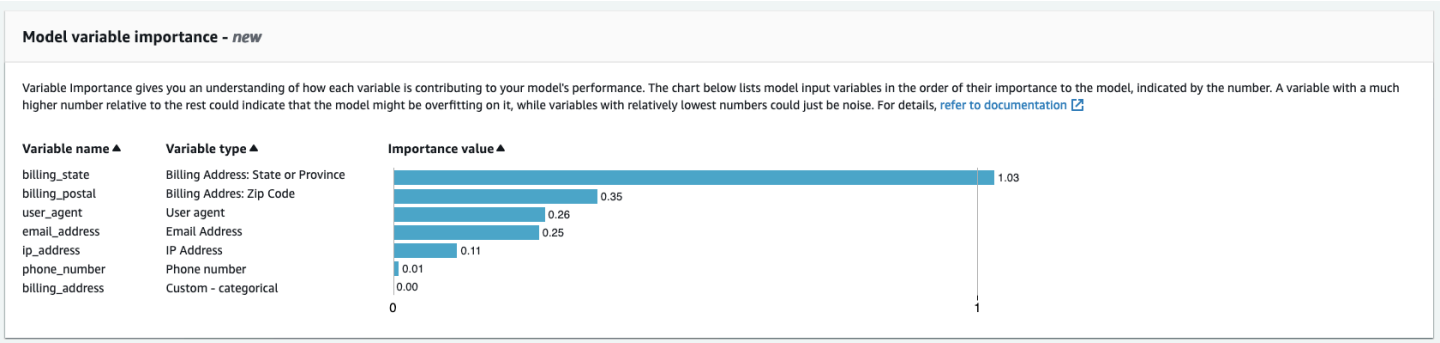
assegnato un valore basato sulla sua importanza relativa per le prestazioni complessive del modello. La variabile di modello con il valore più alto è più importante per il modello rispetto alle altre variabili di modello nel set di dati per quella versione del modello ed è elencata in alto per impostazione predefinita. Allo stesso modo, la variabile di modello con il valore più basso è elencata in basso per impostazione predefinita ed è meno importante rispetto alle altre variabili del modello. Utilizzando i valori di importanza delle variabili del modello, è possibile ottenere informazioni dettagliate su quali input determinano le prestazioni del modello.

Puoi visualizzare i valori di importanza delle variabili del modello per la versione del modello addestrato nella console Amazon Fraud Detector o utilizzando l'DescribeModelVersionAPI.

L'importanza delle variabili del modello fornisce il seguente set di valori per ogni variabile utilizzata per addestrare la versione del modello.

- Tipo di variabile: tipo di variabile (ad esempio, indirizzo IP o e-mail). Per ulteriori informazioni, consulta Tipi variabili. Per i modelli Account Takeover Insights (ATI), Amazon Fraud Detector fornisce un valore di importanza variabile sia per il tipo di variabile grezza che aggregata. I tipi di variabili non elaborati vengono assegnati alle variabili fornite. Il tipo di variabile aggregata viene assegnato a un insieme di variabili non elaborate che Amazon Fraud Detector ha combinato per calcolare un valore di importanza aggregato.
- Nome variabile: nome della variabile di evento utilizzata per addestrare la versione del modello (ad esempio,`ip_address`,`email_address`). `are_creadentials_valid` Per il tipo di variabile aggregata, vengono elencati i nomi di tutte le variabili utilizzate per calcolare il valore di importanza della variabile aggregata.
- Valore di importanza variabile: un numero che rappresenta l'importanza relativa della variabile grezza o aggregata per le prestazioni del modello. Intervallo tipico: 0-10

Nella console Amazon Fraud Detector, i valori di importanza delle variabili del modello vengono visualizzati come segue per un modello Online Fraud Insights (OFI) o un modello Transaction Fraud Insights (TFI). Un modello Account Takeover Insight (ATI) fornirà valori di importanza variabili aggregati oltre ai valori di importanza della variabile grezza. Il grafico grafico semplifica la visualizzazione dell'importanza relativa tra le variabili, con la linea tratteggiata verticale che fa riferimento al valore di importanza della variabile con il punteggio più alto.



Amazon Fraud Detector genera valori di importanza variabili per ogni versione del modello Fraud Detector senza costi aggiuntivi.

> **Important**
>
> Le versioni dei modelli create prima del 9 luglio 2021 non hanno valori di importanza variabili. È necessario addestrare una nuova versione del modello per generare i valori di importanza delle variabili del modello.

Utilizzo dei valori di importanza delle variabili del modello

È possibile utilizzare i valori di importanza delle variabili del modello per ottenere informazioni dettagliate su cosa aumenta o diminuisce le prestazioni del modello e su quali variabili vi contribuisce maggiormente. Quindi modifica il modello per migliorare le prestazioni complessive.

Più specificamente, per migliorare le prestazioni del modello, esaminate i valori di importanza delle variabili rispetto alle conoscenze del dominio ed eseguite il debug dei problemi nei dati di addestramento. Ad esempio, se l'ID account è stato utilizzato come input per il modello ed è elencato in alto, dai un'occhiata al suo valore di importanza variabile. Se il valore di importanza della variabile è significativamente più alto rispetto al resto dei valori, il modello potrebbe adattarsi eccessivamente a uno specifico modello di frode (ad esempio, tutti gli eventi di frode provengono dallo stesso ID account). Tuttavia, è possibile che si verifichi una perdita di etichetta se la variabile dipende dalle etichette antifrode. A seconda del risultato dell'analisi basata sulla conoscenza del dominio, potresti voler rimuovere la variabile e addestrarla con un set di dati più diversificato o mantenere il modello così com'è.

Allo stesso modo, dai un'occhiata alle variabili classificate per ultime. Se il valore di importanza della variabile è significativamente inferiore rispetto al resto dei valori, questa variabile del modello

potrebbe non avere alcuna importanza nell'addestramento del modello. Potresti prendere in considerazione la rimozione della variabile per addestrare una versione del modello più semplice. Se il tuo modello ha poche variabili, ad esempio solo due variabili, Amazon Fraud Detector fornisce comunque i valori di importanza delle variabili e classifica le variabili. Tuttavia, le informazioni in questo caso saranno limitate.

⚠ Important

1. Se noti che mancano delle variabili nella tabella di importanza delle variabili del modello, ciò potrebbe essere dovuto a uno dei seguenti motivi. Valuta la possibilità di modificare la variabile nel set di dati e riqualificare il modello.
   - Il numero di valori univoci per la variabile nel set di dati di addestramento è inferiore a 100.
   - Nel set di dati di addestramento mancano più dello 0,9 dei valori della variabile.
2. È necessario addestrare una nuova versione del modello ogni volta che si desidera modificare le variabili di input del modello.

Valutazione dei valori di importanza delle variabili del modello

Si consiglia di considerare quanto segue quando si valutano i valori di importanza delle variabili del modello:

- I valori di importanza variabile devono sempre essere valutati in combinazione con la conoscenza del dominio.
- Esamina il valore di importanza variabile di una variabile rispetto al valore di importanza variabile delle altre variabili all'interno della versione del modello. Non considerate il valore di importanza variabile per una singola variabile in modo indipendente.
- Confronta i valori di importanza variabile delle variabili all'interno della stessa versione del modello. Non confrontate i valori di importanza variabile delle stesse variabili tra le versioni del modello, poiché il valore di importanza variabile di una variabile in una versione del modello potrebbe differire dal valore della stessa variabile in una versione del modello diversa. Se si utilizzano le stesse variabili e lo stesso set di dati per addestrare diverse versioni del modello, ciò non genera necessariamente gli stessi valori di importanza variabile.

Visualizzazione della classificazione di importanza variabile del modello

Una volta completata la formazione del modello, puoi visualizzare la classificazione a importanza variabile del modello della versione del modello addestrato nella console Amazon Fraud Detector o utilizzando l'DescribeModelVersionAPI.

Per visualizzare la classificazione dell'importanza variabile del modello utilizzando la console,

1. Apri la AWS console e accedi al tuo account. Accedi ad Amazon Fraud Detector.
2. Nel riquadro di navigazione a sinistra scegliere Models (Modelli).
3. Scegli il modello e poi la versione del modello.
4. Assicurati che la scheda Panoramica sia selezionata.
5. Scorri verso il basso per visualizzare il riquadro di importanza della variabile del modello.

Comprendere come viene calcolato il valore di importanza della variabile del modello

Al completamento di ogni formazione sulla versione del modello, Amazon Fraud Detector genera automaticamente i valori di importanza delle variabili del modello e le metriche delle prestazioni del modello. Per questo, Amazon Fraud Detector utilizza Shapley Additive Explanations (SHAP). SHAP è essenzialmente il contributo medio previsto di una variabile del modello dopo aver considerato tutte le possibili combinazioni di tutte le variabili del modello.

SHAP assegna innanzitutto il contributo di ciascuna variabile del modello per la previsione di un evento. Quindi, aggrega queste previsioni per creare una classifica delle variabili a livello di modello. Per assegnare i contributi di ciascuna variabile del modello per una previsione, SHAP considera le differenze nei risultati del modello tra tutte le possibili combinazioni di variabili. Includendo tutte le possibilità di includere o rimuovere set specifici di variabili per generare un output del modello, SHAP può accedere con precisione all'importanza di ciascuna variabile del modello. Ciò è particolarmente importante quando le variabili del modello sono altamente correlate tra loro.

I modelli ML, nella maggior parte dei casi, non consentono di rimuovere variabili. È invece possibile sostituire una variabile rimossa o mancante nel modello con i valori delle variabili corrispondenti di una o più linee di base (ad esempio, eventi non fraudolenti). La scelta delle istanze di base appropriate può essere difficile, ma Amazon Fraud Detector semplifica questa operazione impostando questa linea di base come media della popolazione per te.

Importa un modello SageMaker

Facoltativamente, puoi importare modelli SageMaker ospitati in Amazon Fraud Detector. Analogamente ai modelli, SageMaker i modelli possono essere aggiunti ai rilevatori e generare previsioni di frode utilizzando l'API. `GetEventPrediction` Come parte della `GetEventPrediction` richiesta, Amazon Fraud Detector richiamerà il tuo SageMaker endpoint e passerà i risultati alle tue regole.

Puoi configurare Amazon Fraud Detector per utilizzare le variabili di evento inviate come parte della `GetEventPrediction` richiesta. Se scegli di utilizzare variabili di evento, devi fornire un modello di input. Amazon Fraud Detector utilizzerà questo modello per trasformare le variabili degli eventi nel payload di input richiesto per richiamare l'endpoint. SageMaker In alternativa, puoi configurare il tuo SageMaker modello per utilizzare un ByteBuffer inviato come parte della richiesta. `GetEventPrediction`

Amazon Fraud Detector supporta SageMaker algoritmi di importazione che utilizzano formati di input JSON o CSV e formati di output JSON o CSV. Esempi di SageMaker algoritmi supportati includono XGBoost, Linear Learner e Random Cut Forest.

Importa un modello utilizzando il SageMaker AWS SDK for Python (Boto3)

Per importare un SageMaker modello, utilizza l'`PutExternalModel`API. L'esempio seguente presuppone che l' SageMaker endpoint sia `sagemaker-transaction-model` stato distribuito, sia in stato e utilizzi l'`InService`algoritmo XGBoost.

La configurazione di input specifica che utilizzerà le variabili di evento per costruire l'input del modello (è impostato su). `useEventVariables` `TRUE` Il formato di input è TEXT_CSV, dato che XGBoost richiede un input CSV. csvInputTemplate Specificano come costruire l'input CSV dalle variabili inviate come parte della richiesta. `GetEventPrediction` Questo esempio presuppone che tu abbia creato le variabili`order_amt`, e. `prev_amt` `hist_amt` `payment_type`

La configurazione di output specifica il formato di risposta del SageMaker modello e associa l'indice CSV appropriato alla variabile Amazon Fraud Detector. `sagemaker_output_score` Una volta configurata, puoi utilizzare la variabile di output nelle regole.

> **Note**
>
> L'output di un SageMaker modello deve essere mappato su una variabile con sorgente`EXTERNAL_MODEL_SCORE`. Non è possibile creare queste variabili nella console

utilizzando Variables. È invece necessario crearle quando si configura l'importazione del modello.

```
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'
)
```

Eliminazione di un modello o una versione del modello

Puoi eliminare modelli e versioni di modello in Amazon Fraud Detector, a condizione che non siano associati a una versione del rilevatore. Quando elimini un modello, Amazon Fraud Detector elimina definitivamente quel modello e i dati non vengono più archiviati in Amazon Fraud Detector.

Puoi anche rimuovere SageMaker modelli Amazon se non sono associati a una versione del rilevatore. La rimozione di un SageMaker modello lo disconnette da Amazon Fraud Detector, ma il modello rimane disponibile in SageMaker.

Per eliminare una versione del modello

È possibile eliminare solo le versioni del modello che si trovano nello`Ready to deploy` stato. Per modificare`Ready to deploy` lo stato di`ACTIVE` una versione del modello, disinstallate la versione del modello.

1. Accedere allaAWS Management Console e aprire la console Amazon Fraud Detector all'indirizzo https://console.aws.amazon.com/frauddetector.
2. Nel pannello di navigazione a sinistra della console Amazon Fraud Detector, seleziona Modelli.
3. Scegliere il modello contenente la versione del modello da eliminare.
4. Scegliere la versione del modello da eliminare.
5. Scegli Actions (Operazioni), quindi Delete (Elimina).
6. Immettete il nome della versione del modello, quindi scegliete Elimina versione modello.

Per annullare la distribuzione di una versione del modello

Non è possibile annullare la distribuzione di una versione del modello utilizzata da qualsiasi versione del rilevatore (`ACTIVE`,`INACTIVE`,`DRAFT`). Pertanto, per disinstallare una versione del modello utilizzata da una versione del rilevatore, rimuovete innanzitutto la versione del modello dalla versione del rilevatore.

1. Nel pannello di navigazione a sinistra della console Amazon Fraud Detector, seleziona Modelli.
2. Scegliete il modello che contiene la versione del modello che desiderate disinstallare.
3. Scegliere la versione del modello da eliminare.
4. Scegli Azioni, quindi scegli Annulla versione del modello.

Per eliminare un modello

Prima di eliminare un modello, è necessario innanzitutto eliminare tutte le versioni del modello e associarle al modello.

1. Nel pannello di navigazione a sinistra della console Amazon Fraud Detector, seleziona Modelli.
2. Scegli il modello per cui eseguire l'eliminazione.
3. Scegli Actions (Operazioni), quindi Delete (Elimina).
4. Immettete il nome del modello, quindi scegliete Elimina modello.

Per rimuovere un SageMaker modello Amazon

1. Nel pannello di navigazione a sinistra della console Amazon Fraud Detector, seleziona Modelli.
2. Scegli il SageMaker modello per cui eseguire la rimozione.
3. Scegli Azioni, quindi scegli Rimuovi modello.
4. Immettete il nome del modello e quindi scegliete Rimuovi SageMaker modello.

Rilevatore

Un rilevatore è un contenitore che contiene la logica di rilevamento delle frodi, ad esempio i modelli e le regole, per uno specifico evento aziendale che si desidera valutare per individuare eventuali frodi. Per prima cosa crei un rilevatore specificando l'evento che hai già definito e, facoltativamente, aggiungi una versione del modello già creata e addestrata da Amazon Fraud Detector per l'evento.

Quindi aggiungi regole e ordine di esecuzione delle regole a un rilevatore per creare una versione del rilevatore. Una versione del rilevatore definisce le regole e, facoltativamente, un modello che verrà eseguito come parte della richiesta per la generazione di previsioni di frode. È possibile aggiungere qualsiasi regola definita all'interno di un rilevatore alla versione del rilevatore. È inoltre possibile aggiungere qualsiasi modello addestrato sul tipo di evento valutato alla versione del rilevatore. Un rilevatore può avere più versioni, ognuna delle quali ha regole e ordine di esecuzione delle regole diversi per soddisfare più casi d'uso.

Ogni versione del rilevatore deve avere uno stato di`DRAFT`,`ACTIVE`, oppure`INACTIVE`. È possibile inserire solo una versione del rilevatore`ACTIVE`stato alla volta. Amazon Fraud Detector utilizza la versione del rilevatore con`ACTIVE`stato per generare previsioni di frode.

Crea un rilevatore

Create un rilevatore specificando il tipo di evento che avete già definito. Facoltativamente, puoi aggiungere un modello già addestrato e implementato da Amazon Fraud Detector. Se aggiungi un modello, puoi utilizzare il punteggio del modello generato da Amazon Fraud Detector nell'espressione della tua regola quando crei una regola (ad esempio,`$model score < 90`).

Puoi creare un rilevatore nella console Amazon Fraud Detector, utilizzandoPutDetectorAPI, utilizzandorilevatore di puttcomando, o utilizzando ilAWSSDK. Se utilizzi API, comando o SDK per creare un rilevatore, dopo aver creato il rilevatore segui le istruzioni perCrea una versione del rilevatore.

Crea un rilevatore nella console Amazon Fraud Detector

Questo esempio presuppone che tu abbia creato un tipo di evento e che tu abbia anche creato e distribuito una versione del modello da utilizzare per la previsione delle frodi.

Fase 1: Costruisci il rilevatore

1. Nel riquadro di navigazione a sinistra della console Amazon Fraud Detector, scegliRilevatori.

2. ScegliCrea rilevatore.
3. NelDefinire i dettagli del rilevatorepagina, inserisci`sample_detector`per il nome del rilevatore. Facoltativamente, inserisci una descrizione per il rilevatore, ad esempio`my sample fraud detector`.
4. PerTipo di evento, seleziona il tipo di evento che hai creato per la previsione delle frodi.
5. Seleziona Successivo.

Fase 2: Aggiungere una versione del modello distribuita

1. Tieni presente che si tratta di un passaggio facoltativo. Non è necessario aggiungere un modello al rilevatore. Per saltare questo passaggio, scegli Next (Successivo).
2. NelAggiungi modello - opzionale, scegliAggiungi modello.
3. NelAggiungi modellopagina, perSeleziona modello, scegli il nome del modello Amazon Fraud Detector che hai implementato in precedenza. PerSeleziona la versione, scegli la versione del modello utilizzato.
4. Scegliere Add model (Aggiungi modello).
5. Seleziona Successivo.

Fase 3: Aggiungere regole

Una regola è una condizione che indica ad Amazon Fraud Detector come interpretare i valori delle variabili durante la valutazione della previsione delle frodi. Questo esempio creerà tre regole utilizzando i punteggi del modello come valori variabili:`high_fraud_risk`,`medium_fraud_risk`, `elow_fraud_risk`. Per creare regole, espressioni di regole, ordine di esecuzione delle regole e risultati personalizzati, utilizza valori appropriati per il tuo modello e il tuo caso d'uso.

1. NelAggiungi regolepagina, sottoDefinire una regola, inserisci`high_fraud_risk`per il nome della regola e sottoDescrizione - opzionale, inserisci**`This rule captures events with a high ML model score`**come descrizione della regola.
2. NelEspressione, inserisci la seguente espressione di regola utilizzando il linguaggio di espressione delle regole semplificato di Amazon Fraud Detector:

   ```
   $sample_fraud_detection_model_insightscore > 900
   ```
3. NelEsiti, scegliCrea un nuovo risultato. Un risultato è il risultato di una previsione di frode e viene restituito se la regola corrisponde durante una valutazione.

4. NelCrea un nuovo risultato, inserisciverify_customercome nome del risultato. Facoltativamente, inserisci una descrizione.
5. ScegliSalva risultato.
6. ScegliAggiungi regolaper eseguire il controllo della convalida delle regole e salvare la regola. Dopo la creazione, Amazon Fraud Detector rende la regola disponibile per l'uso nel tuo rilevatore.
7. ScegliAggiungi un'altra regola, quindi scegli ilCrea regolalinguetta.
8. Ripeti questa procedura altre due volte per creare il tuomedium_fraud_riskelow_fraud_riskregole che utilizzano i seguenti dettagli:

   - rischio_fraudolento medio

     Nome della regola:`medium_fraud_risk`

     Risultato:`review`

     Espressione:

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

     ```
     $sample_fraud_detection_model_insightscore > 700
     ```

   - basso_rischio_fraudolento

     Nome della regola:`low_fraud_risk`

     Risultato:`approve`

     Espressione:

     ```
     $sample_fraud_detection_model_insightscore <= 700
     ```

9. Dopo aver creato tutte le regole per il tuo caso d'uso, scegliProssimo.

   Per ulteriori informazioni sulla creazione e la scrittura di regole, vedereRegolamentoeRiferimento linguistico delle regole.

Fase 4: Configurare l'esecuzione e l'ordine delle regole

La modalità di esecuzione delle regole incluse nel rilevatore determina se tutte le regole definite vengono valutate o se la valutazione delle regole si ferma alla prima regola corrispondente. E l'ordine delle regole determina l'ordine in cui si desidera che venga eseguita la regola.

La modalità di esecuzione delle regole predefinita è`FIRST_MATCHED`.

Primo abbinato

La modalità di esecuzione della prima regola corrispondente restituisce i risultati della prima regola corrispondente in base all'ordine delle regole definito. Se si specifica `FIRST_MATCHED`, Amazon Fraud Detector valuta le regole in sequenza, dalla prima all'ultima, fermandosi alla prima regola corrispondente. Amazon Fraud Detector fornisce quindi i risultati per quella singola regola.

L'ordine in cui esegui le regole può influire sul risultato della previsione delle frodi che ne deriva. Dopo aver creato le regole, riordina le regole per eseguirle nell'ordine desiderato seguendo questi passaggi:

Se il tuo`high_fraud_risk`la regola non è già in cima all'elenco delle regole, scegliOrdine, quindi scegli1. Questo si muove`high_fraud_risk`alla prima posizione.

Ripeti questa procedura in modo che`medium_fraud_risk`la regola è in seconda posizione e la tua`low_fraud_risk`la regola è in terza posizione.

Tutto abbinato

La modalità di esecuzione di tutte le regole corrispondenti restituisce i risultati per tutte le regole corrispondenti, indipendentemente dall'ordine delle regole. Se specifichi`ALL_MATCHED`, Amazon Fraud Detector valuta tutte le regole e restituisce i risultati di tutte le regole corrispondenti.

Seleziona`FIRST_MATCHED`per questo tutorial e poi scegliProssimo.

Fase 5: Rivedere e creare la versione del rilevatore

Una versione rilevatrice definisce i modelli e le regole specifici utilizzati per generare previsioni di frode.

1. NelRivedi e creapagina, esamina i dettagli, i modelli e le regole del rilevatore che hai configurato. Se devi apportare modifiche, scegliModificaaccanto alla sezione corrispondente.

2. ScegliCrea rilevatore. Dopo la creazione, la prima versione del rilevatore viene visualizzata nella tabella Versioni del rilevatore con`Draft`stato.

   Usi ilBozzaversione per testare il tuo Detector.

Creare un rilevatore utilizzandoAWS SDK for Python (Boto3)

L'esempio seguente mostra una richiesta di esempio per`PutDetector`API. Un rilevatore funge da contenitore per le versioni del rilevatore. La`PutDetector`L'API specifica il tipo di evento che il rilevatore valuterà. L'esempio seguente presuppone che tu abbia creato un tipo di evento`sample_registration`.

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

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

Crea una versione del rilevatore

Una versione rilevatrice definisce le regole, l'ordine di esecuzione delle regole e, facoltativamente, una versione del modello, che verrà utilizzata come parte della richiesta per generare previsioni di frode. È possibile aggiungere qualsiasi regola definita all'interno di un rilevatore alla versione del rilevatore. Puoi anche aggiungere qualsiasi modello addestrato sul tipo di evento valutato.

Ogni versione del rilevatore ha uno stato di`DRAFT`,`ACTIVE`, oppure`INACTIVE`. È possibile inserire solo una versione del rilevatore`ACTIVE`stato alla volta. Durante il`GetEventPrediction`richiesta, Amazon Fraud Detector utilizzerà il`ACTIVE`rilevatore se no`DetectorVersion`è specificato.

Modalità di esecuzione delle regole

Amazon Fraud Detector supporta due diverse modalità di esecuzione delle regole:`FIRST_MATCHED`e`ALL_MATCHED`.

- Se la modalità di esecuzione delle regole è`FIRST_MATCHED`, Amazon Fraud Detector valuta le regole in sequenza, dalla prima all'ultima, fermandosi alla prima regola corrispondente. Amazon

Fraud Detector fornisce quindi i risultati per quella singola regola. Se una regola risulta falsa (non corrispondente), viene valutata la regola successiva nell'elenco.

- Se la modalità di esecuzione delle regole è`ALL_MATCHED`, quindi tutte le regole di una valutazione vengono eseguite in parallelo, indipendentemente dal loro ordine. Amazon Fraud Detector esegue tutte le regole e restituisce i risultati definiti per ogni regola corrispondente.

Creare una versione del rilevatore utilizzandoAWS SDK for Python (Boto3)

L'esempio seguente mostra una richiesta di esempio per`CreateDetectorVersion`API. La modalità di esecuzione delle regole è impostata su`FIRST_MATCHED`, pertanto Amazon Fraud Detector valuterà le regole in sequenza, dalla prima all'ultima, fermandosi alla prima regola corrispondente. Amazon Fraud Detector fornisce quindi i risultati per quella singola regola durante il`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'
```

```
)
```

Per aggiornare lo stato di una versione del rilevatore, utilizzareUpdateDetectorVersionStatusAPI. L'esempio seguente aggiorna lo stato della versione del rilevatore daDRAFTaACTIVE. Durante unGetEventPredictionrichiesta, se non viene specificato un ID del rilevatore, Amazon Fraud Detector utilizzerà ilACTIVEversione del rilevatore.

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

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

Eliminare un rilevatore, una versione del rilevatore o una versione di una regola

Prima di eliminare un rilevatore in Amazon Fraud Detector, è necessario innanzitutto eliminare tutte le versioni del rilevatore e le versioni delle regole associate al rilevatore.

Quando elimini un rilevatore, una versione del rilevatore o una versione di una regola, Amazon Fraud Detector elimina definitivamente quella risorsa e i dati non vengono più archiviati in Amazon Fraud Detector.

Per eliminare una versione del rilevatore

È possibile eliminare solo le versioni del rilevatore in`DRAFT` o in`INACTIVE` stato di attivazione.

1. Accedere allaAWS Management Console e aprire la console Amazon Fraud Detector Amazon Fraud Detector all'indirizzo https://console.aws.amazon.com/frauddetector.
2. Nel pannello di navigazione a sinistra della console Amazon Amazon Fraud Detector, nel riquadro di navigazione a sinistra della console Amazon Amazon Fraud Detector,
3. Scegli il rilevatore che contiene la versione del rilevatore che desideri eliminare.
4. Scegliere la versione del rilevatore da eliminare.
5. Scegli Actions (Operazioni), quindi Delete (Elimina).

6. Inserisci**`delete`**, quindi scegli Elimina rilevatore.

Come eliminare una versione della regola

È possibile eliminare una versione della regola solo se non è utilizzata da nessuna delle versioni del`ACTIVE`o`INACTIVE` rilevatore. Se necessario, prima di eliminare una versione della regola, sposta prima la versione del`ACTIVE` rilevatore su`INACTIVE`, quindi elimina la versione del`INACTIVE` rilevatore.

1. Nel pannello di navigazione a sinistra della console Amazon Amazon Fraud Detector, nel riquadro di navigazione a sinistra della console Amazon Amazon Fraud Detector,
2. Scegliere il rilevatore contenente la versione della regola da eliminare.
3. Scegliere la scheda Regole associate e scegliere la regola da eliminare.
4. Scegliere la versione della regola da eliminare.
5. Scegli Azioni, quindi scegli Elimina versione della regola.
6. Inserisci**`delete`**, quindi scegli Elimina versione.

Per eliminare un rilevatore

Prima di eliminare un rilevatore, è necessario innanzitutto eliminare tutte le versioni del rilevatore e le versioni delle regole associate al rilevatore.

1. Nel pannello di navigazione a sinistra della console Amazon Amazon Fraud Detector, nel riquadro di navigazione a sinistra della console Amazon Amazon Fraud Detector,
2. Scegliere il rilevatore da eliminare.
3. Scegli Azioni, quindi scegli Elimina rilevatore.
4. Inserisci**`delete`**, quindi scegli Elimina rilevatore.

Risorse

I modelli, le regole e i rilevatori utilizzano risorse come variabili, risultati, etichette, elenchi ed entità per valutare gli eventi che comportano il rischio di frode. In questa sezione vengono fornite informazioni sulla creazione e sulla gestione di informazioni sulla creazione e sulla gestione di informazioni sulla creazione e

Argomenti

Variables

Le variabili rappresentano elementi di dati che desideri utilizzare in una previsione di frode. Queste variabili possono essere prese dal set di dati degli eventi che hai preparato per addestrare il tuo modello, dai risultati del punteggio di rischio del tuo modello Amazon Fraud Detector o dai modelli Amazon. SageMaker Per ulteriori informazioni sulle variabili prese dal set di dati dell'evento, vedereOttieni i requisiti dei set di dati di eventi utilizzando Data models explorer.

Le variabili che desideri utilizzare nella previsione delle frodi devono prima essere create e quindi aggiunte all'evento durante la creazione del tipo di evento. A ogni variabile creata deve essere assegnato un tipo di dati, un valore predefinito e, facoltativamente, un tipo di variabile. Amazon Fraud Detector arricchisce alcune delle variabili fornite, come indirizzi IP, numeri di identificazione bancaria (BIN) e numeri di telefono, per creare input aggiuntivi e migliorare le prestazioni dei modelli che utilizzano queste variabili.

Tipi di dati

Le variabili devono avere un tipo di dati per l'elemento di dati che la variabile rappresenta e, facoltativamente, possono essere assegnati a uno dei valori predefiniti. Tipi variabili Per le variabili

assegnate a un tipo di variabile, il tipo di dati è preselezionato. I tipi di dati possibili includono i seguenti tipi:

Tipo di dati	Descrizione	Valore predefinito	Valori di esempio
Stringa	Qualsiasi combinazione di lettere, numeri interi o entrambi	<empty>	abc, 123, 1D3B
Numero intero	Numeri interi positivi o negativi	0	1, -1
Boolean	Vero o falso	False	Vero, falso
DateTime	Data e ora specificate solo nel formato UTC standard ISO 8601	<empty>	2019-11-30T 13:01:01 Z
Float	Numeri con punti decimali	0,0	4,01, 0,10

Valore predefinito

Le variabili devono avere un valore predefinito. Quando Amazon Fraud Detector genera previsioni di frode, questo valore predefinito viene utilizzato per eseguire una regola o un modello se Amazon Fraud Detector non riceve un valore per una variabile. I valori predefiniti forniti devono corrispondere al tipo di dati selezionato. Nella console AWS, Amazon Fraud Detector assegna il valore predefinito di numeri `0` `false` interi, booleani, `0.0` float e (vuoto) stringhe. È possibile impostare un valore predefinito personalizzato per ognuno di questi tipi di dati.

Tipi variabili

Quando si crea una variabile, è possibile assegnarla facoltativamente a un tipo di variabile. Il tipo di variabile rappresenta gli elementi di dati comuni utilizzati per addestrare modelli e generare previsioni di frode. Per l'addestramento dei modelli è possibile utilizzare solo le variabili con un tipo di variabile associato. Come parte del processo di formazione del modello, Amazon Fraud Detector utilizza il tipo di variabile associato alla variabile per eseguire arricchimenti delle variabili, ingegneria delle funzionalità e valutazione del rischio.

Amazon Fraud Detector ha predefinito i seguenti tipi di variabili che possono essere utilizzati per assegnare le tue variabili.

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
Sessione	IP_ADDRESS	L'indirizzo IP che viene raccolto durante l'evento	Strin	192.0.2.0 Nota: Amazon Fraud Detector arricchisce questi dati. Per ulteriori informazioni, consulta Arricchimento della geolocalizzazione.
	UTENTE/AGENTE	L'agente utente che viene raccolto durante l'evento	Strin	Mozilla 5.0 (Windows NT 10.0, Win64, x64, versione: 68.0)

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
				Gecko 20100101
	IMPRONTA DIGITALE	L'identificatore univoco di un dispositivo utilizzato per l'evento	Strin	sadfo987u 234
	SESSION_I D	L'ID di sessione per la sessione attiva dell'evento	Strin	sid123456 789
	LE CREDENZI LI SONO VALIDE	Indica se le credenziali utilizzate per l'accesso all'event o sono valide	Bool	True
Ut	INDIRIZZO _EMAIL	L'indirizzo email che viene raccolto durante l'evento	Strin	abc@domai n.com

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
	PHONE_NUMBER	Il numero di telefono raccolto durante l'evento	Strin	+1 555-0100 Nota: Amazon Fraud Detector arricchisce questi dati. Per ulteriori informazioni, consulta Arricchimento del numero di telefono.
Fa on	NOME_FATURAZIONE	Il nome associato all'indirizzo di fatturazione	Strin	John Doe

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
	TELEFONO DI FATTURAZONE	Il numero di telefono associato all'indirizzo di fatturazione	Strin	+1 555-0100 Nota: Amazon Fraud Detector arricchisce questi dati. Per ulteriori informazioni, consulta Arricchimento del numero di telefono.
	INDIRIZZO_DI FATTURAZONE L1	La prima riga dell'indirizzo di fatturazione	Strin	Qualsiasi strada
	INDIRIZZO_DI FATTURAZONE L2	La seconda riga dell'indirizzo di fatturazione	Strin	Qualsiasi unità 123

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
	CITTÀ DI FATTURAZONE	La città indicata nell'indirizzo di fatturazione	Strin	Qualsiasi città
	STATO_DI FATTURAZONE	Lo stato o la provincia che si trova nell'indirizzo di fatturazione	Strin	Qualsiasi stato o provincia
	PAESE DI FATTURAZONE	Il paese indicato nell'indirizzo di fatturazione	Strin	Qualsiasi paese Nota: Amazon Fraud Detector arricchisce questi dati. Per ulteriori informazioni, consulta Arricchimento della geolocalizzazione.

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
	FATTURAZONE ZIP	Il codice postale che si trova nell'indirizzo di fatturazione	Strin	01234 Nota: Amazon Fraud Detector arricchisce questi dati. Per ulteriori informazioni, consulta Arricchimento della geolocalizzazione.
Sp i	NOME_SPEDIZIONE	Il nome associato all'indirizzo di spedizione	Strin	John Doe

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
	TELEFONO DI SPEDIZIONE	Il numero di telefono associato all'indirizzo di spedizione	Strin	+1 555-0100 Nota: Amazon Fraud Detector arricchisce questi dati. Per ulteriori informazioni, consulta Arricchimento del numero di telefono.
	INDIRIZZO_DI SPEDIZIONE_L1	La prima riga dell'indirizzo di spedizione	Strin	123 Qualsiasi strada
	INDIRIZZO_DI SPEDIZIONE_L2	La seconda riga dell'indirizzo di spedizione	Strin	Unità 123

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
	CITTÀ_DI SPEDIZIONE	La città che si trova nell'indirizzo di spedizione	Strin	Qualsiasi città
	STATO_DI SPEDIZIONE	Lo stato o la provincia che si trova nell'indirizzo di spedizione	Strin	Qualsiasi stato
	PAESE_DI SPEDIZIONE	Il paese in cui si trova è indicato nell'indirizzo di spedizione	Strin	Qualsiasi Paese Nota: Amazon Fraud Detector arricchisce questi dati. Per ulteriori informazioni, consulta Arricchimento della geolocalizzazione.

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
	ZIP DI SPEDIZIONE	Il codice postale che si trova nell'indirizzo di spedizione	Strin	01234 Nota: Amazon Fraud Detector arricchisce questi dati. Per ulteriori informazioni, consulta Arricchimento della geolocalizzazione.
Pag	ORDER_ID	L'identificatore univoco della transazione	Strin	LUX60
	PREZZO	Il prezzo totale dell'ordine	Strin	560,00
	CODICE_VALUTA	Il codice valuta ISO 4217	Strin	USD

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
	TIPO DI PAGAMENT	Il metodo di pagamento utilizzato per il pagamento durante l'evento	Strin	Carta di credito
	CODICE DI AUTENTICA ZIONE	Il codice alfanumerico inviato dall'emit tente della carta di credito o dalla banca emittente	Strin	0000
	AVS	Il codice di risposta del sistema di verifica degli indirizzi (AVS) del processore della carta	Strin	Y
Pr	CATEGORI _PRODOTT	La categoria di prodotto dell'arti colo dell'ordine	Strin	Cucina
Pe zz	NUMERIC	Qualsiasi variabile che può essere rappresen tata come numero reale	Floa	1.224

Ca	Tipo variabile	Descrizione	Tipo di dati	Es
	CATEGORICAL	Qualsiasi variabile che descrive categorie, segmenti o gruppi	Strin	Large
	FORM_TESTO_LIBERO	Qualsiasi testo in formato libero acquisito come parte dell'evento (ad esempio, una recensione o un commento di un cliente)	Strin	Esempio di immissione di testo in formato libero

Assegnazione di una variabile a un tipo di variabile

Se si prevede di utilizzare una variabile per addestrare il modello, è importante scegliere il tipo di variabile corretto da assegnare alla variabile. L'assegnazione errata del tipo di variabile può influire negativamente sulle prestazioni del modello. Può anche diventare molto difficile modificare l'assegnazione in un secondo momento, soprattutto se più modelli ed eventi hanno utilizzato la variabile.

È possibile assegnare alla variabile uno qualsiasi dei tipi di variabili predefiniti o uno dei tipi di variabili personalizzate:`FREE_FORM_TEXT`,`CATEGORICAL`, o. `NUMERIC`

Note importanti per l'assegnazione di variabili ai tipi di variabili corretti

1. Se la variabile corrisponde a uno dei tipi di variabili predefiniti, utilizzala. Assicurati che il tipo di variabile corrisponda alla variabile. Ad esempio, se assegni una variabile ip_address a un tipo di variabile, la `EMAIL_ADDRESS` variabile ip_address non verrà arricchita con arricchimenti come ASN, ISP, geolocalizzazione e punteggio di rischio. Per ulteriori informazioni, consulta Arricchimenti variabili.

2. Se la variabile non corrisponde a nessuno dei tipi di variabili predefiniti, segui i consigli elencati di seguito per assegnare uno dei tipi di variabili personalizzate.
3. Assegna il tipo di `CATEGORICAL` variabile a variabili che in genere non hanno un ordine naturale e possono essere inserite in categorie, segmenti o gruppi. Il set di dati che stai utilizzando per addestrare il tuo modello potrebbe avere variabili ID come merchant_id, campaign_id o policy_id. Queste variabili rappresentano i gruppi (ad esempio, tutti i clienti con lo stesso policy_id rappresentano un gruppo). Alle variabili con i seguenti dati deve essere assegnato il tipo di variabile CATEGORICA -
   - Variabili che contengono dati come Customer_ID, segment_ID, color_ID, department_code o Product_ID.
   - Variabili che contengono dati booleani con valori true, false o nulle.
   - Variabili che possono essere suddivise in gruppi o categorie come il nome dell'azienda, la categoria di prodotto, il tipo di carta o il mezzo di riferimento.

   > **Note**
   >
   > `ENTITY_ID`è un tipo di variabile riservato utilizzato da Amazon Fraud Detector per assegnare alla variabile ENTITY_ID. La variabile ENTITY_ID è l'ID dell'entità che avvia l'azione che desideri valutare. Se stai creando un tipo di modello Transaction Fraud Insight (TFI), devi fornire la variabile ENTITY_ID. Dovrai decidere quale variabile nei tuoi dati identifica in modo univoco l'entità che avvia l'azione e trasmetterla come variabile ENTITY_ID. Assegna il tipo di variabile CATEGORICAL a tutti gli altri ID nel tuo set di dati, se sono presenti e se li stai utilizzando per l'addestramento dei modelli. Esempi di altri ID che non sono un'entità nel set di dati possono essere Merchant_ID, Policy_ID e Campaign_ID.
4. Assegna il tipo di `FREE_FORM_TEXT` variabile alle variabili che contengono un blocco di testo. Esempi di tipi di variabili FREE_FORM_TEXT sono: recensioni degli utenti, commenti, date e codici di riferimento. I dati FREE_FORM_TEXT contengono più token separati da un delimitatore. I delimitatori possono essere qualsiasi carattere diverso dal simbolo alfanumerico e dal carattere di sottolineatura. Ad esempio, le recensioni e i commenti degli utenti possono essere separati da un delimitatore «spazio», le date e i codici di riferimento possono utilizzare trattini come delimitatori per separare prefisso, suffisso e parti intermedie. Amazon Fraud Detector utilizza i delimitatori per estrarre dati dalle variabili FREE_FORM_TEXT.
5. Assegna il tipo di variabile NUMERIC a variabili che sono numeri reali e hanno un ordine intrinseco. Esempi di variabili NUMERICHE includono day_of_the_week, incident_severity,

customer_rating. Sebbene sia possibile assegnare il tipo di variabile CATEGORICAL a queste variabili, si consiglia vivamente di assegnare tutte le variabili numeriche reali con ordine intrinseco al tipo di variabile NUMERIC.

Arricchimenti variabili

Amazon Fraud Detector arricchisce alcuni degli elementi di dati grezzi che fornisci, come indirizzi IP, numeri di identificazione bancaria (BIN) e numeri di telefono, per creare input aggiuntivi e migliorare le prestazioni dei modelli che utilizzano questi elementi di dati. L'arricchimento aiuta a identificare situazioni potenzialmente sospette e aiuta i modelli a rilevare ulteriori frodi.

Arricchimento del numero di telefono

Amazon Fraud Detector arricchisce i dati dei numeri di telefono con informazioni aggiuntive relative alla geolocalizzazione, al corriere originale e alla validità del numero di telefono. L'arricchimento del numero di telefono viene abilitato automaticamente per tutti i modelli formati a partire dal 13 dicembre 2021 e che dispongono di un numero di telefono che include un prefisso internazionale (+xxx). Se hai incluso la variabile del numero di telefono nel tuo modello e l'hai addestrata prima del 13 dicembre 2021, riqualificalo in modo che possa sfruttare questo arricchimento.

Ti consigliamo vivamente di utilizzare il seguente formato per le variabili dei numeri di telefono per assicurarti che i tuoi dati vengano arricchiti correttamente.

Variabile	Formato	Descrizione
PHONE_NUMBER	Lo standard E.164	Assicurati di includere il prefisso internazionale (+xxx) con il numero di telefono.
BILLING_PHONE e SHIPPING_PHONE	Lo standard E.164	Assicurati di includere il prefisso internazionale (+xxx) con il numero di telefono.

Arricchimento della geolocalizzazione

A partire dall'8 febbraio 2022, Amazon Fraud Detector calcola la distanza fisica tra i valori IP_ADDRESS, BILLING_ZIP e SHIPPING_ZIP che fornisci per un evento. Le distanze calcolate vengono utilizzate come input per il tuo modello di rilevamento delle frodi.

Per abilitare l'arricchimento della geolocalizzazione, i dati dell'evento devono includere almeno due delle tre variabili: IP_ADDRESS, BILLING_ZIP o SHIPPING_ZIP. Inoltre, ogni valore BILLING_ZIP e SHIPPING_ZIP deve avere rispettivamente un codice BILLING_COUNTRY e un codice SHIPPING_COUNTRY validi. Se disponi di un modello che è stato addestrato prima dell'8 febbraio 2022 e include queste variabili, devi riqualificarlo per abilitare l'arricchimento della geolocalizzazione.

Se Amazon Fraud Detector non è in grado di determinare la posizione associata ai valori IP_ADDRESS, BILLING_ZIP o SHIPPING_ZIP per un evento a causa della non validità dei dati, viene utilizzato invece un valore segnaposto speciale. Ad esempio, supponiamo che un evento abbia valori IP_ADDRESS e BILLING_ZIP validi, ma il valore SHIPPING_ZIP non sia valido. In questo caso, l'arricchimento viene eseguito solo per IP_ADDRESS—> BILLING_ZIP. L'arricchimento non viene eseguito per IP_ADDRESS—>SHIPPING_ZIP e BILLING_ZIP—>SHIPPING_ZIP. Invece, i valori segnaposto vengono utilizzati al loro posto. Indipendentemente dal fatto che l'arricchimento della geolocalizzazione sia abilitato o meno per il tuo modello, le prestazioni del tuo modello non cambiano.

Puoi disattivare l'arricchimento della geolocalizzazione mappando le variabili BILLING_ZIP e SHIPPING_ZIP al tipo di variabile CUSTOM_CATEGORICAL. La modifica del tipo di variabile non influisce sulle prestazioni del modello.

Formato variabile di geolocalizzazione

Ti consigliamo vivamente di utilizzare il seguente formato per le variabili di geolocalizzazione per garantire che i dati sulla posizione vengano arricchiti correttamente.

Variabile	Formato	Descrizione
IP_ADDRESS	Indirizzo IPv4	Ad esempio: 1.1.1.1
BILLING_ZIP e SHIPPING_ZIP	Il codice postale ISO 3166-1 alpha-2 per il paese specificato	Per ulteriori informazioni, consulta la sezione Codici di Paese e territorio in questo argomento.

Variabile	Formato	Descrizione
BILLING_COUNTRY e SHIPPING_COUNTRY	Il codice del paese standard ISO 3166-1 alpha-2 a due lettere	Per ulteriori informazioni, consulta la sezione Codici di Paese e territorio in questo argomento. Amazon Fraud Detector cerca di abbinare tutte le varianti più comuni del nome di un paese al codice internazionale standard di due lettere ISO 3166-1. Tuttavia, non possiamo garantire che vengano abbinati correttamente.

Codici dei paesi e dei territori

La tabella seguente fornisce un elenco completo dei paesi e dei territori supportati da Amazon Fraud Detector per l'arricchimento della geolocalizzazione. A ogni paese e territorio è assegnato un codice paese (in particolare, il prefisso internazionale a due lettere ISO 3166-1 alpha-2) e un codice postale.

Formato del codice postale

- 9 - numero
- a - lettera
- [X] - X è opzionale. Ad esempio, «GY9 [9] 9aa» di Guersney significa che sia «GY9 9aa» che «GY99 9aa» sono validi. Usa un formato.
- [X/XX]: è possibile utilizzare X o XX. Ad esempio, «aa [aa/99]» delle Bermuda significa che sia «aa aa» che «aa 99" sono validi. Utilizzate uno di questi formati, ma non entrambi.
- Alcuni paesi hanno un prefisso fisso. Ad esempio, il codice postale di Andorra è AD999. Ciò significa che il prefisso internazionale deve iniziare con le lettere AD seguite da tre numeri.

Codice	Nome	Codice postale
AD	Andorra	ANNUNCIO 999
AR	Antille Olandesi	9999
AT	Austria	9999
AU	Australia	9999
AZ	Azerbaigian	A PARTIRE DA 9999
LETTO	Bangladesh	9999
ESSERE	Belgio	9999
BG	Bulgaria	9999
BM	Bermuda	aa [aa/99]
BY	Bielorussia	999999
CA	Canada	a9a 9a9
CH	Svizzera	9999
CL	Cile	9999999
CO	Colombia	999999
CR	Costa Rica	99999
CY	Cipro	9999
CZ	Cechia	999 99
DE	Germania	99999
DK	Danimarca	9999
DO	Repubblica Dominicana	99999

Codice	Nome	Codice postale
DZ	Algeria	99999
EE	Estonia	99999
ES	Spagna	99999
SE	Finlandia	99999
FM	Stati Federati di Micronesia	99999
PER	Isole Fær Øer	999
FR	Francia	99999
GB	Regno Unito	a [a] 9 [a/9] 9aa
GG	Guernsey	GY9 [9] 9aa
GL	Groenlandia	9999
GP	Guadalupa	99999
GT	Guatemala	99999
GU	Guam	99999
ORE	Croazia	99999
HU	Ungheria	9999
IE	Irlanda	a99 [a/9] [a/9] [a/9]
IM	Isola di Man	IM9 [9] 9aa
IN	India	999999
IS	Islanda	999
ESSO	Italia	99999

Codice	Nome	Codice postale
JE	Jersey	JE9 [9] 9aa
JP	Giappone	999-9999
KR	Repubblica di Corea	99999
LI	Liechtenstein	9999
OK	Sri Lanka	99999
LT	Lituania	99999
LU	Lussemburgo	L-9999
LV	Lettonia	LV-9999
MC	Monaco	99999
MD	Repubblica di Moldavia	9999
MH	Isole Marshall	99999
KM	Nrd Macedonia del Nord	9999
MP	Isole Marianne Settentrionali	99999
MQ	Matinica	99999
MT	Malta	aaa 9999
MX	Messico	99999
MIA	Malesia	99999
NL	Paesi Bassi	999 aa
NO	Norvegia	9999
NZ	Nuova Zelanda	9999

Codice	Nome	Codice postale
PH	Filippine	9999
PK	Pakistan	99999
PL	Polonia	99-999
PR	Porto Rico	99999
PT	Portogallo	9999-999
PW	Palau	99999
RE	Riunione	99999
O	Romania	999999
RU	Federazione Russa	999999
VEDERE	Svezia	999 99
SG	Singapore	999999
SI	Slovenia	9999
SK	Slovacchia	999 99
SM	San Marino	99999
TH	Tailandia	99999
TR	Turchia	99999
UA	Ucraina	99999
USA	Stati Uniti	99999
COMPRARE	Uruguay	99999
VI	Isole Vergini americane	99999

Codice	Nome	Codice postale
WF	Wallis e Futuna	99999
EPPURE	Mayotte	99999
ZA	Sudafrica	9999

Arricchimento dell'agente utente

Se crei il modello Account Takeover Insights (ATI), devi fornire una variabile del tipo di `useragent` variabile nel tuo set di dati. Questa variabile contiene i dati del browser, del dispositivo e del sistema operativo di un evento di accesso. Amazon Fraud Detector arricchisce i dati dell'agente utente con informazioni aggiuntive come, e `user_agent_family` `OS_family`. `device_family`

Creare una variabile

Puoi creare variabili nella console Amazon Fraud Detector, utilizzando il comando create-variable, utilizzando o utilizzando CreateVariableAWS SDK for Python (Boto3)

Crea una variabile utilizzando la console Amazon Fraud Detector

Questo esempio crea due variabili `email_address` e `ip_address` le assegna ai tipi di variabili corrispondenti (`EMAIL_ADDRESS`e`IP_ADDRESS`). Queste variabili vengono utilizzate come esempi. Se state creando variabili da utilizzare per l'addestramento del modello, utilizzate le variabili del set di dati appropriate al vostro caso d'uso. Assicurati di leggere informazioni Tipi variabili e Arricchimenti variabili prima di creare le tue variabili.

Per creare una variabile,

1. Apri la console di AWS gestione e accedi al tuo account.
2. Accedi ad Amazon Fraud Detector, scegli Variabili nella barra di navigazione a sinistra, quindi scegli Crea.
3. Nella pagina Nuova variabile, inserisci `email_address` il nome della variabile. Facoltativamente, inserisci una descrizione della variabile.
4. Nel Tipo variabile, scegli Indirizzo e-mail.
5. Amazon Fraud Detector seleziona automaticamente il tipo di dati per questo tipo di variabile perché questo tipo di variabile è predefinito. Se alla variabile non viene assegnato

automaticamente un tipo di variabile, seleziona un tipo di variabile dall'elenco. Per ulteriori informazioni, consulta Tipi variabili.

6. Se desideri fornire un valore predefinito per la tua variabile, seleziona Definisci un valore predefinito personalizzato e inserisci un valore predefinito per la variabile. Salta questo passaggio se stai seguendo questo esempio.
7. Seleziona Create (Crea).
8. Nella pagina di panoramica dell'indirizzo email_address, conferma i dettagli della variabile che hai appena creato.

   Se devi aggiornare, scegli Modifica e fornisci gli aggiornamenti. Sceglie Save changes (Salva modifiche).
9. Ripeti la procedura per creare un'altra variabile `ip_address` e scegli Indirizzo IP per il tipo di variabile.
10. La pagina Variabili mostra le variabili appena create.

> **Important**
>
> Ti consigliamo di creare tutte le variabili che desideri dal tuo set di dati. In seguito, durante la creazione del tipo di evento, puoi decidere quali variabili includere per addestrare il tuo modello a rilevare le frodi e a generare rilevazioni di frodi.

Creare una variabile utilizzando AWS SDK for Python (Boto3)

L'esempio seguente mostra le richieste per l'CreateVariableAPI. L'esempio crea due variabili `email_address` e `ip_address` le assegna ai tipi di variabili corrispondenti (`EMAIL_ADDRESS`e`IP_ADDRESS`).

Queste variabili vengono utilizzate come esempi. Se state creando variabili da utilizzare per l'addestramento del modello, utilizzate le variabili del set di dati appropriate al vostro caso d'uso. Assicurati di leggere informazioni Tipi variabili e Arricchimenti variabili prima di creare le tue variabili.

Assicurati di specificare una fonte variabile. Aiuta a identificare da dove viene derivato il valore della variabile. Se l'origine della variabile è EVENT, il valore della variabile viene inviato come parte della GetEventPredictionrichiesta. Se il valore della variabile è`MODEL_SCORE`, viene compilato da un Amazon Fraud Detector. Se`EXTERNAL_MODEL_SCORE`, il valore della variabile è popolato da un SageMaker modello importato.

```
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>'
     )
```

Eliminare una variabile

Quando elimini una variabile, Amazon Fraud Detector elimina definitivamente tale variabile e i dati non vengono più archiviati in Amazon Fraud Detector.

Non puoi eliminare le variabili incluse in un tipo di evento in Amazon Fraud Detector. Dovrai prima eliminare il tipo di evento a cui è associata la variabile, quindi eliminare la variabile.

Non puoi eliminare manualmente le variabili di output del modello Amazon Fraud Detector e le variabili di output SageMaker del modello. Amazon Fraud Detector elimina automaticamente le variabili di output del modello quando elimini il modello.

Puoi eliminare una variabile nella console Amazon Fraud Detector, utilizzando il comando CLI delete-variable, utilizzando l'DeleteVariableAPI o utilizzando AWS SDK for Python (Boto3)

Eliminare la variabile utilizzando la console

Per eliminare una variabile,

1. Accedi AWS Management Console e apri la console Amazon Fraud Detector all'indirizzo https://console.aws.amazon.com/frauddetector.

2. Nel riquadro di navigazione a sinistra della console Amazon Fraud Detector, scegli Risorse, quindi scegli Variabili.
3. Scegliete la variabile che desiderate eliminare.
4. Scegli Actions (Operazioni), quindi Delete (Elimina).
5. Immettete il nome della variabile, quindi scegliete Elimina variabile.

Eliminare la variabile utilizzando AWS SDK for Python (Boto3)

Il seguente esempio di codice elimina una variabile customer_name utilizzando l'API. DeleteVariable

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

fraudDetector.delete_variable (

name = 'customer_name'

)
```

Etichette

Un'etichetta classifica un evento come fraudolento o legittimo. Le etichette sono associate ai tipi di evento e vengono utilizzate per addestrare modelli di machine learning in Amazon Fraud Detector. Se si intende addestrare un modello Online Fraud Insights (OFI) o Transaction Fraud Insights (TFI), almeno 400 eventi nel set di dati di formazione devono essere classificati come fraudolenti o legittimi. Puoi utilizzare qualsiasi etichetta come frode, legittimo, 1 o 0 per classificare gli eventi nel tuo set di dati di formazione. Al termine della formazione, il modello addestrato valuta gli eventi per individuare eventuali frodi e utilizza questi valori per classificare gli eventi come fraudolenti o legittimi.

Dovrai prima creare le etichette con i valori utilizzati nel tuo set di dati di formazione e quindi associare le etichette al tipo di evento utilizzato per creare e addestrare il tuo modello di rilevamento delle frodi.

Crea etichetta

Puoi creare etichette nella console di Amazon Fraud Detector, utilizzando il comando put-label, utilizzando l'PutLabelAPI o utilizzando ilAWS SDK for Python (Boto3).

Crea un'etichetta utilizzando la console Amazon Fraud Detector

Per creare etichette,

1. Apri la console diAWS gestione e accedi al tuo account.
2. Vai ad Amazon Fraud Detector, scegli Etichette nella barra di navigazione a sinistra, quindi scegli Crea.
3. Nella pagina Crea etichetta, inserisci il nome dell'etichetta per l'evento fraudolento come nome dell'etichetta. Il nome dell'etichetta deve corrispondere all'etichetta che rappresenta l'attività fraudolenta nel set di dati di formazione. Facoltativamente, inserisci una descrizione dell'etichetta.
4. Scegli Crea etichetta.
5. Crea una seconda etichetta e inserisci un nome per l'evento legittimo. Assicurati che il nome dell'etichetta corrisponda al valore che rappresenta l'attività legittima nel set di dati di allenamento.

Crea un'etichetta usandoAWS SDK for Python (Boto3)

Il seguente codice diAWS SDK for Python (Boto3) esempio crea due etichette (fraudolente, legittima) utilizzando l'PutLabelAPI. Dopo aver creato le etichette, puoi aggiungerle a un tipo di evento per classificare eventi specifici.

```
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'
)
```

Aggiorna etichetta

Se il set di dati degli eventi è archiviato con Amazon Fraud Detector, potresti dover aggiungere o aggiornare le etichette per gli eventi archiviati, ad esempio quando esegui un'indagine antifrode offline per un evento e desideri chiudere il ciclo di feedback di apprendimento automatico.

È possibile aggiungere o aggiornare le etichette per gli eventi memorizzati utilizzando il update-event-labelcomando, utilizzando l'UpdateEventLabelAPI o utilizzando ilAWS SDK for Python (Boto3)

Il codice diAWS SDK for Python (Boto3) esempio seguente aggiunge un'etichetta fraudolenta associata alla registrazione del tipo di evento tramite l'`UpdateEventLabel`API.

```
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'
)
```

Aggiornamento delle etichette degli eventi nei dati degli eventi archiviati in Amazon Fraud Detector

Potrebbe essere necessario aggiungere o aggiornare le etichette antifrode per gli eventi già archiviati in Amazon Fraud Detector, ad esempio quando esegui un'indagine antifrode offline per un evento e desideri chiudere il ciclo di feedback del machine learning. Per aggiornare l'etichetta per un evento già archiviato in Amazon Fraud Detector, utilizza l'operazione`UpdateEventLabel` API. Di seguito viene illustrato un esempio di chiamata UpdateEventLabel API.

```
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'
)
```

Elimina etichetta

Quando elimini un'etichetta, Amazon Fraud Detector elimina definitivamente tale etichetta e i dati non vengono più archiviati in Amazon Fraud Detector.

Non puoi eliminare un'etichetta inclusa in Amazon Fraud Detector. Inoltre, non puoi eliminare un'etichetta assegnata a un ID evento. Devi prima eliminare l'ID evento pertinente.

Puoi eliminare le etichette nella console di Amazon Fraud Detector, utilizzando il comando delete-label, utilizzando l'DeleteLabelAPI o utilizzando ilAWS SDK for Python (Boto3)

Eliminazione di un'etichetta tramite la console

Eliminazione di un'etichetta

1. Accedi allaAWS Management Console e apri la console Amazon Fraud Detector all'indirizzo https://console.aws.amazon.com/frauddetector.
2. Nel riquadro di navigazione sinistro della console Amazon Fraud Detector, scegli Risorse, quindi scegli Etichette.
3. Scegliere l'etichetta da eliminare.
4. Scegli Actions (Operazioni), quindi Delete (Elimina).
5. Inserisci il nome dell'etichetta, quindi scegli Elimina etichetta.

Eliminare un'etichetta utilizzandoAWS SDK for Python (Boto3)

Il seguente codice diAWS SDK for Python (Boto3) esempio elimina un'etichetta legittima utilizzando l'DeleteLabelAPI.

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

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

```
)
```

Regolamento

Una regola è una condizione che indica ad Amazon Fraud Detector come interpretare i valori delle variabili durante una previsione di frode. Una regola fa parte della logica di un rilevatore ed è composta dai seguenti elementi:

- Variabile o elenco: la variabile rappresenta un elemento di dati nel set di dati dell'evento che desideri utilizzare in una previsione di frode. Un elenco è un insieme di elementi di dati di input per una variabile nel set di dati dell'evento. Le variabili utilizzate in una regola devono essere predefinite nel tipo di evento valutato e gli elenchi utilizzati in una regola devono essere associati a un tipo di variabile. Per ulteriori informazioni, consultare Variables e Elenchi.
- Espressione: un'espressione in una regola cattura la logica aziendale. Se si utilizza una variabile nella regola, viene creata una semplice espressione di regola utilizzando una variabile, un operatore di confronto come >, <, <=, >=. == e un valore. Se si utilizza un elenco, l'espressione della regola viene costruita come voce di elenco e nome dell'elenco. `in` Per ulteriori informazioni, consulta Riferimento linguistico delle regole. È possibile combinare più espressioni utilizzando `and` e `or`. Tutte le espressioni devono restituire un valore booleano (vero o falso) e avere una lunghezza inferiore a 4.000 caratteri. Le condizioni di tipo if-else non sono supportate.
- Risultato: un risultato è una risposta restituita da Amazon Fraud Detector quando una regola viene soddisfatta. Il risultato indica il risultato di una previsione di frode. Puoi creare risultati per ogni possibile previsione di frode e aggiungerli a una regola. Per ulteriori informazioni, consulta Esiti.

Un rilevatore deve avere almeno una regola associata. Una regola può avere fino a 3 elenchi e un rilevatore può avere fino a 30 elenchi. La regola viene creata come parte del processo di creazione del rilevatore. Puoi anche creare e associare nuove regole a un rilevatore esistente.

Riferimento linguistico delle regole

La sezione seguente descrive le funzionalità delle espressioni (ovvero la scrittura di regole) in Amazon Fraud Detector.

Utilizzo di variabili

È possibile utilizzare qualsiasi variabile definita nel tipo di evento valutato come parte dell'espressione. Usa il simbolo del dollaro per indicare una variabile:

```
$example_variable < 100
```

Utilizzo degli elenchi

È possibile utilizzare qualsiasi elenco associato a un tipo di variabile e popolato da voci come parte dell'espressione della regola. Usa il simbolo del dollaro per indicare il valore di una voce nell'elenco:

```
$example_list_variable in @list_name
```

Operatori di confronto, appartenenza e identità

Amazon Fraud Detector include i seguenti operatori di confronto: **>**, **>=**, **<**, **<=**,**! =**, **==**, dentro, non dentro

Di seguito vengono mostrati gli esempi:

Esempio: **<**

```
$variable < 100
```

Esempio: dentro, non dentro

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

Esempio:**! =**

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

Esempio: **==**

```
$variable == 1000
```

Tabelle per operatori

Operatore	Operatore di Amazon Fraud Detector
Equal to	==

Operatore	Operatore di Amazon Fraud Detector
Non uguale a	!=
Greater than	>
Less than	<
Maggiore o uguale a	>=
Minore o uguale a	<=
In	in
E	e
Oppure	oppure
Not	!

Matematica di base

È possibile utilizzare operatori matematici di base nell'espressione (ad esempio, +, -, *,/). Un tipico caso d'uso è quando è necessario combinare variabili durante la valutazione.

Nella regola seguente, stiamo aggiungendo la variabile `$variable_1` con `$variable_2` e controllando se il totale è inferiore a 10.

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

Dati della tabella matematica di base

Operatore	Operatore di Amazon Fraud Detector
In più	+
Meno	-
Multiply (Moltiplica)	*

Operatore	Operatore di Amazon Fraud Detector
Divide (Dividi)	/
Modulo	%

Espressione regolare (regex)

Puoi usare regex per cercare modelli specifici come parte della tua espressione. Ciò è particolarmente utile se stai cercando di abbinare una stringa o un valore numerico specifico per una delle tue variabili. Amazon Fraud Detector supporta match solo quando si lavora con espressioni regolari (ad esempio, restituisce True/False a seconda che la stringa fornita corrisponda all'espressione regolare). Il supporto per le espressioni regolari di Amazon Fraud Detector si basa su .matches () in java (utilizzando la libreria RE2J Regular Expression). Esistono diversi siti Web utili su Internet utili per testare diversi modelli di espressioni regolari.

Nel primo esempio riportato di seguito, trasformiamo innanzitutto la variabile `email` in lettere minuscole. Controlliamo quindi se il pattern `@gmail.com` è nella `email` variabile. Notate che il secondo periodo è scappato in modo da poter controllare esplicitamente la stringa. `.com`

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

Nel secondo esempio, controlliamo se la variabile `phone_number` contiene il prefisso internazionale +1 per determinare se il numero di telefono proviene dagli Stati Uniti. Il simbolo più viene eliminato in modo da poter verificare in modo esplicito la presenza della stringa. `+1`

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

Tabella Regex

Operatore	Esempio di Amazon Fraud Detector
Trova qualsiasi stringa che inizia con	regex_match («^mystring», $ variabile)
Corrisponde esattamente all'intera stringa	regex_match («mystring», $ variabile)
Corrisponde a qualsiasi carattere tranne la nuova riga	regex_match (» . «, $ variabile)

Operatore	Esempio di Amazon Fraud Detector
Corrisponde a qualsiasi numero di caratteri tranne la nuova riga precedente a «mystring»	regex_match (». *mystring», $ variabile)
Fuggi dai caratteri speciali	\

Verifica dei valori mancanti

A volte è utile verificare se il valore è mancante. In Amazon Fraud Detector questo valore è rappresentato da null. È possibile eseguire questa operazione utilizzando la seguente sintassi:

```
$variable != null
```

Allo stesso modo, se desideri verificare se un valore non è presente, puoi fare quanto segue:

```
$variable == null
```

Condizioni multiple

È possibile combinare più espressioni utilizzando `and` e`or`. Amazon Fraud Detector si ferma in un'0Respressione quando viene trovato un singolo valore vero e si ferma in un'espressione `AND` quando viene trovato un singolo valore falso.

Nell'esempio seguente, stiamo verificando due condizioni utilizzando la `and` condizione. Nella prima dichiarazione, stiamo controllando se la variabile 1 è inferiore a 100. Nel secondo controlliamo se la variabile 2 non è gli Stati Uniti.

Dato che la regola utilizza un`and`, entrambi devono essere VERI affinché l'intera condizione venga valutata come VERA.

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

È possibile utilizzare le parentesi per raggruppare le operazioni booleane, come illustrato di seguito:

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

Altri tipi di espressione

DateTimefunzioni

Funzione	Descrizione	Esempio
getcurren tdatetime ()	Fornisce l'ora corrente dell'esec uzione della regola in formato UTC ISO8601. Puoi usare getepochm illiseconds (getcurrentdatetime ()) per eseguire operazioni aggiuntive	getcurrentdatetime () == «2023-03-28T 18:34:02 Z»
è prima (DateTime1, DateTime 2)	Restituisce un valore booleano (vero/falso) se il chiamante DateTime 1 è precedente a 2 DateTime	isbefore (getcurrentdatetime (), «2019-11-30T 01:01:01 Z») == «Falso» isbefore (getcurrentdatetime (), «2050-11-30T 01:05:01 Z») == «Vero»
dopo (DateTime1, DateTime 2)	Restituisce un valore booleano (vero/falso) se il chiamante DateTime 1 è dopo 2 DateTime	isafter (getcurrentdatetime (), «2019-11-30T 01:01:01 Z») == «Vero» isafter (getcurrentdatetime (), «2050-11-30T 01:05:01 Z») == «Falso»
ottieni epoche millisecondi () DateTime	Prende a DateTime e lo restituis ce DateTime in millisecondi di epoca. Utile per eseguire operazioni matematiche sulla data	getepoche millisecondi («2019-11 -30T 01:01:01 Z») = 1575032461

Operatori di stringa

Operatore	Esempio
Trasforma la stringa in maiuscolo	maiuscolo ($ variabile)
Trasforma una stringa in lettere minuscole	minuscolo ($ variabile)

Altro

Operatore	Commento
Aggiungi un commento	# il mio commento

Crea regole

Puoi creare regole nella console Amazon Fraud Detector, utilizzando il comando create-rule, utilizzando l'CreateRuleAPI o utilizzando il. AWS SDK for Python (Boto3)

Ogni regola deve contenere una singola espressione che catturi la logica aziendale. Tutte le espressioni devono restituire un valore booleano (vero o falso) e avere una lunghezza inferiore a 4.000 caratteri. Le condizioni di tipo if-else non sono supportate. Tutte le variabili utilizzate nell'espressione devono essere predefinite nel tipo di evento valutato. Allo stesso modo, tutti gli elenchi utilizzati nell'espressione devono essere predefiniti, associati a un tipo di variabile e compilati con voci.

L'esempio seguente crea una regola `high_risk` per un rilevatore `payments_detector` esistente. La regola associa un'espressione e un risultato `verify_customer` alla regola.

Prerequisiti

Per seguire i passaggi indicati di seguito, assicurati di completare quanto segue prima di procedere con la creazione delle regole:

- Crea un rilevatore
- Crea un risultato

Se stai creando un rilevatore, una regola e un risultato per il tuo caso d'uso, sostituisci il nome del rilevatore di esempio, il nome della regola, l'espressione della regola e il nome del risultato con i nomi e le espressioni pertinenti al tuo caso d'uso.

Crea una nuova regola nella console Amazon Fraud Detector

1. Apri la console di AWS gestione e accedi al tuo account. Accedi ad Amazon Fraud Detector.
2. Nel riquadro di navigazione a sinistra, scegli Rilevatori e seleziona il rilevatore che hai creato per il tuo caso d'uso, ad esempio payments_detector.
3. Nella pagina payments_detector, scegli la scheda Regole associate e quindi scegli Crea regola.
4. Nella pagina Nuova regola, inserisci quanto segue:
   a. Nel Nome, inserisci un nome per la regola, ad esempio **`high_risk`**
   b. Nella casella Descrizione - opzionale, inserisci facoltativamente una descrizione della regola, ad esempio, **`This rule captures events with a high ML model score`**
   c. Nell'espressione, inserisci un'espressione di regola per il tuo caso d'uso utilizzando la guida di riferimento rapida Expression. Esempio `$sample_fraud_detection_model_insightscore >900`
   d. In Outcomes, scegli il risultato che hai creato per il tuo caso d'uso, ad esempio verify_customer. Un risultato è il risultato di una previsione di frode e viene restituito se la regola corrisponde durante una valutazione.
5. Scegli Salva regola

Hai creato una nuova regola per il tuo rilevatore. Questa è la versione 1 della regola che Amazon Fraud Detector rende automaticamente disponibile all'uso del rilevatore.

Crea una regola usando AWS SDK for Python (Boto3)

Il codice di esempio seguente utilizza CreateRulel'API per creare una regola `high_risk` per un rilevatore `payments_detector` esistente. Il codice di esempio aggiunge anche un'espressione di regola e un risultato `verify_customer` alla regola.

Prerequisiti

Per utilizzare il codice di esempio, assicurati di aver completato quanto segue prima di procedere con la creazione delle regole:

- Crea un rilevatore
- Crea un risultato

Se stai creando un rilevatore, una regola e un risultato per il tuo caso d'uso, sostituisci il nome del rilevatore di esempio, il nome della regola, l'espressione della regola e il nome del risultato con nomi ed espressioni pertinenti al tuo caso d'uso.

```
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']
)
```

Hai creato la versione 1 della regola che Amazon Fraud Detector mette automaticamente a disposizione del rilevatore.

Regola di aggiornamento

Puoi aggiornare una regola in qualsiasi momento aggiungendo o aggiornando la descrizione della regola, aggiornando l'espressione della regola o aggiungendo o rimuovendo il risultato della regola. Quando si aggiorna una regola, viene creata una nuova versione della regola.

Puoi aggiornare una regola nella console Amazon Fraud Detector, utilizzando il update-rule-versioncomando, utilizzando l'UpdateRuleVersionAPI o utilizzando l'AWSSDK.

Dopo aver aggiornato la regola, assicurati di aggiornare la versione del rilevatore per utilizzare la nuova versione della regola.

Aggiorna la regola nella console Amazon Fraud Detector

Per aggiornare una regola,

1. Apri la console di AWS gestione e accedi al tuo account. Accedi ad Amazon Fraud Detector.
2. Nel riquadro di navigazione a sinistra, scegli Rilevatori.

3. Nel riquadro Rilevatori, seleziona il rilevatore associato alla regola che desideri aggiornare.
4. Nella pagina del rilevatore, scegli la scheda Regole associate e seleziona la regola che desideri aggiornare.
5. Nella pagina delle regole, scegli Azioni e seleziona Crea versione.
6. Nota che la versione è cambiata. Inserisci una descrizione, un'espressione o un risultato aggiornati.
7. Scegli Salva nuova versione

Aggiorna la regola utilizzando AWS SDK for Python (Boto3)

Il codice di esempio seguente utilizza l'UpdateRuleVersionAPI per aggiornare la soglia della regola `high_risk` da 900 a 950. Questa regola è associata al rilevatore`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']
)
```

Elenchi

Un elenco è un set di dati di input per una variabile nel set di dati dell'evento. I dati di input vengono utilizzati in una regola associata al rilevatore. Una regola è una condizione che indica ad Amazon Fraud Detector come interpretare i dati di input durante una previsione di frode. Ad esempio, è possibile creare un elenco di indirizzi IP e quindi creare una regola per negare l'accesso se nell'elenco è presente un indirizzo IP specifico. Le regole che utilizzano gli elenchi sono espresse`$ip_address_value` nel`@list_name` formato in.

Con Amazon Fraud Detector, puoi gestire un elenco aggiungendo o rimuovendo dati senza dover aggiornare una regola associata. Una regola associata all'elenco incorpora automaticamente i dati appena aggiunti o rimossi.

Un elenco può contenere fino a 100.000 voci univoche e ogni voce può contenere fino a 320 caratteri. Ogni elenco utilizzato in una regola è, per impostazione predefinita, associato aTipi variabili FREE_FORM_TEXT di Amazon Fraud Detector. Puoi assegnare un tipo di variabile all'elenco in qualsiasi momento. È possibile utilizzare fino a 3 elenchi in una regola.

Puoi creare un elenco, aggiungere voci all'elenco, eliminare un elenco o eliminare una o più voci nell'elenco oppure assegnare un tipo di variabile all'elenco nella console di Amazon Fraud Detector, utilizzando l'API, utilizzando o utilizzando l'AWSSDK.AWS CLI

Creazione di un elenco

È possibile creare un elenco contenente i dati di input (voci) di una variabile nel set di dati dell'evento e utilizzare l'elenco nell'espressione delle regole. Le voci dell'elenco possono essere gestite dinamicamente senza aggiornare la regola che utilizza l'elenco.

Per creare un elenco, devi prima specificare un nome e poi, facoltativamente, associare l'elenco a un elencoTipi variabili supportato da Amazon Fraud Detector. Per impostazione predefinita, Amazon Fraud Detector presuppone che l'elenco sia di tipo variabile FREE_FORM_TEXT.

Puoi creare un elenco nella console di Amazon Fraud Detector, utilizzando l'APIAWS CLI, utilizzando o utilizzando l'AWSSDK.

Crea un elenco utilizzando la console Amazon Fraud Detector

Creazione di un elenco

1. Apri la console diAWS gestione e accedi al tuo account. Passa ad Amazon Amazon Amazon Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra, scegli Liste.
3. In Dettagli degli elenchi
    a. Nel Nome dell'elenco, inserisci un nome per l'elenco.
    b. Nella Descrizione, inserisci una descrizione.
    c. (Facoltativo) Nel campo Tipo variabile, seleziona un tipo di variabile per l'elenco.

> **Important**
>
> Se l'elenco contiene indirizzi IP, assicurati di selezionare IP_ADDRESS come tipo di variabile. Se non selezioni un tipo di variabile, Amazon Fraud Detector presuppone che l'elenco sia di tipo variabile FREE_FORM_TEXT.

4. In Aggiungi dati di elenco, aggiungi le voci dell'elenco, una voce per riga. Puoi anche copiare e incollare le voci da un foglio di calcolo.

> **Note**
>
> Assicurati che le voci non siano separate da una virgola e siano univoche nell'elenco. Se vengono inserite due voci identiche, ne verrà aggiunta solo una.

5. Seleziona Create (Crea).

Crea un elenco usandoAWS SDK for Python (Boto3)

Si crea un elenco specificando un nome di elenco. Puoi facoltativamente fornire una descrizione, associare un tipo di variabile o aggiungere voci all'elenco durante la creazione di un elenco. In alternativa, puoi aggiornare l'elenco in un secondo momento aggiungendo delle voci o una descrizione. Puoi assegnare un tipo di variabile all'elenco in un secondo momento se non l'hai assegnato al momento della creazione dell'elenco. Il tipo di variabile di un elenco non può essere modificato dopo l'assegnazione.

> **Important**
>
> Se l'elenco contiene indirizzi IP, assicurati di assegnare IP_ADDRESS come tipo di variabile. Se non assegni un tipo di variabile, Amazon Fraud Detector presuppone che l'elenco sia di tipo variabile FREE_FORM_TEXT.

L'esempio seguente utilizza l'operazione CreateListAPI per creare un`allow_email_ids` elenco fornendo una descrizione, un tipo di variabile e aggiungendo quattro voci di elenco.

```
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']
     )
```

Aggiungere voci in un elenco

Dopo aver creato l'elenco, puoi aggiungere o aggiungere voci all'elenco in qualsiasi momento. Quando si aggiungono o si aggiungono voci nell'elenco, non è necessario aggiornare la regola a cui è associato l'elenco. La regola incorpora automaticamente le nuove voci aggiunte.

L'elenco può contenere fino a 100.000 voci uniche e ogni voce può contenere fino a 320 caratteri.

Puoi aggiungere voci nella console di Amazon Fraud Detector, utilizzando l'APIAWS CLI, utilizzando o utilizzando l'AWSSDK.

Aggiungere voci in un elenco utilizzando la console Amazon Fraud Detector

Per aggiungere una o più voci in un elenco

1. Apri la console diAWS gestione e accedi al tuo account. Passa ad Amazon Amazon Amazon Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra, scegli Liste.
3. Nella pagina Elenchi, seleziona l'elenco a cui desideri aggiungere le voci.
4. Nella pagina dei dettagli dell'elenco, seleziona la scheda Elenca dati e scegli Aggiungi dati.
5. Nella casella Aggiungi dati dell'elenco, aggiungi una voce in ogni riga o copia e incolla le voci da un foglio di calcolo. Assicurati di non utilizzare la virgola per separare le voci.
6. Scegli Add (Aggiungi).

Aggiungere voci in un elenco utilizzando ilAWS SDK for Python (Boto3)

L'esempio seguente utilizza l'operazione UpdateListAPI per aggiungere due nuove voci nell'`allow_email_ids`elenco. Assicurati che le voci che stai aggiungendo siano uniche nell'elenco.

```
import boto3
```

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

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

Assegnare un tipo di variabile a un elenco

Ogni elenco utilizzato in una regola deve essere associato al tipo diTipi variabili variabile di Amazon Fraud Detector. Per impostazione predefinita, Amazon Fraud Detector presuppone che l'elenco sia di tipo variabile FREE_FORM_TEXT. È importante notare che un elenco composto da indirizzi IP deve essere associato al tipo di variabile IP_ADDRESS.

È possibile associare l'elenco a un tipo di variabile al momento della creazione dell'elenco o in qualsiasi momento successivo. Se hai già associato l'elenco a un tipo di variabile e desideri modificarlo in seguito, devi creare un nuovo elenco. Non è possibile modificare il tipo di variabile di un elenco.

Puoi assegnare un tipo di variabile nella console di Amazon Fraud Detector, utilizzando l'APIAWS CLI, utilizzando o utilizzando l'AWSSDK.

Assegna un tipo di variabile a un elenco utilizzando la console Amazon Fraud Detector

Per assegnare un tipo di variabile a un elenco

1. Apri la console diAWS gestione e accedi al tuo account. Passa ad Amazon Amazon Amazon Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra, scegli Liste.
3. Nella pagina Elenchi, seleziona l'elenco a cui desideri assegnare un tipo di variabile.
4. Nella pagina dei dettagli dell'elenco, scegli Azioni e seleziona Modifica elenco.
5. Nella casella Modifica elenco, seleziona il tipo di variabile per l'elenco.
6. Seleziona Salva.

Assegna il tipo di variabile a un elenco utilizzando ilAWS SDK for Python (Boto3)

L'esempio seguente utilizza l'operazione UpdateListAPI per assegnare un tipo di variabile all'`allow_ip_address`elenco.

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

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

Eliminazione di un elenco

È possibile eliminare un elenco che non viene utilizzato in nessuna regola. Quando elimini un elenco, Amazon Fraud Detector elimina definitivamente tale elenco e tutte le sue voci.

Puoi eliminare un elenco nella console di Amazon Fraud Detector, utilizzando l'APIAWS CLI o l'AWSSDK.

Elimina l'elenco utilizzando la console Amazon Fraud Detector

Come eliminare un elenco

1. Apri la console diAWS gestione e accedi al tuo account. Passa ad Amazon Amazon Amazon Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra, scegli Liste.
3. Nella pagina Elenchi, seleziona l'elenco che intendi copiare.
4. Nella pagina dei dettagli dell'elenco, scegli Azioni e seleziona Elimina elenco.
5. Scegli Elimina elenco.

Eliminare l'elenco utilizzandoAWS SDK for Python (Boto3)

L'esempio seguente utilizza l'operazione DeleteListAPI per eliminare`allow_email_ids`.

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

Eliminare le voci da un elenco

Puoi eliminare una o più voci dai tuoi elenchi in qualsiasi momento. Quando si eliminano le voci dall'elenco, non è necessario aggiornare la regola a cui è associato l'elenco. La regola incorpora automaticamente l'elenco aggiornato.

Puoi eliminare le voci da un elenco nella console di Amazon Fraud Detector, utilizzando l'APIAWS CLI o l'AWSSDK.

Elimina le voci da un elenco utilizzando la console Amazon Fraud Detector

Come eliminare una o più voci da un elenco

1. Apri la console diAWS gestione e accedi al tuo account. Passa ad Amazon Amazon Amazon Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra, scegli Liste.
3. Nella pagina Elenchi, seleziona l'elenco che contiene le voci da eliminare.
4. Nella pagina dei dettagli dell'elenco, seleziona la scheda Elenca dati e seleziona le voci che desideri eliminare.
5. Scegli Elimina e scegli nuovamente Elimina per confermare.

Eliminare le voci da un elenco utilizzandoAWS SDK for Python (Boto3)

Nell'esempio seguente l'operazione UpdateListAPI elimina le voci dall'`allow_email_ids`elenco.

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

Eliminare tutte le voci da un elenco

Puoi eliminare tutte le voci dell'elenco, se l'elenco non viene utilizzato in una regola. È possibile eliminare tutte le voci presenti nell'elenco e successivamente aggiungere voci nello stesso elenco.

Puoi eliminare le voci da un elenco nella console di Amazon Fraud Detector, utilizzando l'APIAWS CLI o l'AWSSDK.

Elimina tutte le voci da un elenco utilizzando la console Amazon Fraud Detector

Per eliminare tutte le voci da un elenco

1. Apri la console diAWS gestione e accedi al tuo account. Passa ad Amazon Amazon Amazon Amazon Fraud Detector.
2. Nel pannello di navigazione a sinistra, scegli Liste.
3. Nella pagina Elenchi, seleziona l'elenco che contiene le voci da eliminare.
4. Nella pagina dei dettagli dell'elenco, seleziona la scheda Elenca dati e scegli Elimina tutto.
5. Nella casella Elimina tutto, digita`delete all` per confermare, quindi scegli Elimina tutti i dati dell'elenco.

Eliminare tutte le voci da un elenco utilizzandoAWS SDK for Python (Boto3)

Nell'esempio seguente l'operazione UpdateListAPI elimina tutte le voci dall'`allow_email_ids`elenco.

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

Esiti

Un risultato è il risultato di una previsione di frode. Puoi creare un risultato per ogni possibile risultato di previsione delle frodi. Ad esempio, potresti voler che i risultati rappresentino i livelli di rischio (rischio elevato, medio e basso rischio) o le azioni (approvazione, revisione). Dopo la creazione di un risultato, puoi aggiungere a una regola uno o più risultati. Come parte della GetEventPredictionrisposta, Amazon Fraud Detector restituisce i risultati definiti per ogni regola corrispondente.

Crea un risultato

Puoi creare risultati nella console di Amazon Fraud Detector, utilizzando il comando put-outcome, utilizzando l'PutOutcomeAPI o utilizzando ilAWS SDK for Python (Boto3).

Crea un risultato utilizzando la console Amazon Fraud Detector

Per creare uno o più risultati,

1. Apri la console diAWS gestione e accedi al tuo account. Passa ad Amazon Fraud Detector.
2. Nel riquadro di navigazione a sinistra, scegliere Risultati.
3. Nella pagina Risultati, scegli Crea.
4. Nella pagina Nuovi risultati, inserisci quanto segue:
    a. Nel nome del risultato, inserisci un nome per il risultato.
    b. Nella descrizione dei risultati, puoi inserire facoltativamente una descrizione.
5. Scegli Salva risultato.
6. Ripeti i passaggi da 2 a 5 per creare risultati aggiuntivi.

Crea un risultato usando ilAWS SDK for Python (Boto3)

L'esempio seguente utilizza l'`PutOutcome`API per creare tre risultati. Lo sono`verify_customer`, `review`, `approve`. Dopo aver creato i risultati, puoi assegnarli alle regole.

```
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'
)
```

Eliminare un risultato

Non puoi eliminare un risultato utilizzato in una versione di regola.

Quando elimini un risultato, Amazon Fraud Detector elimina definitivamente tale risultato e i dati non vengono più archiviati in Amazon Fraud Detector.

Puoi eliminare un risultato nella console di Amazon Fraud Detector, utilizzando il comando delete-outcome, utilizzando l'DeleteOutcomeAPI o utilizzando ilAWS SDK for Python (Boto3)

Elimina un risultato nella console Amazon Fraud Detector

Eliminare un risultato

1. Accedi allaAWS Management Console e apri la console Amazon Fraud Detector all'indirizzo https://console.aws.amazon.com/frauddetector.
2. Nel riquadro di navigazione sinistro della console Amazon Fraud Detector, scegli Risorse, quindi scegli Risultati.
3. Scegliere il risultato che si desidera eliminare.
4. Scegli Actions (Operazioni), quindi Delete (Elimina).
5. Inserisci il nome del risultato, quindi scegli Elimina risultato.

Eliminare un risultato utilizzando ilAWS SDK for Python (Boto3)

L'esempio seguente utilizza l'DeleteOutcomeAPI per eliminare il`verify_customer` risultato. Dopo l'eliminazione del risultato, non è più possibile assegnarlo a una regola.

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

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

Entità

Un'entità rappresenta una persona o una cosa che sta eseguendo l'evento. Un tipo di entità classifica l'entità. Le classificazioni di esempio includono cliente, commerciante, utente o account. Fornisci il tipo di entità (ENTITY_TYPE) e un identificatore di entità (ENTITY_ID) come parte del set di dati dell'evento per indicare l'entità specifica che ha eseguito l'evento.

Amazon Fraud Detector utilizza il tipo di entità quando genera una previsione delle frodi per un evento per indicare chi ha eseguito l'evento. Il tipo di entità che desideri utilizzare nelle tue previsioni di frode deve essere prima creato in Amazon Fraud Detector e quindi aggiunto all'evento durante la creazione del tipo di evento.

Creare un tipo di entità

Puoi creare un tipo di entità nella console di Amazon Fraud Detector, utilizzando il put-entity-typecomando, utilizzando l'PutEntityTypeAPI o utilizzando ilAWS SDK for Python (Boto3). Nel seguente esempio viene creato un tipo di entità`customer` nella console Amazon Fraud Detector utilizzando l'SDK for Python (Boto3). Se stai creando un tipo di entità da associare a un tipo di evento per addestrare un modello di rilevamento delle frodi, utilizza il tipo di entità dal set di dati dell'evento appropriato al tuo caso d'uso.

Crea un tipo di entità utilizzando la console Amazon Fraud Detector

Per creare un tipo di entità,

1. Apri la console diAWS gestione e accedi al tuo account.
2. Vai ad Amazon Fraud Detector, scegli Entità nella barra di navigazione a sinistra, quindi scegli Crea.
3. Nella pagina Crea entità, inserisci cliente come nome del tipo di entità. Facoltativamente, inserisci una descrizione dell'entità.
4. Scegliere Create entity (Crea entità).

Crea un tipo di entità utilizzando ilAWS SDK for Python (Boto3)

Il seguente esempio diAWS SDK for Python (Boto3) codice utilizza l'`PutEntityType`API per creare un tipo di entità`customer`. Se stai creando un tipo di entità da associare a un tipo di evento per addestrare un modello di rilevamento delle frodi, utilizza l'entità del set di dati dell'evento appropriata per il tuo caso d'uso.

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

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

Eliminare un tipo di entità

In Amazon Fraud Detector non è possibile eliminare un tipo di entità incluso in un tipo di evento. Dovrai prima eliminare il tipo di evento a cui è associata l'entità e quindi eliminare il tipo di entità.

Quando elimini un tipo di entità, Amazon Fraud Detector elimina definitivamente quel tipo di entità e i dati non vengono più archiviati in Amazon Fraud Detector.

Un tipo di entità può essere eliminato nella console di Amazon Fraud Detector, utilizzando il delete-entity-typecomando, utilizzando l'DeleteEntityTypeAPI o utilizzando ilAWS SDK for Python (Boto3)

Eliminare un tipo di entità nella console di Amazon Fraud Detector

Per eliminare un tipo di entità,

1. AccedereAWS Management Console e aprire la console Amazon Fraud Detector all'indirizzo https://console.aws.amazon.com/frauddetector.
2. Nel riquadro di navigazione sinistro della console Amazon Fraud Detector, scegli Risorse, quindi scegli Entità.
3. Scegliere il tipo di entità che si desidera eliminare.
4. Scegli Actions (Operazioni), quindi Delete (Elimina).
5. Inserisci il nome del tipo di entità, quindi scegli Elimina tipo di entità.

Eliminare il tipo di entità utilizzando ilAWS SDK for Python (Boto3)

Il seguente codice diAWS SDK for Python (Boto3) esempio elimina il tipo di entità customer utilizzando l'DeleteEntityTypeAPI.

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

```
fraudDetector.delete_entity_type (

name = 'customer'

)
```

Gestisci le risorse di Amazon Fraud Detector utilizzandoAWS CloudFormation

raector raector raector raector raector raector raector raector raector raector raector raector Fraud Detector raector raector raector raector raector raector raector raector raector raector raector raector raector raector raector raector raAWS CloudFormation Puoi creare un modello che descrive tutte le risorse Amazon Fraud Detector ra EntityType EventTypeAWS CloudFormation È possibile riutilizzare il modello per eseguire il provisioning e la configurazione delle risorse in modo coerente e ripetitivo in più regioni e account AWS per il provisioning e la configurazione delle risorse in modo coerente e ripetitivo in più regioni

L'utilizzo di AWS CloudFormation non costi supplementari costi supplementari supplementari costi supplementari supplementari

etector rarararararararararara

Per eseguire il provisioning e la configurazione delle risorse per Amazon Fraud Detector raector raector raector raector raector raector raector AWS CloudFormationraector raector I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse di cui intendi effettuare il provisioning negli stack AWS CloudFormation. Se non hai familiarità con JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a utilizzare i modelli AWS CloudFormation. Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation.

Puoi creare, aggiornare ed eliminare le risorse Amazon Fraud Detector raector raector raectorAWS CloudFormation raector Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per le risorse, consulta Riferimento ai tipi di risorse Amazon Fraud Detector raector raector raector raector raector AWS CloudFormationraector raector

Se lo stai già utilizzando CloudFormation, non è necessario gestire policy o CloudTrail registrazioni IAM aggiuntive.

raector raector raector raector raector raector rarara

Puoi creare, aggiornare ed eliminare gli stack di Amazon Fraud Detector tramite la CloudFormation console o tramite l'interfaccia a riga di comando di AWS.

Per creare uno stack, è necessario disporre di un modello che descrive quali risorse AWS CloudFormation verranno incluse nello stack. Puoi anche CloudFormation gestire le risorse di Amazon Fraud Detector che hai già creato importandole in uno stack nuovo o esistente.

Per istruzioni dettagliate sulla gestione degli stack, consulta la Guida perAWS CloudFormation l'utente per scoprire come creare, aggiornare ed eliminare gli stack.

raector raector raector raector raector Fraud Detector rarararara

Il modo in cui organizzi i tuoiAWS CloudFormation stack dipende interamente da te. In genere è consigliabile organizzare gli stack per ciclo di vita e proprietà. Ciò significa raggruppare le risorse in base alla frequenza con cui vengono modificate o in base ai team responsabili dell'aggiornamento.

Puoi scegliere di organizzare i tuoi stack creando uno stack per ogni rilevatore e la relativa logica di rilevamento (ad esempio regole, variabili, ecc.). Se utilizzi altri servizi, dovresti valutare se vuoi mettere insieme le risorse di Amazon Fraud Detector con le risorse di altri servizi. Ad esempio, potresti creare uno stack che includa risorse Kinesis che aiutano a raccogliere dati e risorse Amazon Fraud Detector che elaborano i dati. Questo può essere un modo efficace per garantire che tutti i prodotti del tuo team antifrode funzionino insieme.

raector raector raector raector raector raector CloudFormation ra

Oltre ai parametri standard disponibili in tutti i CloudFormation modelli, Amazon Fraud Detector introduce due parametri aggiuntivi che ti aiuteranno a gestire il comportamento di distribuzione. Se non includi uno o entrambi questi parametri, CloudFormation utilizzerà il valore predefinito mostrato di seguito.

Parametro	Valori	Valore predefinito
DetectorVersionStatus	ATTIVO: imposta la versione nuova/aggiornata del rilevatore sullo stato Attivo	BOZZA

Parametro	Valori	Valore predefinito
	BOZZA: imposta la nuova versione del rilevator e o aggiornata sullo stato Bozza	
In riga	TRraud: CloudFormation consente di creazione/aggiornamento/eliminazione della risorsa in fase di creazione/aggiornamento/eli minazione dello stack. FALSO: CloudFormation consente di convalida re l'esistenza dell'oggetto ma non di apportare modifiche all'oggetto.	TRUE

AWS CloudFormationModello di esempio per le risorse raector raector Fraud Detector raector ra

Di seguito è riportato un modelloAWS CloudFormation YAML di esempio per la gestione di un rilevatore e delle versioni del rilevatore di etector raector raector raector raector raector raector

```
# 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'
```

Ulteriori informazioni su AWS CloudFormation

Per ulteriori informazioni su AWS CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- Guida per l'utente di AWS CloudFormation
- Documentazione di riferimento dell'API AWS CloudFormation
- Guida per l'utente dell'interfaccia a riga di comando di AWS CloudFormation

Previsioni di frode

Puoi utilizzare Amazon Fraud Detector per ottenere previsioni di frode per un singolo evento in tempo reale oppure offline per una serie di eventi. Per generare previsioni antifrode per un singolo evento o per una serie di eventi, dovrai fornire ad Amazon Fraud Detector le seguenti informazioni:

- Logica di previsione di frode
- Metadati degli eventi

Logica di rilevamento delle frodi

La logica di previsione delle frodi utilizza una o più regole per valutare i dati associati a un evento e quindi fornisce un risultato e un punteggio di previsione delle frodi. Crei la tua logica di previsione delle frodi utilizzando i seguenti componenti:

- Tipi di evento: definisce la struttura dell'evento
- Modelli: definisce i requisiti di algoritmi e dati per la previsione delle frodi
- Variabili: rappresenta un elemento di dati associato all'evento
- Regole: indica ad Amazon Fraud Detector come interpretare i valori delle variabili durante la previsione di frode
- Risultati: risultati generati da una previsione di frode
- Versione del rilevatore: contiene la logica di previsione delle frodi per un particolare evento

Per ulteriori informazioni sui componenti utilizzati per creare la logica di rilevamento delle frodi, consulta i concetti di Amazon Fraud Detector. Prima di iniziare a generare previsioni di frode, assicurati di aver creato e pubblicato la versione del rilevatore che contiene la tua logica di previsione delle frodi. È possibile creare e pubblicare la versione del rilevatore utilizzando la console o l'API Fraud Detector. Per istruzioni su come usare la console, consulta Guida introduttiva (console). Per istruzioni sull'utilizzo dell'API, consulta Creare una versione del rilevatore.

Metadati degli eventi

I metadati degli eventi forniscono dettagli sull'evento da valutare. Ogni evento che si desidera valutare deve includere il valore per ogni variabile nel tipo di evento associato alla versione del rilevatore. Inoltre, i metadati degli eventi devono includere i seguenti parametri:

- EVENT_ID — Un identificatore per l'evento. Ad esempio, se l'evento è una transazione online, EVENT_ID potrebbe essere il numero di riferimento della transazione fornito al cliente.

  Note importanti su EVENT_ID

  - Deve essere unico per quell'evento
  - Dovrebbe rappresentare informazioni significative per la tua attività
  - Deve soddisfare il modello di espressione regolare:`^[0-9a-z_-]+$.`
  - Deve essere salvato. EVENT_ID è il riferimento per l'evento e viene utilizzato per eseguire operazioni sull'evento, ad esempio eliminarlo.
  - L'aggiunta di timestamp a EVENT_ID non è consigliata in quanto potrebbe causare problemi quando in seguito si desidera aggiornare l'evento, poiché sarà necessario fornire esattamente lo stesso EVENT_ID.
- ENTITY_TYPE — L'entità che esegue l'evento, ad esempio un commerciante o un cliente.
- ENTITY_ID - Un identificatore per l'entità che esegue l'evento. L'ENTITY_ID deve soddisfare il seguente schema di espressione regolare:`^[0-9a-z_-]+$`. Se ENTITY_ID non è disponibile al momento della valutazione, passa la stringa unknown.
- EVENT_TIMESTAMP - Timestamp quando si è verificato l'evento. La timestamp deve essere nello standard ISO 8601 in UTC.

Previsione in tempo reale

Puoi valutare le attività online per individuare eventuali frodi in tempo reale chiamando`GetEventPrediction` l'API. Fornisci informazioni su un singolo evento in ogni richiesta e ricevi in modo sincrono un punteggio del modello e un risultato in base alla logica di previsione delle frodi associata al rilevatore specificato.

Come funziona la previsione delle frodi in tempo reale

L'`GetEventPrediction`API utilizza una versione del rilevatore specificata per valutare i metadati dell'evento forniti per l'evento. Durante la valutazione, Amazon Fraud Detector genera innanzitutto i punteggi dei modelli che vengono aggiunti alla versione del rilevatore, quindi passa i risultati alle regole per la valutazione. Le regole vengono eseguite come specificato dalla modalità di esecuzione delle regole (vedere Creare una versione del rilevatore). Come parte della risposta, Amazon Fraud Detector fornisce i punteggi dei modelli e tutti i risultati associati alle regole corrispondenti.

Ottenere una previsione delle frodi in tempo reale

Per ottenere previsioni sulle frodi in tempo reale, assicurati di aver creato e pubblicato un rilevatore che contenga il tuo modello e le tue regole di previsione delle frodi o semplicemente un set di regole.

Puoi ottenere una previsione delle frodi per un evento in tempo reale chiamando l'operazione GetEventPredictionAPI utilizzando l'interfaccia a riga diAWS comando (AWSCLI) o uno degli SDK di Amazon Fraud Detector.

Per utilizzare l'API, fornisci le informazioni di un singolo evento con ogni richiesta. Come parte della richiesta, devi specificare`detectorId` che Amazon Fraud Detector utilizzerà per valutare l'evento. È inoltre possibile specificare un`detectorVersionId`. Se non`detectorVersionId` viene specificato un valore, Amazon Fraud Detector utilizzerà la`ACTIVE` versione del rilevatore.

Facoltativamente, puoi inviare dati per richiamare un SageMaker modello passando i dati nel campo`externalModelEndpointBlobs`.

Ottieni una previsione delle frodi utilizzando ilAWS SDK for Python (Boto3)

Per generare una previsione delle frodi, chiama l'`GetEventPrediction`API. L'esempio seguente presuppone che tu abbia completatoParte B: Generazione di previsioni sulle frodi. Come parte della risposta, riceverai un punteggio del modello, nonché tutte le regole corrispondenti e i risultati corrispondenti. Puoi trovare altri esempi di`GetEventPrediction` richieste nel aws-fraud-detector-samples GitHub repository.

```
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'
}
)
```

Previsioni in batch

Puoi utilizzare un processo di previsione in batch in Amazon Fraud Detector per ottenere previsioni per una serie di eventi che non richiedono punteggi in tempo reale. Ad esempio, è possibile creare un processo di previsione in batch per eseguire un processo offline proof-of-concept o per valutare retrospettivamente il rischio di eventi su base oraria, giornaliera o settimanale.

Puoi creare un processo di previsione batch utilizzando la console Amazon Fraud Detector o richiamando l'operazione CreateBatchPredictionJobAPI utilizzando l'interfaccia a riga di AWS comando (AWSCLI) o uno degli SDK di Amazon Fraud Detector.

Argomenti

- Come funzionano le previsioni in batch
- File di input e output
- Ottenere previsioni in batch
- Guida sui ruoli IAM
- Ottieni previsioni di frode in batch utilizzando AWS SDK for Python (Boto3)

Come funzionano le previsioni in batch

L'operazione `CreateBatchPredictionJob` API utilizza una versione del rilevatore specificata per effettuare previsioni basate sui dati forniti in un file CSV di input che si trova in un bucket Amazon S3. L'API restituisce quindi il file CSV risultante in un bucket S3.

I processi di previsione in batch calcolano i punteggi dei modelli e i risultati di previsione allo stesso modo dell'operazione. `GetEventPrediction` Analogamente a`GetEventPrediction`, per creare un processo di previsione in batch, è necessario innanzitutto creare un tipo di evento, eventualmente addestrare un modello e quindi creare una versione del rilevatore che valuti gli eventi nel processo batch.

I prezzi per i punteggi di rischio degli eventi valutati dai processi di previsione in batch sono gli stessi dei prezzi per i punteggi creati dall'API. `GetEventPrediction` Per maggiori dettagli, consulta i prezzi di Amazon Fraud Detector.

È possibile eseguire un solo processo di previsione batch alla volta.

File di input e output

Il file CSV di input deve contenere intestazioni che corrispondono al tipo di evento associato alla versione del rilevatore selezionata. La dimensione massima del file di dati di input è 1 GB. Il numero di eventi varierà in base alle dimensioni dell'evento.

Amazon Fraud Detector crea il file di output nello stesso bucket del file di input, a meno che tu non specifichi una posizione separata per i dati di output. Il file di output contiene i dati originali del file di input e le seguenti colonne aggiunte:

- `MODEL_SCORES`— Descrive in dettaglio i punteggi del modello per l'evento di ciascun modello associato alla versione del rilevatore selezionata.
- `OUTCOMES`— Descrive in dettaglio i risultati dell'evento valutati dalla versione del rilevatore selezionata e dalle relative regole.
- `STATUS`— Indica se l'evento è stato valutato con successo. Se l'evento non è stato valutato correttamente, questa colonna mostra un codice di motivazione dell'errore.
- `RULE_RESULTS`— Un elenco di tutte le regole corrispondenti, in base alla modalità di esecuzione delle regole.

Ottenere previsioni in batch

I passaggi seguenti presuppongono che tu abbia già creato un tipo di evento, addestrato un modello utilizzando quel tipo di evento (opzionale) e creato una versione del rilevatore per quel tipo di evento.

Per ottenere una previsione batch

1. Accedi alla AWS Management Console e apri la console Amazon Fraud Amazon Fraud all'indirizzo https://console.aws.amazon.com/frauddetector.
2. Nel riquadro di navigazione a sinistra della console Amazon Fraud Detector, scegli Previsioni batch, quindi scegli Nuova previsione batch.
3. In Nome Job, specifica un nome per il processo di previsione batch. Se non specifichi un nome, Amazon Fraud Detector genera casualmente un nome di lavoro.
4. In Detector, scegli il rilevatore per questa previsione batch.
5. Nella versione Detector, scegli la versione del rilevatore per questa previsione batch. Puoi scegliere una versione del rilevatore in qualsiasi stato. Se il rilevatore ha una versione del

rilevatore in `Active` stato, tale versione viene selezionata automaticamente, ma è anche possibile modificare questa selezione, se necessario.

6. Nel ruolo IAM, scegli o crea un ruolo con accesso di lettura e scrittura ai tuoi bucket Amazon S3 di input e output. Per ulteriori informazioni, consulta Guida sui ruoli IAM.

   Per ottenere previsioni batch, il ruolo IAM che chiama l'`CreateBatchPredictionJob`operazione deve disporre delle autorizzazioni di lettura nel bucket S3 di input e delle autorizzazioni di scrittura nel bucket S3 di output. Per ulteriori informazioni sulle autorizzazioni dei bucket, consulta gli esempi di policy per gli utenti nella Guida per l'utente di Amazon S3.

7. In Posizione dei dati di input, specifica la posizione Amazon S3 dei tuoi dati di input. Se desideri che il file di output si trovi in un bucket S3 diverso, seleziona Separate data location for output e fornisci la posizione Amazon S3 per i tuoi dati di output.
8. (Facoltativo) Crea tag per il tuo processo di previsione in batch.
9. Scegli Start (Avvia).

   Amazon Fraud Detector crea il processo di previsione batch e lo stato del processo è. `In progress` I tempi di elaborazione dei processi di previsione in batch variano a seconda del numero di eventi e della configurazione della versione del rilevatore.

Per interrompere un processo di previsione batch in corso, vai alla pagina dei dettagli del processo di previsione batch, scegli Azioni, quindi scegli Interrompi previsione batch. Se interrompi un processo di previsione in batch, non riceverai alcun risultato per il processo.

Quando lo stato del processo di previsione batch cambia in`Complete`, puoi recuperare l'output del processo dal bucket Amazon S3 di output designato. Il nome del file di output è nel formato`batch prediction job name_file creation timestamp_output.csv`. Ad esempio, il file di output di un job denominato `mybatchjob` è`mybatchjob_ 1611170650_output.csv`.

Per cercare eventi specifici valutati da un processo di previsione in batch, nel riquadro di navigazione a sinistra della console Amazon Fraud Detector, scegli Cerca previsioni precedenti.

Per eliminare un processo di previsione batch completato, vai alla pagina dei dettagli del processo di previsione batch, scegli Azioni e quindi scegli Elimina previsione batch.

Guida sui ruoli IAM

Per ottenere previsioni batch, il ruolo IAM che chiama l'CreateBatchPredictionJoboperazione deve disporre delle autorizzazioni di lettura nel bucket S3 di input e delle autorizzazioni di scrittura nel bucket S3 di output. Per ulteriori informazioni sulle autorizzazioni bucket, consulta Esempi di policy bucket nella Guida per l'utente di Amazon S3. Sulla console Amazon Fraud Detector, hai tre opzioni per selezionare un ruolo IAM per Batch Predictions:

1. Crea un ruolo quando crei un nuovo job di Batch Prediction.
2. Seleziona un ruolo IAM esistente che hai creato in precedenza nella console Amazon Fraud Detector. Assicurati di aggiungere l'`S3:PutObject`autorizzazione al ruolo prima di eseguire questo passaggio.
3. Inserisci un ARN personalizzato per un ruolo IAM creato in precedenza.

Se viene visualizzato un errore relativo al tuo ruolo IAM, verifica quanto segue:

1. I bucket di input e output Amazon S3 si trovano nella stessa regione del tuo rilevatore.
2. Il ruolo IAM che stai utilizzando ha l'`s3:GetObject`autorizzazione per il tuo bucket S3 di input e l'`s3:PutObject`autorizzazione per il tuo bucket S3 di output.
3. Il ruolo IAM che stai utilizzando ha una politica di affidabilità per il responsabile del servizio`frauddetector.amazonaws.com`.

Ottieni previsioni di frode in batch utilizzando AWS SDK for Python (Boto3)

Nell'esempio seguente viene illustrata una risposta di esempio per l'CreateBatchPredictionJobAPI. Un processo di previsione batch deve includere le seguenti risorse esistenti: rilevatore, versione del rilevatore e nome del tipo di evento. L'esempio seguente presuppone che tu abbia creato un tipo di evento`sample_registration`, un rilevatore e una `sample_detector` versione del rilevatore. 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-
**'
)
```

Spiegazioni delle previsioni

Le spiegazioni delle previsioni forniscono informazioni su come ogni variabile di evento ha influito sul punteggio di previsione delle frodi del modello e vengono generate automaticamente come parte della previsione delle frodi. Ogni previsione di frode ha un punteggio di rischio compreso tra 1 e 1000. Le spiegazioni relative alle previsioni forniscono dettagli sull'influenza di ogni variabile di evento sui punteggi di rischio in termini di entità (0-5, 5 è il valore più alto) e direzione (punteggio di guida più alto o più basso). Puoi anche utilizzare le spiegazioni di previsione per le seguenti attività:

- Identificare i principali indicatori di rischio durante le indagini manuali quando un evento viene segnalato per essere esaminato.
- Per restringere le cause profonde che portano a previsioni false positive (ad esempio, punteggi di rischio elevati per eventi legittimi).
- Per analizzare i modelli di frode tra i dati relativi agli eventi e rilevare eventuali distorsioni nel set di dati.

> **Important**
>
> Le spiegazioni delle previsioni vengono generate automaticamente e sono disponibili solo per i modelli addestrati a partire dal 30 giugno 2021. Per ricevere spiegazioni di previsione per i modelli addestrati prima del 30 giugno 2021, riqualifica tali modelli.

Le spiegazioni delle previsioni forniscono il seguente set di valori per ogni variabile di evento utilizzata per addestrare il modello.

Impatto relativo

Fornisce un riferimento visivo dell'impatto della variabile in termini di entità sui punteggi di previsione delle frodi. I valori di impatto relativo sono costituiti da una valutazione a stelle (0-5, 5 è il valore più alto) e dalla direzione (aumento/diminuito) dell'impatto del rischio di frode.

- Le variabili che aumentano il rischio di frode sono indicate da stelle rosse. Più alto è il numero di stelle rosse, più la variabile aumenta il punteggio di frode e aumenta la probabilità di frode.
- Le variabili che riducono il rischio di frode sono indicate da stelle di colore verde. Più alto è il numero di partenze di colore verde, più la variabile riduce il punteggio di rischio di frode e diminuisce la probabilità di frode.
- Il numero zero di stelle per tutte le variabili indica che nessuna delle variabili da sola ha modificato in modo significativo il rischio di frode.

Valore esplicativo non elaborato

Fornisce un valore grezzo e non interpretato rappresentato come probabilità logaritmica della frode. Questi valori sono generalmente compresi tra -10 e +10, ma vanno da - infinito a + infinito.

- Un valore positivo indica che la variabile ha fatto salire il punteggio di rischio.
- Un valore negativo indica che la variabile ha ridotto il punteggio di rischio.

Nella console Amazon Fraud Detector, i valori di spiegazione delle previsioni vengono visualizzati come segue. Le classificazioni a stelle colorate e i corrispondenti valori numerici grezzi consentono di vedere facilmente l'influenza relativa tra le variabili.

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

Visualizzazione delle spiegazioni delle previsioni

Dopo aver generato le previsioni di frode, puoi visualizzare le spiegazioni delle previsioni nella console Amazon Fraud Detector. Per visualizzare le spiegazioni delle previsioni utilizzando le API dell'AWSSDK, devi prima chiamare l'API per ottenere il timestamp di previsione dell'evento, quindi chiamare l'`ListEventPrediction`API per ottenere le spiegazioni delle previsioni. `GetEventPredictionMetadata`

Visualizza le spiegazioni delle previsioni utilizzando la console Amazon Fraud Detector

Per visualizzare le spiegazioni delle previsioni utilizzando la console,

1. Apri la AWS console e accedi al tuo account. Accedi ad Amazon Fraud Detector.
2. Nel riquadro di navigazione a sinistra, scegli Cerca previsioni precedenti.
3. Usa i filtri Proprietà, Operatore e Valore per selezionare la previsione che desideri rivedere.

4. Nel riquadro Filtro superiore, assicurati di selezionare il periodo di tempo in cui è stata generata la previsione che desideri rivedere.
5. Il riquadro Risultati mostra un elenco di tutte le previsioni generate durante il periodo di tempo specificato. Fai clic sull'ID evento della previsione per visualizzare le spiegazioni della previsione.
6. Scorri verso il basso fino al riquadro delle spiegazioni delle previsioni.
7. Imposta il pulsante Mostra il valore non elaborato della spiegazione della previsione per visualizzare il valore non elaborato della spiegazione della previsione di tutte le variabili.

Visualizza le spiegazioni delle previsioni utilizzando l'SDK AWS per Python (Boto3)

Gli esempi seguenti mostrano esempi di richieste per la visualizzazione delle spiegazioni di previsione utilizzando le API dell'SDK. `ListEventPredictions` `GetEventPredictionMetadata` AWS

Esempio 1: ottieni un elenco delle previsioni più recenti utilizzando l'API **`ListEventPredictions`**

```
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'
    }
 )
```

Esempio 2; Ottieni un elenco di previsioni passate per il tipo di evento «registrazione» tramite l'API **`ListEventPredictions`**

```
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'
    }
 )
```

Esempio 3: ottieni i dettagli di una previsione passata per un ID di evento, un tipo di evento, un ID del rilevatore e un ID di versione del rilevatore specificati generati nel periodo di tempo specificato utilizzando l'API. **`GetEventPredictionMetadata`**

Il valore `predictionTimestamp` specificato per questa richiesta si ottiene chiamando prima l'API. `ListEventPredictions`

```
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'
 )
```

Comprendere come vengono calcolate le spiegazioni delle previsioni

Amazon Fraud Detector utilizza SHAP (ShapeLey Additive Explanations) per spiegare le previsioni dei singoli eventi calcolando i valori di spiegazione non elaborati di ogni variabile di evento utilizzata per l'addestramento dei modelli. I valori di spiegazione non elaborati vengono calcolati dal modello come parte dell'algoritmo di classificazione durante la generazione delle previsioni. Questi valori esplicativi grezzi rappresentano il contributo di ciascun input al logaritmo delle probabilità di frode. I valori esplicativi non elaborati (da -infinity a +infinity) vengono convertiti in un valore di impatto relativo (da -5 a +5) utilizzando una mappatura. Il valore di impatto relativo derivato dal valore esplicativo grezzo rappresenta il numero di volte in cui le probabilità di frode (positive) o legittime (negative) aumentano, semplificando la comprensione delle spiegazioni delle previsioni.

Sicurezza in Amazon Fraud Detector

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili ad Amazon Fraud Detector, consulta AWS Services in Scope by Compliance Program AWS Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon Fraud Detector. I seguenti argomenti mostrano come configurare Amazon Fraud Detector per raggiungere i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon Fraud Detector.

Argomenti

Protezione dei dati in Amazon Fraud Detector

Il modello di responsabilità AWS condivisa Modello si applica alla protezione dei dati in Amazon Fraud Detector. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò vale anche quando lavori con Amazon Fraud Detector o altri dispositivi che Servizi AWS utilizzano la console, l'API o AWS gli AWS CLI SDK. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati a riposo

Amazon Fraud Detector crittografa i tuoi dati inattivi con una chiave di crittografia a tua scelta. È possibile scegliere una delle seguenti opzioni:

- Una chiave AWS KMS di proprietà. Se non specifichi una chiave di crittografia, i dati vengono crittografati con questa chiave per impostazione predefinita.
- Una chiave KMS gestita dal cliente. Puoi controllare l'accesso alla tua chiave KMS gestita dai clienti utilizzando le politiche chiave. Per informazioni sulla creazione e la gestione di una chiave KMS gestita dal cliente, consulta. Gestione delle chiavi

Crittografia dei dati in transito

Amazon Fraud Detector copia i dati dal tuo account e li elabora in un sistema interno AWS .
Per impostazione predefinita, Amazon Fraud Detector utilizza TLS 1.2 con AWS certificati per crittografare i dati in transito.

Gestione delle chiavi

Amazon Fraud Detector crittografa i dati utilizzando uno dei due tipi di chiavi:

- Una chiave AWS KMS di proprietà. Questa è l'impostazione predefinita.
- Una chiave KMS gestita dal cliente.

Creazione di una chiave KMS gestita dal cliente

Puoi creare una chiave KMS gestita dal cliente utilizzando la console AWS KMS o l'API. CreateKey
Quando crei la chiave assicurati di:

- Seleziona una chiave KMS con crittografia simmetrica gestita dal cliente, Amazon Fraud Detector non supporta chiavi KMS asimmetriche. Per ulteriori informazioni, consulta Asymmetric Keys nella Key Management Service Developer Guide. AWS KMS AWS
- Crea una chiave KMS per regione singola. Amazon Fraud Detector non supporta chiavi KMS multiregionali. Per ulteriori informazioni, consulta le chiavi multiregionali AWS KMS nella AWS Key Management Service Developer Guide.
- Fornisci la seguente politica chiave per concedere le autorizzazioni ad Amazon Fraud Detector per utilizzare la chiave.

```
        {
    "Effect": "Allow",
    "Principal": {
        "Service": "frauddetector.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
    ],
    "Resource": "*"
}
```

Per informazioni sulle politiche chiave, consulta Using Key Policies in AWS KMS nella AWS Key Management Service Developer Guide.

Crittografia dei dati utilizzando una chiave KMS gestita dal cliente

Utilizza l'EncryptionKeyAPI PutKMS di Amazon Fraud Detector per crittografare i dati inattivi di Amazon Fraud Detector utilizzando la chiave KMS gestita dal cliente. Puoi modificare la configurazione di crittografia in qualsiasi momento utilizzando l'API. `PutKMSEncryptionKey`

Note importanti sui dati crittografati

- I dati generati dopo la configurazione della chiave KMS gestita dal cliente sono crittografati. I dati generati prima della configurazione della chiave KMS gestita dal cliente rimarranno non crittografati.
- Se la chiave KMS gestita dal cliente viene modificata, i dati crittografati utilizzando la precedente configurazione di crittografia non verranno ricrittografati.

Visualizzare i dati

Quando utilizzi una chiave KMS gestita dal cliente per crittografare i dati di Amazon Fraud Detector, i dati crittografati con questo metodo non sono ricercabili utilizzando i filtri nell'area Search Past

Predictions della console Amazon Fraud Detector. Per garantire risultati di ricerca completi, utilizza una o più delle seguenti proprietà per filtrare i risultati:

- ID evento
- Timestamp di valutazione
- Stato del rilevatore
- Versione del rilevatore
- Versione del modello
- Tipo di modello
- Stato di valutazione delle regole
- Modalità di esecuzione delle regole
- Stato della corrispondenza delle regole
- Versione della regola
- Fonte di dati variabile

Se la chiave KMS gestita dal cliente è stata eliminata o è pianificata per l'eliminazione, i tuoi dati potrebbero non essere disponibili. Per ulteriori informazioni, consulta Eliminazione della chiave KMS.

Amazon Fraud Detector e endpoint VPC di interfaccia ()AWS PrivateLink

Puoi stabilire una connessione privata tra il tuo VPC e Amazon Fraud Detector creando un endpoint VPC di interfaccia. Gli endpoint di interfaccia sono basati su una tecnologia che consente di accedere in modo privato alle API di Amazon Fraud Detector senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione AWS Direct Connect. AWS PrivateLink Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con le API di Amazon Fraud Detector. Il traffico tra il tuo VPC e Amazon Fraud Detector non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più interfacce di rete elastiche nelle tue sottoreti.

Per ulteriori informazioni, consulta Interface VPC endpoints (AWS PrivateLink) nella Amazon VPC User Guide.

Considerazioni sugli endpoint VPC Amazon Fraud Detector

Prima di configurare un endpoint VPC di interfaccia per Amazon Fraud Detector, assicurati di esaminare le proprietà e le limitazioni degli endpoint dell'interfaccia nella Amazon VPC User Guide.

Amazon Fraud Detector supporta le chiamate a tutte le sue azioni API dal tuo VPC.

Le politiche degli endpoint VPC sono supportate per Amazon Fraud Detector. Per impostazione predefinita, l'accesso completo ad Amazon Fraud Detector è consentito tramite l'endpoint. Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Creazione di un endpoint VPC di interfaccia per Amazon Fraud Detector

Puoi creare un endpoint VPC per il servizio Amazon Fraud Detector utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Creazione di un endpoint dell'interfaccia nella Guida per l'utente di Amazon VPC.

Crea un endpoint VPC per Amazon Fraud Detector utilizzando il seguente nome di servizio:

- com.amazonaws.*region*.frauddetector

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API ad Amazon Fraud Detector utilizzando il nome DNS predefinito per la regione, ad esempio. `frauddetector.us-east-1.amazonaws.com`

Per ulteriori informazioni, consulta Accesso a un servizio tramite un endpoint dell'interfaccia in Guida per l'utente di Amazon VPC.

Creazione di una policy sugli endpoint VPC per Amazon Fraud Detector

Puoi creare una policy per gli endpoint VPC di interfaccia per Amazon Fraud Detector per specificare quanto segue:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite
- Le risorse sui cui si possono eseguire le azioni

Per ulteriori informazioni, consultare Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Il seguente esempio di policy sugli endpoint VPC specifica che tutti gli utenti che hanno accesso all'endpoint dell'interfaccia VPC possono accedere al rilevatore Amazon Fraud Detector denominato. `my_detector`

```
{
  "Statement": [
      {
          "Action": "frauddetector:*Detector",
          "Effect": "Allow",
          "Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/
my_detector",
          "Principal": "*"
      }
  ]
}
```

In questo esempio, viene rifiutato quanto segue:

- Altre azioni dell'API Amazon Fraud Detector
- Richiamo dell'API Amazon Fraud `GetEventPrediction` Detector

> **Note**
>
> In questo esempio, gli utenti possono comunque eseguire altre azioni dell'API Amazon Fraud Detector dall'esterno del VPC. Per informazioni su come limitare chiamate API per gli utenti interni al VPC, consulta Politiche basate sull'identità di Amazon Fraud Detector.

Rifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio

I dati storici sugli eventi che fornisci per addestrare modelli e generare previsioni vengono utilizzati esclusivamente per fornire e mantenere il tuo servizio. Questi dati potrebbero essere utilizzati anche per migliorare la qualità di Amazon Fraud Detector. La tua fiducia, la tua privacy e la sicurezza dei tuoi contenuti sono la nostra massima priorità e garantiscono che il nostro utilizzo sia conforme agli impegni che ci siamo assunti nei tuoi confronti. Per ulteriori informazioni, consulta le domande frequenti sulla privacy dei dati

Puoi scegliere di non utilizzare i dati degli eventi per sviluppare o migliorare la qualità di Amazon Fraud Detector visitando la pagina delle politiche di opt-out dei servizi di intelligenza artificiale nella Guida per l'utente di AWS Organizations e seguendo la procedura ivi spiegata.

> **Note**
>
> I tuoi account AWS dovranno essere gestiti centralmente da AWS Organizations per poter utilizzare la policy di opt-out. Se non hai ancora creato un'organizzazione per i tuoi account AWS, visita la pagina Creazione e gestione di un'organizzazione e segui la procedura qui spiegata.

Gestione delle identità e degli accessi per Amazon Fraud Detector

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Amazon Fraud Detector. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon Fraud Detector.

Utente del servizio: se utilizzi il servizio Amazon Fraud Detector per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Amazon Fraud Detector per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Amazon

Fraud Detector, consulta. Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Fraud Detector

Amministratore del servizio: se sei responsabile delle risorse di Amazon Fraud Detector della tua azienda, probabilmente hai pieno accesso ad Amazon Fraud Detector. È tuo compito determinare a quali funzionalità e risorse di Amazon Fraud Detector devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon Fraud Detector, consulta. Come funziona Amazon Fraud Detector con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler saperne di più su come scrivere policy per gestire l'accesso ad Amazon Fraud Detector. Per visualizzare esempi di policy basate sull'identità di Amazon Fraud Detector che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità di Amazon Fraud Detector

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Utenti e gruppi

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per

effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon Fraud Detector con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon Fraud Detector, è necessario comprendere quali funzionalità IAM sono disponibili per l'uso con Amazon Fraud Detector. Per avere una visione di alto livello di come Amazon Fraud Detector e AWS altri servizi funzionano con IAM, AWS consulta Services That Work with IAM nella IAM User Guide.

Argomenti

- Politiche basate sull'identità di Amazon Fraud Detector
- Politiche basate sulle risorse di Amazon Fraud Detector
- Autorizzazione basata sui tag Amazon Fraud Detector
- Ruoli IAM di Amazon Fraud Detector

Politiche basate sull'identità di Amazon Fraud Detector

Con le policy basate su identità di IAM, è possibile specificare quali azioni e risorse sono consentite o rifiutate, nonché le condizioni in base alle quali le azioni sono consentite o rifiutate. Amazon Fraud Detector supporta azioni, risorse e codici di condizione specifici. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Per iniziare a usare Amazon Fraud Detector, ti consigliamo di creare un utente con accesso limitato alle operazioni di Amazon Fraud Detector e autorizzazioni richieste. È possibile aggiungere altre autorizzazioni in base alle esigenze. Le seguenti politiche forniscono l'autorizzazione richiesta per utilizzare Amazon Fraud Detector: `AmazonFraudDetectorFullAccessPolicy` e. `AmazonS3FullAccess` Per ulteriori informazioni sulla configurazione di Amazon Fraud Detector utilizzando queste politiche, consulta. Configurazione per Amazon Fraud Detector

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le azioni politiche in Amazon Fraud Detector utilizzano il seguente prefisso prima dell'azione:. `frauddetector:` Ad esempio, per creare una regola con l'operazione dell'`CreateRule`API Amazon Fraud Detector, includi l'`frauddetector:CreateRule`azione nella policy. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Amazon Fraud Detector definisce il proprio set di azioni che descrivono le attività che puoi eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "frauddetector:action1",
      "frauddetector:action2"
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "frauddetector:Describe*"
```

Per visualizzare un elenco delle azioni di Amazon Fraud Detector, consulta Actions Defined by Amazon Fraud Detector nella IAM User Guide.

Risorse

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire

questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

I tipi di risorse definiti da Amazon Fraud Detector elencano tutti gli ARN di risorse Amazon Fraud Detector.

Ad esempio, per specificare il `my_detector` rilevatore nella dichiarazione, utilizza il seguente ARN:

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/my_detector"
```

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Per specificare tutti i rilevatori che appartengono a un account specifico, usa il carattere jolly (*):

```
"Resource": "arn:aws:frauddetector:us-east-1:123456789012:detector/*"
```

Alcune azioni di Amazon Fraud Detector, come quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse di Amazon Fraud Detector e dei relativi ARN, consulta Resources Defined by Amazon Fraud Detector nella IAM User Guide. Per sapere quali azioni puoi specificare l'ARN di ogni risorsa, consulta Actions Defined by Amazon Fraud Detector.

Chiavi di condizione

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni

condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Amazon Fraud Detector definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta AWS Global Condition Context Keys nella IAM User Guide.

Per visualizzare un elenco dei codici di condizione di Amazon Fraud Detector, consulta Condition Keys for Amazon Fraud Detector nella IAM User Guide. Per sapere quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Actions Defined by Amazon Fraud Detector.

Esempi

Per visualizzare esempi di politiche basate sull'identità di Amazon Fraud Detector, consulta. Esempi di policy basate sull'identità di Amazon Fraud Detector

Politiche basate sulle risorse di Amazon Fraud Detector

Amazon Fraud Detector non supporta politiche basate sulle risorse.

Autorizzazione basata sui tag Amazon Fraud Detector

Puoi allegare tag alle risorse Amazon Fraud Detector o passare i tag in una richiesta ad Amazon Fraud Detector. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento

condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Ruoli IAM di Amazon Fraud Detector

Un ruolo IAM è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Amazon Fraud Detector

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Ottieni credenziali di sicurezza temporanee chiamando operazioni AWS STS API come o. AssumeRoleGetFederationToken

Amazon Fraud Detector supporta l'utilizzo di credenziali temporanee.

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Amazon Fraud Detector non supporta ruoli collegati ai servizi.

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un ruolo di servizio per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli del servizio sono visualizzati nell'account e sono di proprietà dell'account. Ciò significa che un amministratore può modificare le autorizzazioni per questo ruolo. Tuttavia, il farlo potrebbe pregiudicare la funzionalità del servizio.

Amazon Fraud Detector supporta i ruoli di servizio.

Esempi di policy basate sull'identità di Amazon Fraud Detector

Per impostazione predefinita, gli utenti e i ruoli IAM non sono autorizzati a creare o modificare risorse Amazon Fraud Detector. Inoltre, non possono eseguire attività utilizzando l' AWS API AWS Management Console AWS CLI, o. Un amministratore deve creare le policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore devi quindi collegare queste policy a utenti o gruppi che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Argomenti

Best practice delle policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon Fraud Detector nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le politiche AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando

SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Policy gestita da AWS (predefinita) per Amazon Fraud Detector

AWS affronta molti casi d'uso comuni fornendo politiche IAM autonome create e amministrate da. AWS Queste policy AWS gestite concedono le autorizzazioni necessarie per i casi d'uso comuni, in modo da evitare di dover verificare quali autorizzazioni sono necessarie. Per ulteriori informazioni, consulta AWS Managed Policies nella AWS Identity and Access Management Management User Guide.

La seguente politica AWS gestita, che puoi allegare agli utenti del tuo account, è specifica di Amazon Fraud Detector:

`AmazonFraudDetectorFullAccess`: Garantisce l'accesso completo alle risorse, alle azioni e alle operazioni supportate di Amazon Fraud Detector, tra cui:

- Elenca e descrivi tutti gli endpoint del modello in Amazon SageMaker
- Elenca tutti i ruoli IAM nell'account
- Elenca tutti i bucket Amazon S3
- Consenti a IAM Pass Role di trasferire un ruolo ad Amazon Fraud Detector

Questa policy non fornisce un accesso S3 illimitato. Se devi caricare set di dati di addestramento dei modelli su S3, è richiesta anche la policy `AmazonS3FullAccess` gestita (o la policy di accesso personalizzata di Amazon S3 delimitata).

Puoi rivedere le autorizzazioni della policy accedendo alla console IAM e cercando in base al nome della policy. Puoi anche creare policy IAM personalizzate per consentire le autorizzazioni per le azioni e le risorse di Amazon Fraud Detector quando ne hai bisogno. Puoi collegare queste policy personalizzate agli utenti o ai gruppi che ne hanno bisogno.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
```

```
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Consenti l'accesso completo alle risorse di Amazon Fraud Detector

L'esempio seguente fornisce a un utente l'accesso Account AWS completo a tutte le risorse e le azioni di Amazon Fraud Detector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "frauddetector:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Consenti l'accesso in sola lettura alle risorse di Amazon Fraud Detector

In questo esempio, concedi a un utente in Account AWS sola lettura l'accesso alle tue risorse Amazon Fraud Detector.

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

Consenti l'accesso a una risorsa specifica

In questo esempio di politica a livello di risorsa, concedi a un utente l' Account AWS accesso a tutte le azioni e le risorse ad eccezione di una particolare risorsa Detector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "frauddetector:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "frauddetector:*Detector"
            ],
            "Resource": "arn:${Partition}:frauddetector:${Region}:${Account}:detector/
${detector-name}"
        }
    ]
}
```

Consenti l'accesso a risorse specifiche quando utilizzi l'API in modalità doppia

Amazon Fraud Detector fornisce API get in doppia modalità che funzionano sia come operazioni di elenco che di descrizione. Un'API in doppia modalità, se chiamata senza parametri, restituisce un elenco della risorsa specificata associata al tuo. Account AWS Un'API dual-mode quando viene chiamata con un parametro restituisce i dettagli della risorsa specificata. La risorsa può essere costituita da modelli, variabili, tipi di eventi o tipi di entità.

Le API dual-mode supportano le autorizzazioni a livello di risorsa nelle policy IAM. Tuttavia, le autorizzazioni a livello di risorsa vengono applicate solo quando uno o più parametri vengono forniti come parte della richiesta. Ad esempio, se l'utente chiama l'GetVariablesAPI e fornisce un nome variabile e se è presente una policy IAM Deny associata alla risorsa variabile o al nome della variabile, l'utente `AccessDeniedException` riceverà un errore. Se l'utente chiama l'`GetVariables`API e non specifica un nome di variabile, vengono restituite tutte le variabili, il che può causare perdite di informazioni.

Per consentire agli utenti di visualizzare solo i dettagli di risorse specifiche, utilizza un elemento di `NotResource` policy IAM in una policy IAM Deny. Dopo aver aggiunto questo elemento di policy a una policy IAM Deny, gli utenti possono solo visualizzare i dettagli delle risorse specificate nel `NotResource` blocco. Per ulteriori informazioni, consulta IAM JSON Policy elements: NotResource nella IAM User Guide.

La seguente policy di esempio consente agli utenti di accedere a tutte le risorse di Amazon Fraud Detector. Tuttavia, l'elemento `NotResource` policy viene utilizzato per limitare le chiamate GetVariablesAPI solo ai nomi delle variabili con i prefissi `euser*`. `job_*` `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*"
      ]
    }
  ]
}
```

Risposta

Per questo criterio di esempio, la risposta presenta il seguente comportamento:

- Una GetVariables chiamata che non include nomi di variabili genera un `AccessDeniedException` errore perché la richiesta è mappata all'istruzione Deny.
- Una GetVariables chiamata che include un nome di variabile non consentito genera un `AccessDeniedException` errore perché il nome della variabile non è mappato al nome della variabile nel `NotResource` blocco. Ad esempio, una GetVariables chiamata con un nome di variabile `email_address` genera un `AccessDeniedException` errore.
- Una GetVariables chiamata che include un nome di variabile che corrisponde a un nome di variabile nel `NotResource` blocco viene restituita come previsto. Ad esempio, una GetVariables chiamata che include il nome della variabile `job_cpa` restituisce i dettagli della `job_cpa` variabile.

Limitazione dell'accesso in base ai tag

Questo esempio di policy dimostra come limitare l'accesso ad Amazon Fraud Detector in base ai tag delle risorse. Questo esempio presuppone che:

- Nel tuo Account AWS hai definito due gruppi diversi, denominati Team1 e Team2
- Hai creato quattro rilevatori
- Vuoi consentire ai membri di Team1 di effettuare chiamate API su 2 rilevatori
- Vuoi consentire ai membri di Team2 di effettuare chiamate API sugli altri 2 rilevatori

Per controllare l'accesso alle chiamate API (esempio)

1. Aggiungi un tag con la chiave `Project` e il valore `A` ai rilevatori utilizzati da Team1.
2. Aggiungi un tag con la chiave `Project` e il valore `B` ai rilevatori utilizzati da Team2.
3. Crea una policy IAM con una `ResourceTag` condizione che neghi l'accesso ai rilevatori che hanno tag con chiave `Project` e valore `B` e allega tale policy a Team1.

4. Crea una policy IAM con una `ResourceTag` condizione che neghi l'accesso ai rilevatori che hanno tag con chiave `Project` e valore e allega tale policy a `A` Team2.

Di seguito è riportato un esempio di policy che nega azioni specifiche su qualsiasi risorsa Amazon Fraud Detector con un tag con una chiave e un `Project` valore di: `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"
        }
      }
    }
  ]
}
```

Prevenzione del "confused deputy"

Il problema del vicesceriffo si verifica quando un'entità che non è autorizzata a eseguire un'azione può costringere un'entità con più privilegi a eseguire l'azione. AWS fornisce strumenti che ti aiutano

a proteggere il tuo account se fornisci a terze parti (chiamati cross-account) o altri AWS servizi (chiamati cross-service) l'accesso alle risorse del tuo account.

Il problema dell'interlocutore confuso tra servizi può verificarsi quando un servizio (il servizio chiamante) chiama un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare che ciò si verifichi, potete creare policy che vi aiutino a proteggere i dati di tutti i servizi, affidando ai responsabili del servizio l'accesso alle risorse del servizio.

Amazon Fraud Detector supporta l'utilizzo dei ruoli di servizio nelle tue politiche di autorizzazione per consentire a un servizio di accedere alle risorse di un altro servizio per tuo conto. Un ruolo richiede due policy: una policy di attendibilità del ruolo, che specifica il principale a cui è consentito assumere il ruolo, e una policy delle autorizzazioni, che specifica le operazioni da eseguire con il ruolo. Quando un servizio assume un ruolo per tuo conto, il principale del servizio deve essere autorizzato a svolgere l'operazione `sts:AssumeRole` nella policy di attendibilità del ruolo. Quando un servizio chiama`sts:AssumeRole`, AWS STS restituisce un set di credenziali di sicurezza temporanee che il responsabile del servizio utilizza per accedere alle risorse consentite dalla politica di autorizzazione del ruolo.

Per evitare problemi di confusione tra servizi diversi, Amazon Fraud Detector consiglia di utilizzare `aws:SourceArn`le chiavi di contesto `aws:SourceAccount`e le chiavi di contesto della condizione globale nella politica di fiducia dei ruoli per limitare l'accesso al ruolo solo alle richieste generate dalle risorse previste.

`aws:SourceAccount`specifica l'ID account e `aws:SourceArn` specifica l'ARN della risorsa associata all'accesso tra servizi. `aws:SourceArn`Deve essere specificato utilizzando il formato ARN. Assicurati che entrambi `aws:SourceAccount` utilizzino lo stesso ID account quando vengono utilizzati nella stessa dichiarazione politica. `aws:SourceArn`

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn`con l'ARN completo della risorsa. Se non conosci l'ARN completo della risorsa o se stai specificando più risorse, usa la chiave `aws:SourceArn` global context condition con un wildcard (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`. Per informazioni sulle risorse e le azioni di Amazon Fraud Detector che puoi utilizzare nelle tue politiche di autorizzazione, consulta Azioni, risorse e codici di condizione per Amazon Fraud Detector.

Il seguente esempio di policy di role trust utilizza wildcard (*) nella chiave di `aws:SourceArn` condizione per consentire ad Amazon Fraud Detector di accedere a più risorse associate all'ID account.

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

La seguente politica di trust dei ruoli consente ad Amazon Fraud Detector di accedere solo `external-model` alle risorse. Notate il `aws:SourceArn` parametro nel blocco Condition. Il qualificatore di risorse viene creato utilizzando l'endpoint del modello fornito per effettuare la chiamata API. `PutExternalModel`

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

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Fraud Detector

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon Fraud Detector e IAM.

Argomenti

- Non sono autorizzato a eseguire alcuna azione in Amazon Fraud Detector
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Amazon Fraud Detector
- Amazon Fraud Detector non ha potuto assumere il ruolo assegnato

Non sono autorizzato a eseguire alcuna azione in Amazon Fraud Detector

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare il tuo amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'`mateojackson`utente tenta di utilizzare la console per visualizzare i dettagli su un *`rilevatore`* ma non dispone delle `frauddetector:`*`GetDetectors`* autorizzazioni.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 frauddetector:GetDetectors on resource: my-example-detector
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *my-example-detector* utilizzando l'azione `frauddetector:GetDetectors`.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon Fraud Detector.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon Fraud Detector. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse Amazon Fraud Detector

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon Fraud Detector supporta queste funzionalità, consulta. Come funziona Amazon Fraud Detector con IAM
- Per sapere come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Amazon Fraud Detector non ha potuto assumere il ruolo assegnato

Se ricevi un errore che indica che Amazon Fraud Detector non è in grado di assumere il ruolo specificato, devi aggiornare la relazione di trust per il ruolo specificato. Specificando Amazon Fraud Detector come entità affidabile, il servizio può assumere il ruolo. Quando utilizzi Amazon Fraud Detector per creare un ruolo, questa relazione di fiducia viene impostata automaticamente. Devi solo stabilire questa relazione di fiducia per i ruoli IAM che non sono stati creati da Amazon Fraud Detector.

Stabilire una relazione di fiducia per un ruolo esistente in Amazon Fraud Detector

1. Apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/
2. Nel riquadro di navigazione scegli Ruoli.
3. Scegli il nome del ruolo che desideri modificare e scegli la scheda Relazioni di fiducia.
4. Seleziona Modifica relazione di attendibilità.
5. In Policy Document (Documento policy), incolla quanto indicato di seguito, quindi seleziona Update Trust Policy (Aggiorna policy di trust).

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

```
            "Effect": "Allow",
            "Principal": {
                "Service": "frauddetector.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        } ]
    }
```

Registrazione e monitoraggio in Amazon Fraud Detector

AWS fornisce i seguenti strumenti di monitoraggio per monitorare Amazon Fraud Detector, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Per ulteriori informazioni CloudWatch, consulta la Amazon CloudWatch User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Per ulteriori informazioni sul monitoraggio di Amazon Fraud Detector, consulta. Monitora Amazon Fraud Detector

Convalida della conformità per Amazon Fraud Detector

I revisori di terze parti valutano la sicurezza e la conformità dei AWS servizi nell'ambito di più programmi di AWS conformità, come SOC, PCI, FedRAMP e HIPAA.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Ambito per programma di conformitàServizi AWS in Ambito di applicazione per programma Servizi AWS di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono i passaggi per l'implementazione di ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Amazon Fraud Detector

L'infrastruttura globale di è basata su regioni e zone di disponibilità . Le regioni forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle regioni e sulle zone di disponibilità AWS, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura in Amazon Fraud Detector

In quanto servizio gestito, Amazon Fraud Detector è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad Amazon Fraud Detector attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Monitora Amazon Fraud Detector

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon Fraud Detector e delle altre soluzioni AWS. AWS fornisce i seguenti strumenti di monitoraggio per monitorare Amazon Fraud Detector, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.

Argomenti

Monitoraggio di Amazon Fraud Detector con Amazon CloudWatch

Puoi monitorare Amazon Fraud Detector utilizzando CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Argomenti

Utilizzo di CloudWatch Metrics for Amazon Fraud Detector.

Per utilizzare i parametri, devi specificare le seguenti informazioni:

- Lo spazio dei nomi delle metriche. Un namespace è un contenitore in cui CloudWatch Amazon Fraud Detector pubblica le sue metriche. Se utilizzi l' CloudWatch ListMetricsAPI o il comando list-metrics per visualizzare i parametri per Amazon Fraud Detector, specifica lo spazio dei nomi. `AWS/FraudDetector`
- La dimensione del parametro. Una dimensione è una coppia nome-valore che ti aiuta a identificare in modo univoco una metrica, ad esempio può essere un nome di dimensione. `DetectorId` La specificazione di una dimensione metrica è facoltativa.
- Il nome del parametro, ad esempio `GetEventPrediction`.

Puoi ottenere dati di monitoraggio per Amazon Fraud Detector utilizzando l' AWS Management Console AWS CLI, la o l' CloudWatch API. Puoi anche utilizzare l' CloudWatch API tramite uno degli Amazon AWS Software Development Kit (SDK) o gli strumenti CloudWatch API. La console mostra una serie di grafici basati sui dati grezzi dell'API. CloudWatch In base alle tue esigenze, potresti decidere di utilizzare i grafici visualizzati nella console o quelli recuperati dall'API.

L'elenco seguente mostra alcuni usi comuni dei parametri. Questi suggerimenti sono solo introduttivi e non costituiscono un elenco completo.

Come?	Parametri rilevanti
Come posso tenere traccia del numero di previsioni che sono state eseguite?	Monitorare il parametro `GetEventPrediction` .
Come posso monitorare `GetEventPrediction` gli errori?	Usa le `GetEventPrediction4xxError` metriche `GetEventPrediction5xxError` e.
Come è possibile monitorare la latenza delle chiamate `GetEventPrediction` ?	Utilizza il parametro `GetEventPrediction Latency` .

È necessario disporre delle CloudWatch autorizzazioni appropriate per monitorare Amazon Fraud Detector CloudWatch. Per ulteriori informazioni, consulta Authentication and Access Control for Amazon CloudWatch.

Accedi ai parametri di Amazon Fraud Detector

I passaggi seguenti mostrano come accedere ai parametri di Amazon Fraud Detector utilizzando la console. CloudWatch

Come visualizzare i parametri (console)

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegli Metriche, scegli la scheda Tutte le metriche, quindi scegli Fraud Detector.
3. Scegli la dimensione dei parametri.
4. Selezionare il parametro desiderato dall'elenco e scegliere un periodo di tempo per il grafico.

Creazione di un allarme

Puoi creare un CloudWatch allarme che invia un messaggio Amazon Simple Notification Service (Amazon SNS) quando l'allarme cambia stato. Un allarme monitora un singolo parametro per un periodo di tempo specificato. L'allarme esegue una o più operazioni basate sul valore del parametro relativo a una soglia prestabilita per un certo numero di periodi. L'operazione corrisponde all'invio di una notifica a un argomento di Amazon SNS o a una policy di Auto Scaling.

Gli allarmi richiamano azioni solo per cambiamenti di stato sostenuti. CloudWatch gli allarmi non richiamano azioni semplicemente perché si trovano in uno stato particolare. È necessario che lo stato cambi e rimanga costante per un periodo specificato

Per impostare un allarme (console)

1. Accedi AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, scegli Allarmi e scegli Crea allarme. Si apre la procedura guidata per la creazione di allarmi.
3. Scegli Select Metric (Seleziona parametro).
4. Nella scheda Tutte le metriche, scegli Fraud Detector.
5. Scegli Per ID Detector, quindi scegli la metrica. GetEventPrediction

6. Seleziona la scheda Graphed metrics (Parametri nel grafico).
7. Per Statistic (Statistica), scegliere Sum (Somma).
8. Scegli Select Metric (Seleziona parametro).
9. Per Conditions, scegli Statico per il tipo di soglia e Maggiore per Whenever..., quindi inserisci un valore massimo a tua scelta. Seleziona Successivo.
10. Per inviare allarmi a un argomento Amazon SNS esistente, in Invia notifica a:, scegli un argomento SNS esistente. Per impostare il nome e gli indirizzi e-mail per un nuovo elenco di sottoscrizioni e-mail, scegli Nuova lista. CloudWatch salva l'elenco e lo visualizza sul campo in modo da poterlo utilizzare per impostare allarmi futuri.

> **Note**
>
> Se utilizzi New list per creare un nuovo argomento Amazon SNS, gli indirizzi e-mail devono essere verificati prima che i destinatari previsti ricevano le notifiche. Le e-mail vengono inviate da Amazon SNS solo quando l'allarme passa allo stato definito. Se questa modifica dello stato di allarme avviene prima della verifica degli indirizzi e-mail, i destinatari previsti non ricevono alcuna notifica.

11. Seleziona Successivo. Aggiungi un nome e una descrizione opzionale per la tua sveglia. Seleziona Successivo.
12. Scegli Crea allarme.

Metriche di Amazon Fraud Detector

Amazon Fraud Detector invia le seguenti metriche a. CloudWatch Tutte le metriche supportano queste statistiche:`Average`,,,`Minimum`. `Maximum` `Sum`

Parametro	Descrizione
`GetEventPrediction`	Il numero di richieste GetEventPrediction API. Dimensioni valide: `DetectorID`
`GetEventPredictionLatency`	L'intervallo di tempo impiegato per rispondere a una richiesta del client proveniente dalla GetEventPrediction richiesta.

Parametro	Descrizione
	Dimensioni valide: `DetectorID` Unità: millisecondi
`GetEventPrediction4XXError`	Il numero di GetEventPrediction richieste in cui Amazon Fraud Detector ha restituito un codice di risposta HTTP 4xx. Per ogni risposta 4xx, ne viene inviata 1. Dimensioni valide: `DetectorID`
`GetEventPrediction5XXError`	Il numero di GetEventPrediction richieste in cui Amazon Fraud Detector ha restituito un codice di risposta HTTP 5xx. Per ogni risposta 5xx, ne viene inviata 1. Dimensioni valide: `DetectorID`
`Prediction`	Il numero di previsioni. 1 viene inviato in caso di successo. Dimensioni valide:`DetectorID` , `DetectorVersionID`
`PredictionLatency`	L'intervallo di tempo impiegato per un'operazione di previsione. Dimensioni valide:, `DetectorID` `DetectorVersionID` Unità: millisecondi
`PredictionError`	Il numero di previsioni in cui Amazon Fraud Detector ha riscontrato un errore. Se si verifica un errore, viene inviato 1. Dimensioni valide:, `DetectorID` `DetectorVersionID`

Parametro	Descrizione
`VariableUsed`	Il numero di GetEventPrediction richieste in cui la variabile è stata utilizzata come parte della valutazione. Dimensioni valide:`DetectorID` ,`DetectorVersionID` , `VariableName`
`VariableDefaultReturned`	Il numero di GetEventPrediction richieste in cui la variabile non era presente come parte degli attributi degli eventi e quindi il valore predefinito per la variabile è stato utilizzato durante la valutazione. Dimensioni valide:`DetectorID` ,`DetectorVersionID` , `VariableName`
`RuleNotEvaluated`	Il numero di GetEventPrediction richieste per le quali la regola non è stata valutata perché una regola precedente corrispondeva. Dimensioni valide:`DetectorID` ,, `DetectorVersionID` `RuleID`
`RuleEvaluateTrue`	Il numero di GetEventPrediction richieste in cui la regola è stata attivata come True e il risultato della regola è stato restituito. Dimensioni valide:`DetectorID` ,, `DetectorVersionID` `RuleID`
`RuleEvaluateFalse`	Il numero di GetEventPrediction richieste per le quali la regola è stata valutata come False. Dimensioni valide:`DetectorID` ,, `DetectorVersionID` `RuleID`

Parametro	Descrizione
`RuleEvaluateError`	Il numero di GetEventPrediction richieste per le quali la regola viene valutata in modo errato Dimensioni valide:`DetectorID` , `DetectorVersionID` `RuleID`
`OutcomeReturned`	Il numero di GetEventPrediction chiamate in cui è stato restituito il risultato specificato. Dimensioni valide:`DetectorID` ,`DetectorVersionID` , `OutcomeName`
`ModelInvocation (Amazon SageMaker model endpoint)`	Il numero di GetEventPrediction richieste in cui l'endpoint del SageMaker modello è stato richiamato come parte della valutazione. Dimensioni valide:`DetectorID` ,, `DetectorVersionID` `ModelEndpoint`
`ModelInvocationError (Amazon SageMaker model endpoint)`	Il numero di GetEventPrediction richieste in cui l'endpoint del SageMaker modello richiamato ha restituito un errore durante la valutazione. Dimensioni valide:`DetectorID` ,, `DetectorVersionID` `ModelEndpoint`
`ModelInvocationLatency (Amazon SageMaker model endpoint)`	L'intervallo di tempo impiegato dal modello importato per rispondere visualizzato da Amazon Fraud Detector. Questo intervallo include solo la chiamata del modello. Dimensioni valide:,, `DetectorID` `DetectorVersionID` `ModelEndpoint` Unità: millisecondi

Parametro	Descrizione
`ModelInvocation`	Il numero di GetEventPrediction richieste in cui il modello è stato richiamato come parte della valutazione. Dimensioni valide:`DetectorID` ,,`DetectorVersionID` , `ModelType` `ModelID`
`ModelInvocationError`	Il numero di GetEventPrediction richieste in cui il modello Amazon Fraud Detector ha restituito un errore durante la valutazione. Dimensioni valide:`DetectorID` ,,`DetectorVersionID` , `ModelType` `ModelID`
`ModelInvocationLatency`	L'intervallo di tempo impiegato dal modello Amazon Fraud Detector per rispondere come visualizzato da Amazon Fraud Detector. Questo intervallo include solo la chiamata del modello. Dimensioni valide:`DetectorID` ,,, `DetectorVersionID` `ModelType` `ModelID` Unità: millisecondi

Registrazione delle chiamate API Amazon Fraud Detector con AWS CloudTrail

Amazon Fraud Detector è integrato con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon Fraud Detector. CloudTrail acquisisce tutte le chiamate API per Amazon Fraud Detector come eventi, incluse le chiamate dalla console Amazon Fraud Detector e le chiamate dal codice alle API di Amazon Fraud Detector.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon Fraud Detector. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata ad Amazon

Fraud Detector, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Informazioni su Amazon Fraud Detector in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Amazon Fraud Detector, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon Fraud Detector, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Amazon Fraud Detector supporta la registrazione di ogni azione (operazione API) come evento nei CloudTrail file di registro. Per ulteriori informazioni, consulta Operazioni.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di registro di Amazon Fraud Detector

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia stack ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`GetDetectors`operazione.

```
{
    "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"
}
```

Risoluzione dei problemi

Le seguenti sezioni ti aiutano a risolvere i problemi che potresti riscontrare quando lavori con Amazon Fraud Detector.

Risolvi i problemi relativi ai dati di addestramento

Utilizza le informazioni contenute in questa sezione per diagnosticare e risolvere i problemi che potresti riscontrare nel riquadro Model training diagnostico nella console Amazon Fraud Detector durante l'addestramento del modello.

I problemi visualizzati nel riquadro di diagnostica di addestramento del modello sono classificati come segue. Il requisito per risolvere il problema dipende dalla categoria del problema.

- Errore: causa il fallimento dell'addestramento del modello. Affinché il modello possa essere addestrato correttamente, è necessario risolvere questi problemi.
- Avverte fa sì che l'addestramento del modello continui, tuttavia alcune variabili potrebbero essere escluse dal processo di addestramento. Consulta le linee guida pertinenti in questa sezione per migliorare la qualità del tuo set di dati.
- Informa (Informazioni): non ha alcun impatto sull'addestramento del modello e tutte le variabili vengono utilizzate per l'addestramento. Ti consigliamo di consultare le linee guida pertinenti in questa sezione per migliorare ulteriormente la qualità del set di dati e le prestazioni del modello.

Argomenti

- Tipo di variabile mancante o errato
- Valori delle variabili mancanti
- Valori variabili univoci insufficienti
- Espressione variabile errata
- Entità uniche insufficienti

Tasso di frode instabile nel set di dati specificato

Tipo di problema: errore

Descrizione

Il tasso di frode nei dati forniti è troppo instabile nel tempo. Assicurati che le frodi e gli eventi legittimi vengano analizzati in modo uniforme nel tempo.

Causa

Questo errore si verifica se la frode e gli eventi legittimi presenti nel tuo set di dati sono distribuiti in modo non uniforme e provengono da fasce orarie diverse. Il modello di addestramento di Amazon Fraud Detector esegue esempi e partiziona il set di dati in base a EVENT_TIMESTAMP. Ad esempio, se il set di dati è composto da eventi di frode tratti dagli ultimi 6 mesi, ma è incluso solo l'ultimo mese di eventi legittimi, il set di dati è considerato instabile. Un set di dati instabile potrebbe portare a distorsioni nella valutazione delle prestazioni del modello.

Soluzione

Assicurati di fornire i dati sugli eventi fraudolenti e legittimi nello stesso intervallo di tempo e il tasso di frode non cambi drasticamente nel tempo.

Dati insufficienti

1. Tipo di problema: errore

   Descrizione

   Meno di 50 righe sono etichettate come eventi fraudolenti. Assicurati che sia gli eventi fraudolenti che quelli legittimi superino il numero minimo di 50 e riadatta il modello.

   Causa

Questo errore si verifica se il set di dati contiene un numero inferiore di eventi etichettati come fraudolenti rispetto a quelli richiesti per la formazione del modello. Amazon Fraud Detector richiede almeno 50 eventi fraudolenti per addestrare il tuo modello.

Soluzione

Assicurati che il set di dati includa almeno 50 eventi fraudolenti. Puoi garantirlo coprendo un periodo di tempo più lungo, se necessario.

2. Tipo di problema: Errore

   Descrizione

   Meno di 50 righe sono etichettate come eventi legittimi. Assicurati che sia gli eventi fraudolenti che quelli legittimi superino il numero minimo di $threshold e riaddestra il modello.

   Causa

   Questo errore si verifica se il set di dati contiene meno eventi etichettati come legittimi di quelli richiesti per l'addestramento del modello. Amazon Fraud Detector richiede almeno 50 eventi legittimi per addestrare il tuo modello.

   Soluzione

   Assicurati che il set di dati includa almeno 50 eventi legittimi. Puoi garantirlo coprendo un periodo di tempo più lungo, se necessario.

3. Tipo di problema: Errore

   Descrizione

   Il numero di entità uniche associate alla frode è inferiore a 100. Valuta la possibilità di includere altri esempi di entità fraudolente per migliorare le prestazioni.

   Causa

   Questo errore si verifica se il set di dati contiene un numero inferiore di entità con eventi fraudolenti rispetto a quanto richiesto per l'addestramento dei modelli. Il modello Transaction Fraud Insights (TFI) richiede almeno 100 entità con eventi fraudolenti per garantire la massima copertura del settore antifrode. Il modello potrebbe non essere generico se tutti gli eventi di frode vengono eseguiti da un piccolo gruppo di entità.

Soluzione

Assicurati che il set di dati includa almeno 100 entità con eventi fraudolenti. Puoi assicurarti che copra un periodo di tempo più lungo, se necessario.

4. Tipo di problema: Errore

   Descrizione

   Il numero di entità uniche associate a legittime è inferiore a 100. Valuta la possibilità di includere altri esempi di entità legittime per migliorare le prestazioni.

   Causa

   Questo errore si verifica se il set di dati contiene un numero di entità con eventi legittimi inferiore a quello richiesto per l'addestramento del modello. Il modello Transaction Fraud Insights (TFI) richiede almeno 100 entità con eventi legittimi per garantire la massima copertura del settore antifrode. Il modello potrebbe non generalizzare bene se tutti gli eventi legittimi vengono eseguiti da un piccolo gruppo di entità.

   Soluzione

   Assicurati che il set di dati includa almeno 100 entità con eventi legittimi. Puoi assicurarti che copra un periodo di tempo più lungo, se necessario.

5. Tipo di problema: Errore

   Descrizione

   Il set di dati contiene meno di 100 righe. Assicurati che ci siano più di 100 righe nel set di dati totale e che almeno 50 righe siano etichettate come fraudolente.

   Causa

   Questo errore si verifica se il set di dati contiene meno di 100 record. Amazon Fraud Detector richiede i dati di almeno 100 eventi (record) nel set di dati per la formazione dei modelli.

   Soluzione

   Assicurati di avere dati provenienti da più di 100 eventi nel tuo set di dati.

Valori EVENT_LABEL mancanti o diversi

1. Tipo di problema: errore

   Descrizione

   Più dell'1% della colonna EVENT_LABEL sono nulli o sono valori diversi da quelli definiti nella configurazione del modello. **`$label_values`** Assicurati di avere meno dell'1% dei valori mancanti nella colonna EVENT_LABEL e che i valori siano quelli definiti nella configurazione del modello. **`$label_values`**

   Causa

   Questo errore si verifica per uno dei seguenti motivi:

   - Oltre l'1% dei record nel file CSV contenente i dati di allenamento presenta valori mancanti nella colonna EVENT_LABEL.
   - Più dell'1% dei record del file CSV contenente i dati di allenamento hanno valori nella colonna EVENT_LABEL diversi da quelli associati al tipo di evento.

   Il modello Online Fraud Insights (OFI) richiede che la colonna EVENT_LABEL di ogni record sia compilata con una delle etichette associate al tipo di evento (o mappata). `CreateModelVersion`

   Soluzione

   Se questo errore è dovuto ai valori EVENT_LABEL mancanti, valuta la possibilità di assegnare etichette appropriate a tali record o di eliminare tali record dal set di dati. Se questo errore è dovuto al fatto che le etichette di alcuni record non sono presenti**`label_values`**, assicurati di aggiungere tutti i valori nella colonna EVENT_LABEL alle etichette del tipo di evento e di averli mappati in modo fraudolento o legittimo (fraudolento, legittimo) nella creazione del modello.
2. Tipo di problema: Informazioni

   Descrizione

   La colonna EVENT_LABEL contiene valori nulli o valori di etichetta diversi da quelli definiti nella configurazione del modello. **`$label_values`** Questi valori incoerenti sono stati convertiti in «non fraudolenti» prima dell'addestramento.

   Causa

Ottieni queste informazioni per uno dei seguenti motivi:

- Meno dell'1% dei record nel file CSV contenente i dati di allenamento presenta valori mancanti nella colonna EVENT_LABEL
- Meno dell'1% dei record del file CSV contenente i dati di allenamento hanno valori nella colonna EVENT_LABEL diversi da quelli associati al tipo di evento.

Il modello di formazione in entrambi i casi avrà successo. Tuttavia, i valori di etichetta di quegli eventi con valori di etichetta mancanti o non mappati vengono convertiti in legittimi. Se ritieni che questo sia un problema, segui la soluzione fornita di seguito.

Soluzione

Se nel set di dati mancano dei valori EVENT_LABEL, valuta la possibilità di eliminare tali record dal set di dati. Se i valori forniti per tali EVENT_LABELS non sono mappati, assicurati che tutti quei valori siano mappati su valori fraudolenti o legittimi (fraudolenti, legittimi) per ogni evento.

Valori EVENT_TIMESTAMP mancanti o errati

1. Tipo di problema: errore

   Descrizione

   Il set di dati di allenamento contiene EVENT_TIMESTAMP con timestamp che non sono conformi ai formati accettati. Assicurati che il formato sia uno dei formati di data/ora accettati.

   Causa

   Questo errore si verifica se la colonna EVENT_TIMESTAMP contiene un valore non conforme ai formati di timestamp supportati da Amazon Fraud Detector.

   Soluzione

   Assicurati che i valori forniti per la colonna EVENT_TIMESTAMP siano conformi ai formati di timestamp supportati. Se nella colonna EVENT_TIMESTAMP mancano dei valori, puoi riempirli con valori utilizzando il formato di timestamp supportato o considerare di eliminare completamente l'evento invece di inserire stringhe come, o. `none` `null` `missing`
2. Tipo di problema: Errore

Il set di dati di allenamento contiene EVENT_TIMESTAMP con valori mancanti. Assicurati di non avere valori mancanti.

Causa

Questo errore si verifica se la colonna EVENT_TIMESTAMP nel set di dati presenta valori mancanti. Amazon Fraud Detector richiede che la colonna EVENT_TIMESTAMP nel set di dati contenga valori.

Soluzione

Assicurati che la colonna EVENT_TIMESTAMP nel tuo set di dati contenga dei valori e che tali valori siano conformi ai formati di timestamp supportati. Se nella colonna EVENT_TIMESTAMP mancano dei valori, puoi riempirli con valori utilizzando il formato di timestamp supportato o considerare di eliminare completamente l'evento invece di inserire stringhe come,, o. `none` `null` `missing`

Dati non ingeriti

Tipo di problema: errore

Descrizione

Nessun evento importato trovato per la formazione, controlla la configurazione dell'allenamento.

Causa

Questo errore si verifica se stai creando un modello con dati sugli eventi archiviati con Amazon Fraud Detector ma non hai importato il set di dati in Amazon Fraud Detector prima di iniziare ad addestrare il modello.

Soluzione

Utilizza l'operazione `SendEvent` API, l'operazione `CreateBatchImportJob` API o la funzionalità di importazione in batch nella console Amazon Fraud Detector per importare prima i dati degli eventi e poi addestrare il modello. Per ulteriori informazioni, consulta Set di dati di eventi archiviati.

> **Note**
>
> Ti consigliamo di attendere 10 minuti dopo aver terminato l'importazione dei dati prima di utilizzarli per addestrare il modello.

Puoi utilizzare la console Amazon Fraud Detector per verificare il numero di eventi già archiviati per ogni tipo di evento. Per ulteriori informazioni, consulta Visualizzazione delle metriche degli eventi memorizzati.

Variabili insufficienti

Tipo di problema: errore

Descrizione

Il set di dati deve contenere almeno 2 variabili adatte all'addestramento.

Causa

Questo errore si verifica se il set di dati contiene meno di 2 variabili adatte per l'addestramento del modello. Amazon Fraud Detector considera una variabile adatta per l'addestramento dei modelli solo se supera tutte le convalide. Se una variabile non viene convalidata, viene esclusa dall'addestramento del modello e verrà visualizzato un messaggio in Model training diagnostic.

Soluzione

Assicurati che il set di dati contenga almeno due variabili popolate con valori e che abbia superato tutte le convalide dei dati. Tieni presente che la riga dei metadati dell'evento in cui hai fornito le intestazioni delle colonne (EVENT_TIMESTAMP, EVENT_ID, ENTITY_ID, EVENT_LABEL, ecc.) non è considerata variabile.

Tipo di variabile mancante o errato

Tipo di problema: avviso

Descrizione

Il tipo di dati previsto per **`$variable_name`** è NUMERIC. Rivedi e aggiorna **`$variable_name`** il tuo set di dati e riaddestra il modello.

Causa

Questo avviso viene visualizzato se una variabile è definita come variabile NUMERIC, ma nel set di dati contiene valori che non possono essere convertiti in NUMERIC. Di conseguenza, tale variabile viene esclusa dall'addestramento del modello.

Soluzione

Se desideri mantenerla come variabile NUMERIC, assicurati che i valori forniti possano essere convertiti in numeri mobili. Nota che se la variabile contiene valori mancanti, non riempirla con stringhe comenonene, `null` o. `missing` Se la variabile contiene valori non numerici, ricreala come tipo di variabile CATEGORICAL o FREE_FORM_TEXT.

Valori delle variabili mancanti

Tipo di problema: avviso

Descrizione

Nel set di dati di allenamento non **`$variable_name`** sono presenti **`$threshold`** valori superiori a «for». Valuta la possibilità di modificare **`$variable_name`** il set di dati e riaddestrarlo per migliorare le prestazioni.

Causa

Questo avviso viene visualizzato se la variabile specificata viene eliminata a causa di troppi valori mancanti. Amazon Fraud Detector consente valori mancanti per una variabile. Tuttavia, se una variabile ha troppi valori mancanti, non contribuisce molto al modello e tale variabile viene eliminata durante la formazione del modello.

Soluzione

Innanzitutto, verifica che i valori mancanti non siano dovuti a errori nella raccolta e nella preparazione dei dati. Se si tratta di errori, puoi prendere in considerazione l'idea di eliminarli dalla tua formazione sui modelli. Tuttavia, se ritieni che i valori mancanti siano importanti e desideri comunque mantenere tale variabile, puoi riempire manualmente i valori mancanti con una costante sia nell'addestramento del modello che nell'inferenza in tempo reale.

Valori variabili univoci insufficienti

Tipo di problema: avviso

Descrizione

Il numero di valori univoci di **`$variable_name`** è inferiore a 100. Rivedi e aggiorna **`$variable_name`** il tuo set di dati e riaddestra il modello.

Causa

Viene visualizzato questo avviso se il numero di valori univoci della variabile specificata è inferiore a 100. Le soglie variano a seconda del tipo di variabile. Con pochissimi valori univoci, c'è il rischio che il set di dati non sia abbastanza generale da coprire lo spazio delle funzionalità di quella variabile. Di conseguenza, il modello potrebbe non generalizzare bene sulle previsioni in tempo reale.

Soluzione

Innanzitutto, assicurati che la distribuzione variabile sia rappresentativa del traffico aziendale reale. Quindi, puoi adottare variabili più elaborate con cardinalità più elevata, ad esempio utilizzarle `full_customer_name` al posto di `first_name` e `last_name` separatamente, oppure modificare il tipo di variabile in CATEGORICAL, che consente una cardinalità inferiore.

Espressione variabile errata

1. Tipo di problema: Informazioni

   Descrizione

   Più del 50% dei **`$email_variable_name`** valori non corrispondono all'espressione regolare prevista http://emailregex.com. Valuta la possibilità di modificare **`$email_variable_name`** il set di dati e riaddestrarlo per migliorare le prestazioni.

   Causa

   Queste informazioni vengono visualizzate se più del 50% dei record del set di dati contengono valori di posta elettronica che non sono conformi a un'espressione e-mail normale e non sono quindi convalidati.

   Soluzione

   Formattate i valori delle variabili e-mail in modo che siano conformi all'espressione regolare. Se mancano dei valori e-mail, consigliamo di lasciarli vuoti invece di riempirli con stringhe come `nonenull`, `omissing`.
2. Tipo di problema: Informazioni

   Descrizione

Più del 50% dei **$IP_variable_name** valori non corrisponde all'espressione regolare per gli indirizzi IPv4 o IPv6 https://digitalfortress.tech/tricks/top-15 - /. commonly-used-regex Valuta la possibilità di modificare il set di dati e **$IP_variable_name** riaddestrarlo per migliorare le prestazioni.

Causa

Queste informazioni vengono visualizzate se più del 50% dei record del set di dati presentano valori IP che non sono conformi a un'espressione IP normale e non sono quindi convalidati.

Soluzione

Formatta i valori IP in modo che siano conformi all'espressione regolare. Se mancano dei valori IP, consigliamo di lasciarli vuoti invece di riempirli con stringhe come `nonenull`, o`missing`.

3. Tipo di problema: Informazioni

   Descrizione

   Oltre il 50% dei **$phone_variable_name** valori non corrisponde all'espressione regolare telefonica di base /$pattern/. Valuta la possibilità di modificare il **$phone_variable_name** set di dati e riaddestrarlo per migliorare le prestazioni.

   Causa

   Queste informazioni vengono visualizzate se più del 50% dei record del set di dati contengono numeri di telefono che non sono conformi alla normale espressione di un numero di telefono e non sono quindi convalidati.

   Soluzione

   Formatta i numeri di telefono in modo che rispettino l'espressione regolare. Se mancano dei numeri di telefono, consigliamo di lasciarli vuoti invece di riempirli con stringhe come`none`,`null`, o`missing`.

Entità uniche insufficienti

Tipo di problema: Informazioni

Descrizione

Il numero di entità uniche è inferiore a 1500. Valuta la possibilità di includere più dati per migliorare le prestazioni.

Causa

Queste informazioni vengono visualizzate se il set di dati ha un numero inferiore di entità uniche rispetto al numero consigliato. Il modello Transaction Fraud Insights (TFI) utilizza sia aggregati di serie temporali che funzionalità di transazione generiche per fornire le migliori prestazioni. Se il set di dati contiene troppo poche entità univoche, la maggior parte dei dati generici, come IP_ADDRESS, EMAIL_ADDRESS, potrebbe non avere valori univoci. Inoltre, c'è anche il rischio che questo set di dati non sia abbastanza generico da coprire lo spazio delle funzionalità di quella variabile. Di conseguenza, il modello potrebbe non generalizzarsi bene sulle transazioni provenienti da nuove entità.

Soluzione

Includi più entità. Estendi l'intervallo temporale dei dati di allenamento, se necessario.

Quote

Il tuoAccount AWS dispone di quote di default, precedentemente definite limiti, per ogni servizio Web Amazon. Salvo dove diversamente specificato, ogni quota si applica a una regione specifica. Puoi richiedere un aumento di quota per tutte le quote regolabili menzionate nelle tabelle di seguito. Per ulteriori informazioni, consulta Richiesta esta esta esta esta esta esta esta esta esta esta esta esta esta esta esta esta

Le tabelle seguenti descrivono le quote di Amazon Fraud Detector per componente.

Modelli Amazon Fraud Detector

Nome quota	Quota predefinita	Adattabile
Dimensione dei dati di addestramento	5 GB	No
Modelli per account	50	No
Versioni per modello	200	No
Versioni dei modelli implementati per account	5	No
Processi di addestramento simultanei per account	3	No
Processi di addestramento simultanei per modello	1	No

Rilevatori di frodi Amazon Fraud Detector /variabili/risultati/regole

Nome quota	Quota predefinita	Adattabile
Variabili per account	5000	No

Nome quota	Quota predefinita	Adattabile
Regole per account	5000	No
Elenchi per regola	3	No
Risultati per account	5000	No
Rilevatori per account	100	No
Elenchi per rilevatore	30	No
Versioni di default per rivelatore	100	No
Modelli per versione di rilevatore	10	No
Etichette per account	100	No
Tipi di eventi per account	100	No
Tipi di entità per account	100	No

API di Amazon Fraud Detector

Nome quota	Quota predefinita	Adattabile
GetEventPrediction Chiesta API al secondo	200 TPS	Sì
Dimensione del payload per chiamata GetEventPrediction API	256 KB	No
Numero di ingressi per chiamata GetEventPrediction API	5000	No

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti nella Guida per l'utente di Amazon Fraud Detector. Inoltre, aggiorniamo frequentemente la Guida per l'utente di Amazon Fraud Detector per rispondere al feedback che ci invii.

Modifica	Descrizione	Data
Nuovi tipi di variabili e dati	Amazon Fraud Detector introduce nuovi tipi di variabili e un tipo di dati che puoi utilizzare per estrarre informazioni utili.	5 giugno 2023
Orchestrazione di eventi	L'orchestrazione degli eventi semplifica l'invio di eventi per l'elaborazione a Servizi AWS valle, utilizzando Amazon. EventBridge	30 maggio 2023
Elenchi	La risorsa Lists consente di fare riferimento a un set di valori come indirizzi IP o indirizzi e-mail, come parte di una regola. Utilizza gli elenchi in una regola per consentire o negare l'accesso o una transazione.	14 febbraio 2023
Esplora modelli di dati	Data Models Explorer fornisce informazioni sugli elementi di dati richiesti da Amazon Fraud Detector per creare il tuo modello di rilevamento delle frodi. Usa Data Models Explorer prima di preparare il set di dati dell'evento.	15 dicembre 2022

Modello Account Takeover Insights	Utilizza il modello Account takeover insights (ATI) per rilevare gli account compromessi a causa di acquisizioni dolose, phishing o furto di credenziali.	21 luglio 2022
Aggiornamento del capitolo	È stato aggiornato il capitolo introduttivo con informazioni aggiuntive su Amazon Fraud Detector	11 aprile 2022
Arricchimento variabile	Abilita l'arricchimento di alcuni dei dati grezzi che fornisci per migliorare le prestazioni dei modelli che utilizzano questi elementi di dati e che sono stati addestrati prima dell'8 febbraio 2022.	8 febbraio 2022
Politiche di opt-out	Utilizza le politiche di opt-out per rifiutare l'utilizzo dei dati del tuo evento per sviluppare o migliorare la qualità di Amazon Fraud Detector.	6 gennaio 2022
Prevenzione sostitutiva confusa	Crea politiche per impedire a un'entità terza o inter-ser vice di manipolare un'entità autorizzata ad agire per suo conto per accedere alle risorse del tuo account.	6 dicembre 2021
Crea set di dati di eventi	Usa la guida fornita in Crea set di dati per eventi per preparare e raccogliere dati per addestrare il tuo modello.	22 novembre 2021

Spiegazioni della previsione	Usa le spiegazioni sulla previsione per scoprire in che modo ogni variabile di evento ha influito sui punteggi di previsione delle frodi del tuo modello.	10 novembre 2021
Risoluzione dei problemi	Usa le informazioni in Risoluzione dei problemi relativi ai dati di addestramento per diagnosticare e risolvere i problemi che potresti riscontrare nella console Amazon Fraud Detector durante l'addestramento del tuo modello.	11 ottobre 2021
Modello di analisi sulle frodi nelle transazioni	Utilizza il modello Transaction Fraud Insights (TFI) per rilevare frodi online o card-not-present relative a transazioni.	11 ottobre 2021

Eventi memorizzati	Archivia i dati dei tuoi eventi in Amazon Fraud Detector e utilizza i dati memorizzati per addestrare successivamente i tuoi modelli. Archiviando i dati degli eventi in Amazon Fraud Detector, puoi addestrare modelli che utilizzano variabili calcolate automaticamente per migliorare le prestazioni, semplificare la riqualificazione dei modelli e aggiornare le etichette antifrode per chiudere il ciclo di feedback sull'apprendimento automatic o.	11 ottobre 2021
Importanza della variabile del modello	Usa l'importanza delle variabili del modello per ottenere informazioni su ciò che determina l'aumento o il calo delle prestazioni del tuo modello e quali delle variabili del tuo modello contribui scono maggiormente. Quindi modifica il tuo modello per migliorare le prestazioni complessive.	9 luglio 2021
Integrazione con AWS CloudFormation	Utilizzalo AWS CloudForm ation per gestire le tue risorse di Amazon Fraud Detector.	10 maggio 2021

Previsioni in batch	Usa le previsioni in batch per ottenere previsioni per una serie di eventi che non richiedono punteggi in tempo reale.	31 marzo 2021
Rielaborazione dei capitoli	Rielaborazione di Guida introduttiva e di altre sezioni	17 luglio 2020
Versione iniziale	Versione iniziale	2 dicembre 2019

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.